II. TECHNOLOGY

The NII has the potential to be a robust and widely used medium for the creation, dissemination and use of information-based products and services. To realize this goal, the technical and security needs of users, service providers, carriers and content providers must be addressed. First, to be successful, the NII must deliver on its promise to facilitate the flow of information and information-based products and services to consumers. The easier it is for a consumer to retrieve, purchase or use an information product or service, the more likely it is that the consumer will do so. Second, content providers must have secure and reliable means for delivering information products and services to consumers. This means that content providers must be confident that the systems developed to distribute these works will be secure and that works placed on these systems will remain authentic and unaltered. If content providers cannot be assured that they will be able to realize a commercial gain from the sale and use of their products using the NII, they will have little incentive to use it. Third, service providers and carriers must be able to ensure that their systems which will serve as the physical infrastructure of the NII will address the needs of users and content providers.

Technological solutions are playing and will continue to play a significant role in meeting these needs. A wide variety of new tools to facilitate access and use of Internet-based information products and services are being rapidly developed and deployed. Concurrently, copyright owners are developing and implementing technical solutions to facilitate the delivery of protected works in an easy, consumer-friendly yet reliable and secure way. These solutions enable copyright owners not only to protect their works against unauthorized access, reproduction, manipulation, distribution, performance or display, but also serve to assure the integrity of these works and to address copyright management and licensing concerns.

A. CONTENT SECURITY AND USER ACCESS NEEDS

It is important to recognize that access needs of users of the NII have to be considered in context with the needs of copyright owners to ensure that their rights in their works are recognized and protected. One important factor is the extent to which the marketplace will tolerate measures that restrict access to or use of a copyrighted work. Conversely, without providing a secure environment where copyright owners can be assured that there will be some degree of control over who may access, retrieve and use a work, and, perhaps most importantly, how to effectuate limits on subsequent dissemination of that work without the copyright owner's consent, copyright owners will not make those works available through the NII.[505]

Technology can provide the solutions for these needs. Technological solutions exist today and improved means are being developed to better protect digital works through varying combinations of hardware and software. Protection schemes can be implemented at the level of the copyrighted work or at more comprehensive levels such as the operating system, the network or both. For example, technological solutions can be used to prevent or restrict access to a work; limit or control access to the source of a work; limit reproduction, adaptation, distribution, performance or display of the work; identify attribution and ownership of a work; and manage or facilitate copyright licensing.

[505] For a detailed discussion of these and other applications of technology that may be used to provide protection for copyrighted works, *see* Symposium, Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment, cosponsored by the Coalition for Networked Information, Harvard University, Interactive Multimedia Association, and the Massachusetts Institute of Technology (April 2-3, 1993); *see also* M. D. Goldberg & J. M. Feder, *Copyright and Technology: The Analog, the Digital, and the Analogy*, Symposium, WIPO Worldwide Symposium on the Impact of Digital Technology on Copyright and Neighboring Rights, 37 (March 31 - April 2, 1993).

B. THE INTERNET EXPERIENCE

In the past few years, there has been an explosion in the popularity and volume of use of the Internet. The Internet serves today, through electronic mail and remote access, to connect people to information and to deliver information products and services. An almost incomprehensible variety of information has been made widely and easily accessible through this system, originally designed to serve the needs of the Department of Defense in the 1960s.

Because the Internet and applications which use it, like electronic mail and "World Wide Web," have exploded in popularity and use, systems used today and being designed for short term implementation are likely to serve as the foundation for communications through the NII. Indeed, in one very real sense, the Internet that is in use today is a prototype for the NII. Therefore, it is useful to discuss briefly the foundation of the Internet as it exists today.

The Internet provides individuals many different ways to disseminate and retrieve information. The basic concept of communications underlying the Internet is that a user with his or her personal computer or workstation can "connect," either directly or through a succession of intermediary computers, in a uniform manner to a "remote" computer that acts as a "server" of information. The user attaches to the remote computer and uses the services offered by the remote computer system (hence the term "server" for the remote system). The service may provide for immediate transfer of information (*e.g.*, file transfer) or eventual transmission (*e.g.*, electronic mail). For example, a user can direct a remote computer to send data through an established connection to the user's computer. Alternatively, the user can send information to the remote computer that will eventually result in information being sent back to the user's computer from that remote computer. In either sense, there is a "connection" established between the two computers that permits the flow of information, typically at the request of the user.

The simplest type of connections use a character-based "dumb terminal" interface (*e.g.*, characters alone are used to convey information to and from the user). This type of scheme consists essentially of the user using his computer to do nothing more than type commands which the computer executes. The "controlled" computer executes the appropriate programs that handle location and transfer of data. One such scheme is the "telnet" protocol. Telnet uses a command line interface (*e.g.*, one types commands) to initiate actions at the remote computer. Using telnet, a user can execute a program or routine on a remote computer to obtain a directory of files resident on that computer, navigate among directories of information, and transfer files.

If a user wishes to simply retrieve information stored as a file on the remote server, he or she can execute a process on the remote computer termed "file transfer protocol" or ftp. This is the most basic form of transfer; one simply instructs the remote computer to send to a specific file resident on the remote computer to the requester's computer. A menu driven interface and service for retrieving files from remote servers was subsequently developed by the University of Minnesota. This scheme, termed "gopher," relies on established directories of information that are consolidated at specific sites on the Internet. The requester uses his or her computer to instruct the remote computer to execute the gopher program, which then establishes a connection to a directory server (*e.g.*, a "gopher server"). The gopher server will provide the requesting user easily navigable listings of files that can be retrieved from the gopher server. The gopher server acts more or less as a conduit for identifying a specific file and delivering it to the requesting computer.

Other schemes have been established for searching pre-established indices of information about information resources on the Internet. Examples include "Archie," "Veronica" and the Wide Area Information Search (WAIS).[506] All of these examples were originally developed as UNIX-implemented programs to perform file transfer-related tasks; namely, searching and retrieval of information about either the location of remote servers with certain types of information or of remote servers that had specific files. The information sent back to the user with these tools consists of information about these servers that can then be used with the other tools (*e.g.*, ftp or gopher) to retrieve a specific file.

There are now more sophisticated tools for users to access and retrieve information on remote servers on the Internet. These tools typically are programs that implement the common UNIX-based protocols but which actually run on the user's personal computer or workstation. Thus, once a connection to an appropriate "Internet provider" is established, a user may start a program on his personal computer that acts as a "gopher client." The "gopher client" will permit the user to retrieve information from a remote server directly to his or her personal computer. Connections between the user's personal computer and the "Internet provider" to carry these communications can be established using a "dial-up" or analog phone connection using an appropriate communication protocol or a link over a digital transmission line. The most significant benefit of these tools is that they are typically based on a graphical interface, which makes it easier for the user to manage the connection and interact with remote servers.

Many of the established protocols have been integrated and enhanced using tools that can access what is termed the World Wide Web. The World Wide Web (Web) is a scheme whereby organizations use graphical

[506] Archie is a service which provides directories of repositories of gopher servers; Veronica provides indices of documents which contain key words.

"front ends" to provide remote users with point and click access to information stored on their servers, as well as access through "links" to information stored on other remote servers. Web "browsers" are programs that run on a personal computer or workstation that enable a user to establish connections to these graphical front ends, view, retrieve and manipulate data provided by those remote servers. Examples of popular, currently available Web browsers include: Mosaic, from the National Center for Supercomputing Applications; Netscape Navigator, from Netscape Communications Corporation; and Enhanced Mosaic, from Spyglass, Inc. Web browsers typically provide support for electronic mail, gopher and ftp sessions, and, most importantly, support retrieval and display of a much broader variety of information (*e.g.*, text, audio, image and multimedia data).

At the root of the Web are several of the established protocols (*e.g.*, gopher, ftp, various e-mail standards) and three new protocols: the Hypertext Markup Language (HTML), a file format for embedding navigational information in graphical and text-based documents; the Hypertext Transfer Protocol (HTTP), a communications protocol for communicating navigational information and other data between the remote server and the requesting computer; and the Uniform Resource Locator (URL) scheme for identifying the location (*e.g.*, the location of the remote server and the location on that server of the file corresponding to the URL) of Web-accessible documents. A number of organizations and groups are also working to develop additional protocols to enable secure communications. Some of these protocols have been published as draft specifications at this point, including the Secure Sockets Layer (SSL), the Secure Hypertext Transfer Protocol (SHTTP) and the Enhanced Mosaic Security Framework. The integration of these various protocols into a single, easy to use, understandable interface has led to a tremendous increase in the popularity and use of the World Wide Web and, correspondingly, of the Internet as a means for providing and retrieving information.

C. ACCESS AND USE TECHNOLOGICAL CONTROLS

1. SERVER AND FILE LEVEL CONTROLS

Technology will likely play a central role in implementing controls on the access to and use of protected works at both the file and server level.

Distribution of digital works can be regulated by controlling access to the source of copies of the works -- information or data servers. Access to these servers can vary from completely uncontrolled access (*e.g.*, the full contents of the server are available without restriction) to partially controlled access (*e.g.*, unrestricted access is granted to only certain data on the server) to completely controlled access (*e.g.*, no uncontrolled access in any form is permitted). Access control is affected through user identification and authentication procedures that deny access to unauthorized users to a server or to particular information on a server.[507]

[507] The most common elements of such systems involve authentication of the user desiring access to the server. Typically, the server will require entry of a user name and a password. More elaborate mechanisms, however, have been developed. For example, some servers do not grant access once a user is verified, but rather, they terminate the connection and reestablish it from the server to the registered user's site. Such call-back systems tend to govern fully controlled server environments (*e.g.*, where access will only be granted to known and verified users). Other systems are being implemented that use more elaborate authentication systems. For example, a number of companies are developing hardware key systems that require the user, after establishing a preliminary connection, to verify that connection by inserting a hardware device similar to a credit card into the user's computer system. That device then sends an indecipherable code to verify the identity of the user.

Protection of works by means of access control mechanisms assumes that the system in question is in a physically secure environment and is not vulnerable to external means to circumvent access control. Several instances have been reported where the security of a supposedly secure server system was compromised, for example, through passive monitoring during the exchange of unencrypted passwords. As a consequence, many are currently pursuing efforts to improve security at the access control level.

Nearly all service providers, including commercial on-line services such as CompuServe and America Online, private dial-up bulletin board systems, and servers accessible through the Internet, control access to their systems. For example, via the Internet, users today can connect to a bewildering array of public servers using a variety of schemes, including telnet, ftp, gopher and the World Wide Web. Some information providers grant full unrestricted access to all the information contained on their servers, and use control simply to comport with physical limitations of their servers (*e.g.*, to limit the number of concurrent users). Other information providers restrict access to users with accounts or grant only limited access to unregistered users. For example, using ftp a user can often log on to a remote server through the Internet as an "anonymous" user (*e.g.*, a user for which no account has been created in advance); however, such a user will normally only be able to access specific data on the server. Of course, an information provider can elect not to provide uncontrolled access, and permit only those with pre-established accounts to access the server. This is more common with commercially-oriented on-line service providers. Control over access to a server containing protected works will typically be the first level of protection a content provider will look for before making their protected works accessible through the server.

A second level for controlling access to and use of protected works can be exerted through control measures tied to the electronic file containing the work.

Restrictions on access at the file level can be implemented using features in "rendering" software. For example, a content provider may develop specialized software products or implement features in general purpose software products that would control by whom, and to what degree, a protected work may be used. Such restrictions could be implemented using features in the rendering software, a unique file format or features in an established file format, or a combination of both. "Control" measures could also be implemented to determine if the content provider had authorized certain uses of the work, as well as some means to control the degree to which a user would be able to subsequently "manipulate" the work. For example, the rendering software could preclude a user who had not obtained the appropriate authority from the content provider or who enters an unauthorized or expired password from using the data. Rendering software can also be written to deny general access to the work if the file containing the work is not a properly authenticated copy (*e.g.*, the file has been altered from the version as distributed by the content provider). Such features will be possible provided that sufficient information regarding authorized use can be associated with the file containing the information product (*e.g.*, through inclusion in a file header, packaged and sealed in an "electronic envelope" sealed with a digital signature, embedded through steganographic means,[508] etc.).[509]

2. ENCRYPTION

In its most basic form, encryption amounts to a "scrambling" of data using mathematical principles that can be followed in reverse to "unscramble" the data. File encryption thus simply converts a file from a manipulable file format (*e.g.*, a word processor document or a picture file that can be opened or viewed with appropriate software) to a scrambled format.[510] Authorization in the form of possession of an appropriate "key" is required to "decrypt" the file and restore it to its manipulable format.

[508] *See* discussion of stenography *infra* pp. 188-89.

[509] For example, the software may deny access to a work if the electronic file containing the work has been altered or information stored in the file does not match data supplied by a user necessary to open and use the file. *See* discussion of digital signatures *infra* pp. 187-88.

[510] Rendering or viewing software may integrate encryption and file manipulation into a single software package. In other words, the rendering software, after getting a password, will decode the file and permit the user to manipulate the work (*e.g.*, view it or listen to it), but only with the provided rendering software.

Encryption techniques use "keys" to control access to data that has been "encrypted." Encryption keys are actually strings of alphanumeric digits that are plugged into a mathematical algorithm and used to scramble data using that algorithm. Scrambling means that the original sequence of binary digits (*i.e.*, the 1s and 0s that make up a digital file) that constitute the information object is transformed using a mathematical algorithm into a new sequence of binary digits (*i.e.*, a new string of 1s and 0s). The result is a new sequence of digital data that represents the "encrypted" work.[511] Anyone with the key can decrypt the work by plugging it into a program that applies the mathematical algorithm in reverse to yield the original sequence of binary digits that comprise the file. Although most commonly thought of as a tool for protecting works transmitted via computer networks, encryption can be and is used with virtually all information delivery technologies, including telephone, satellite and cable communications. Of course, once the work is decrypted by someone with the key, there may be no technological protection for the work if it is stored and subsequently redistributed in its "decrypted" or original format.

A widely publicized technique for sending secure transmissions of data is "public key" encryption. This technique can be used to encrypt data using an algorithm requiring *two* particular keys -- a "public" key and a "private" key. The two keys are affiliated with the recipient to which the information is to be sent. The "public" key is distributed publicly, while the private key is kept secret by recipient. Data encrypted using a person's public key can only be decrypted using that person's secret, private key. For instance, a copyright owner could encrypt a work using the public key of the intended recipient. Once the recipient receives the encrypted transmission, he could then use his private key to decrypt that transmission. No secret (private)

[511] An algorithm is a set of logical rules or mathematical specification of a process which may be implemented in a computer.

keys need to be exchanged in this transaction. Without the private key of the intended recipient, the work cannot be read, manipulated or otherwise deciphered by other parties. Of course, if a decrypted copy is made and shared, then others could manipulate the work unless other means are used to protect it.

There may be instances where someone other than the communicating parties needs access to the encrypted data. A key escrow system is one way such access might be obtained. A key escrow system would hold the key needed to decrypt an encrypted transmission in "escrow." Such a system could be maintained by a private organization or the government, and anyone seeking access to an encrypted transmission would have to demonstrate their need for the key through a process, such as obtaining a search warrant, that ensures the legitimate privacy and security needs of users of encrypted transmissions.

3. DIGITAL SIGNATURES

Mathematical algorithms can also be used to create digital "signatures" that, in effect, place a "seal" on a digitally represented work. Generating a digital signature is referred to as "signing" the work. The algorithms can be implemented through software or hardware, or both. The digital signature serves as means for authenticating the work, both as to the identity of the entity that authenticated or "signed" it and as to the contents of the file that encodes the information that constitutes the work. Thus, by using digital signatures one will be able to identify from whom a particular file originated as well as verify that the contents of that file have not been altered from the contents as originally distributed.

A digital signature is a unique sequence of digits that is computed based on (1) the work being protected, (2) the digital signature algorithm being used, and (3) the key used in digital signature generation.[512] Generating a digital signature uses cryptographic techniques, but is not encryption of the work; the work may remain unencrypted so it can be accessed and used without decryption. In fact, digital signatures and encryption can be used simultaneously to protect works. Generally, a signature is computed for a copyrighted work first and then the work (including the seal) is encrypted. When the work is to be used, the work is decrypted, then the signature (*i.e.*, the seal) is verified to be sure the work has not been modified (either in its original or encrypted form). If the work is never changed, the seal need never be removed or changed. If the work is changed, a new seal must be computed on the revised information.

Typically, the digital signature is incorporated in some manner in the transmission that constitutes the work. Often, the sender will also distribute his public key as well. The signature serves as a "seal" for the work because the seal enables the information to be independently checked for unauthorized modification.[513] If the seal is verified (independently computed signature matches the original signature), then the work is a bona fide copy of the original work -- *i.e.*, nothing has been changed in the file that constitutes the work.

4. STEGANOGRAPHY

Innovative new techniques are being developed to address security or management driven concerns relating to dissemination and use of digitally-encoded information.

[512] The signature is generated using the binary digits of the work plus the value of the private key as inputs to the computation defined by the algorithm. Thus, the digital signature for an information object is a unique sequence of digits for that work. Specifically, a signature is not the same for different works using the same private key.

[513] Anyone who has access to an information object, in addition to having access to the work, also has access to the digital signature for the object. Consequently, the digital signature for the object may be recomputed and used to independently confirm the integrity of the object by comparing it to the digital signature appended to the object.

For example, methods have been developed that can encode digitized information with attributes that cannot be disassociated from the file that contains that information. This field of technology has been termed "steganography" and been conceptually referred to as "digital fingerprinting" or "digital watermarking."

In essence, using steganographic techniques, a party can embed hidden messages in digitized visual or audio data. The embedded information does not degrade or otherwise interfere with the audio or visual quality of the work. Instead, the embedded information can only be detected if specifically sought out. More advanced steganographic techniques based on statistical or entropically-directed encoding are proving to be difficult to defeat. For example, one system modulates a known noise signal with the information to be embedded and adds the "scaled" signal to the original data. Once encoded in this fashion, the steganographically encoded identification data is distributed throughout the work as subliminal noise and, like noise, cannot be fully eliminated from the work. Thus, one can ensure detection of an embedded message even after substantial corruption of the data, such as might occur through compression/decompression, encoding, alteration or excerpting of the original data. By providing a means to indelibly tag a work with specific information, steganography is likely to play a complementary role to encryption as well as authentication techniques based on digital signatures.

D. CONTROLLING USE OF PROTECTED WORKS

Content providers will rely on a variety of technologies, based in software and hardware, to protect them against unauthorized uses of their information products and services.

One example can be found in the Audio Home Recording Act. This Act requires that manufacturers of digital audio recording devices and digital audio interface devices incorporate features that limit serial copying.[514] The hardware is programmed to read certain coding information contained in the "digital subcode channel" of digital sound recordings and broadcasts. Based on the information it reads, the hardware circuitry will permit unrestricted copying, permit copying but label the copies it makes with codes to restrict further copying, or disallow copying. The serial copy management system allows unlimited first generation copying -- digital reproduction of originals (such as CDs distributed by record companies), but prevents further digital copying from those reproductions.[515]

Similar systems can be implemented through hardware, software or both, using the concepts discussed above (*e.g.*, rendering software and encryption technology). For example, files containing works can include instructions used solely to govern or control distribution of the work. This information might be placed in the "header" section of a file[516] or another part of the file. In conjunction with receiving hardware or software, the information, whether in the header or elsewhere, can be used to limit what can be done with the original or a copy of the file containing the work. It can limit the use of the file to view- or listen-only. It can also limit the number of times the work can be retrieved, opened, duplicated or printed.

[514] *See* 17 U.S.C. § 1002 (Supp. V 1993).

[515] *See* H.R. REP. NO. 102-873(I), 102d Cong., 2d Sess., *reprinted in* 1992 U.S.C.C.A.N. 3578, 3579-80, 3583 n15.

[516] A "header" is a section of a digital work where information, data, codes and permitted uses may be embedded. Such information may actually be embedded anywhere in the work, but for ease of reference, this Report refers to such information as embedded in a header. Terms such as "label" and "wrapper" are also used to refer to what this Report refers to as a "header."

E. MANAGING RIGHTS IN PROTECTED WORKS

Systems for managing rights in works are being contemplated in the development of the NII. These systems will serve the functions of tracking and monitoring uses of copyrighted works as well as licensing of rights and indicating attribution, creation and ownership interests. A combination of file- and system-based access controls using encryption technologies, digital signatures and steganography are, and will continue to be, employed by owners of works to address copyright management concerns. Such security measures must be carefully designed and implemented to ensure that they not only effectively protect the owner's interests in the works but also do not unduly burden use of the work by consumers or compromise their privacy. And measures should be studied to ensure that systems established to serve these functions are not readily defeated.

To implement these rights management functions, information will likely be included in digital versions of a work (*i.e.*, copyright management information) to inform the user about the authorship and ownership of a work (*e.g.*, attribution information) as well as to indicate authorized uses of the work (*e.g.*, permitted use information). For instance, information may be included in an "electronic envelope" containing a work that provides information regarding authorship, copyright ownership, date of creation or last modification, and terms and conditions of authorized uses. As measures for this purpose become incorporated at lower levels (*e.g.*, at the operating system level), such information may become a fundamental component of a file or information object.

Once information such as this is affiliated with a particular information object (*e.g.*, data constituting the work) and readily accessible, users will be able to easily address questions over licensing and use of the work. For example, systems for electronic licensing may be developed based on the attribution or permitted use information associated with an information object. Electronic contracts may be used.[517] Providers may inform the user that a certain action -- the entering of a password, for instance, to gain access to the service or a particular work, or merely the use of the service -- will be considered acceptance of the specified terms and conditions of the electronic license.

The Library of Congress' Electronic Copyright Management System may be instrumental in rights management schemes. The proposed system, which is under development, has three distinct components: (1) a registration and recordation system, (2) a digital library system with affiliated repositories of copyrighted works, and (3) a rights management system.[518] The system will serve as a testbed to gain experience with the technology, identify issues, prototype appropriate standards, and serve as a working prototype if full deployment is pursued later.

An important element of doing business in the digital environment will be the ability to move money from users to the providers of the various information and entertainment products and services.[519] Presently,

[517] *See* discussion of electronic contracting *supra* pp. 53-59.

[518] *See* R.E. Kahn, *Deposit, Registration and Recordation in an Electronic Copyright Management System*, Proceedings of Technical Strategies for Protecting Intellectual Property in the Networked Multimedia Environment, Interactive Multimedia Assoc. (Jan. 1994). The registration and recordation system will be operated by the Library of Congress and will enable electronic filing of documents, automated registration and recordation of transfers of ownership and other copyright-related documents. The digital library system will be composed of a set of distributed repositories for copyrighted works, and will support search and retrieval based upon an electronic bibliographic record. The rights management system will be a distributed system which will permit use of selected copyrighted materials on the Internet, and will have some on-line rights-granting services. Electronic mail will be used to license nonexclusive rights, with or without recordation of the transactions.

[519] The IITF Committee on Applications and Technology is addressing electronic commerce issues, including the electronic transfer of funds through the NII.

transactions follow models wherein the actual assets do not move in the system, but rather only representations of the assets. That is to say, if a consumer selects a pay-for-view motion picture from a cable service provider, the consumer gives the service provider a credit card number. The service provider sends the credit information to a clearinghouse where it is verified and sent on to a bank for payment. Such methods of payment are relatively expensive because of the number of players and transactions involved.

Some believe that a more efficient and cheaper method of payment is "digital cash." Using a digital cash system, actual assets are transferred through digital communications means in the form of individually identified representations of bills and coins -- similar to serial numbers on hard currency. There are a number of systems being developed to accomplish such money movement, which should allow consumers to move actual assets through the NII or GII, rather than simply transferring a message to other existing systems to move the money for a transaction.

One payment system relies on the existing credit and debit card and banking systems. It avoids transaction costs by simply accumulating users' transactions and charging their debit card or billing the accumulated charges to their credit card once in a fixed time period, depending on volume and the cumulative amount of charges. However, the use of the third party bank for verification and collection adds cost to the transactions. In addition, the anonymity of cash purchases is lost, and there is an increased risk that transactions may be monitored by organizations that track spending habits of consumers.

A more complex system uses “smart cards” and public key encryption to move actual assets within the system. Such systems are common in Europe, for instance, for public transportation and telephone charges. Under such systems, a pre-paid card with a programmed amount of value or "cash" is issued to a consumer, and the card's account is debited when it is used for a purchase. Such systems protect anonymity because debiting of the card does not require the consumer to reveal her identity; it is legal tender just like cash. Such systems for use in the NII and GII are under development by both European and U.S. firms.

F. ENCRYPTION EXPORT CONTROL

U.S. manufacturers are currently prevented from exporting software and hardware with certain types of encryption technology.[520] This is due to an export licensing system developed over the last 50 years in order to limit proliferation of encryption technology that could hinder efficient intelligence gathering and effective law enforcement. U.S. software manufacturers that produce "mass market" products indicate that there is a significant demand internationally for software products with strong encryption capabilities. They believe that their inability to deliver such products is leading to the development and sale of these needed products by foreign software developers. Relaxation of export controls would permit U.S. businesses to compete with foreign companies that presently incorporate strong encryption technology in their products, but would make it even more difficult for the United States and its allies to fight international terrorism, narcotic trafficking, corruption, smuggling of nuclear materials, and other criminal activities.

Export controls are administered through a bifurcated system in the United States. The nature of the technology, product or information to be exported dictates the Agency

[520] There is an ongoing review of policies governing the export of computer and networking technologies that incorporate effective encryption technology, and there has been some relaxation of prior controls. For example, technologies used to identify and authenticate users and files are generally not restricted. This, however, does not address the concerns as articulated by U.S. manufacturers.

from which the party wishing to export must turn to obtain a license to export.

- Export licensing of arms, ammunition, and implements of war is handled by the Office of Defense Trade Controls (ODTC) of the Department of State pursuant to the Arms Export Control Act.[521]

- Export licensing of items not exclusively controlled for export by another Department or agency of the Federal Government is handled by the Bureau of Export Administration (BXA) of the Department of Commerce.[522]

When a party wishes to export products containing an encryption technology, a Commodity Jurisdiction (CJ) Ruling is made that determines whether the item is on the Munitions List or the Commerce Control List (CCL). If the item is determined to be on the Munitions list, the State Department reviews the request for an export license. Conversely, if the item is found to be on the CCL, then it is assigned an Export Control Classification Number (ECCN) which is used to determine the requirements for its export licensing.[523] The Commerce Department has exclusive statutory jurisdiction over licensing of CCL items, and in practice presents a less stringent licensing scheme than for munitions items.

Development of an optimal NII and GII requires strong security as well as strong intellectual property rights.

[521] ODTC maintains the U.S. Munitions List -- a list of specific technologies subject to their review for export licensing purposes. *See* 22 U.S.C. § 2778 (1988).

[522] BXA maintains the Commerce Control List (CCL), which governs export control of all items (commodities, software, and technical data) subject to BXA export controls. *See* 15 C.F.R. § 799.1(a) (1994).

[523] *See* 15 C.F.R. § 799.1(g) (1994).

Copyright owners will not use the NII or GII unless they can be assured of strict security to protect against piracy. Therefore, encryption technology is vital because it gives copyright owners an additional degree of protection against misappropriation.

Encryption is equally important to other users of the NII and GII as well. Industries that transmit sensitive information -- either internally or to other businesses -- also require high levels of security. Banks, accounting firms, and securities houses are prime examples of businesses that routinely transmit sensitive transactional information. In addition, absent strong encryption, medical and legal professionals using the NII may have difficulty reassuring their clients that sensitive personal information will not be compromised.

The growth of the NII and GII is sparking increased international demand for encryption technology. However, for national security reasons, the United States strictly controls the export of many encryption products for sale abroad. This policy protects vital U.S. national security and law enforcement interests, but critics contend that it is slowing the spread of encryption technologies that could be used to protect intellectual property transmitted through the NII and GII and causing U.S. manufacturers to lose sales to foreign competitors who are not constrained by U.S. export controls. To evaluate these complaints, the Clinton Administration has directed the Commerce Department, through the newly created Office of Strategic Industries and Economic Security, to conduct studies on the export controls of encrypted software and their impact on U.S. manufacturers -- which were expected to be completed by July 1995.

Recognizing the important role that encryption technology plays in fostering a secure and useful NII, the Working Group supports efforts to work with industry on key-escrow encryption technologies and other encryption products which could be exported without compromising

U.S. intelligence gathering and law enforcement. The Working Group believes that proliferation of such technology will enable U.S. industry to meet the needs of the international market for these products and continue to lead the development of the GII.

G. DEVELOPMENT OF STANDARDS

A common concern related to development of the NII is the development of standards. Obviously, some level of interconnection, interoperability and standardization of telecommunications, computer, wireless, satellite, broadcast and cable television technologies and networks will be needed to achieve the full potential of the NII. The need for standards, however, does not suggest that any one entity must be established to develop and implement a comprehensive suite of standards. Rather, consistent with historical trends firmly established in the computer industry, the marketplace will develop the best suite of standards to make the NII viable.

The computer industry tends to follow certain general trends in the development and implementation of solutions to commonly encountered problems.[524] The most common

[524] Many examples of this evolutionary pattern exist. Examples of *de facto* and formally recognized standards that derived from a single company include the Hayes-compatible modem command set, developed by the Hayes Company to control its modem products; the Ethernet local area network standard developed by Xerox to link minicomputers at the Palo Alto Research Center which eventually led to the development of the IEEE 802.3 standard; and the PCL and Postscript printer control/page description languages, developed by Hewlett-Packard and Adobe, respectively.

Examples of standards that evolved from a collaboration of companies include: the Extended Industry Standard Architecture (EISA) bus standard, introduced by a consortium of nine companies including AST Research, Compaq, Epson, Hewlett-Packard, NEC, Olivetti, Tandy, Wyse, and Zenith; the Musical Instrument Digital Interface (MIDI) interface standard for the connection of synthesizers, instruments, and computers, developed by the major synthesizer manufacturers; and the Personal Computer Memory Card International Association (PCMCIA) standard for PC Cards, PC Card-based peripherals, and the slot designed to accept them developed by the PCMCIA group of manufacturers and vendors.

trend is for an "early implementer" to develop a "point-to-point" solution to a specific problem (*e.g.*, a solution which solves the problem solely from the perspective of that developer's needs). Alternatively, a consortium of companies will work together to jointly develop a solution to address the problem. Depending on the frequency of the problem, other individual companies or consortia will develop different solutions to the problem. Over time, one solution will begin to emerge as a *de facto* industry standard. It may gain that status through consumer or user preference, through effective promotion by one company or a consortium of companies, or, more typically, a combination of both. Once it appears that an industry consensus is emerging, efforts begin to convert that *de facto* standard into a more formally recognized industry standard. This can occur through accreditation efforts sponsored by private organizations, such as the American National Standards Institute (ANSI) or the Institute for Electrical and Electronic Engineers (IEEE); through domestic governmental standard setting organizations, such as the National Institute for Standards and Technology (NIST), the Department of Energy (DOE) or the Department of Defense (DOD); or through international organizations like the International Telecommunication Union. As these *de facto* standards become established, either informally or formally, vendors and systems providers incorporate these standards into their products or make those products compatible with those standards. Once established, the standards tend to evolve to accommodate improvements using the standard setting organizations. Eventually, many standards are implemented at the operating system level.[525]

Understanding this common progression is important in understanding how the NII will likely develop. At this point in time, many different solutions are being developed

[525] For example, essentially every modern personal computer operating system available today supports a number of *de facto* or recognized industry standards such as Ethernet, PCL/Postscript, and TCP/IP.

to address the needs of users, content providers, service providers and carriers. Most of these developments fall into the class of point-to-point solutions to serve specific needs. As these early systems lead to development of standards, the various industries supporting the NII's development will formally or informally establish *de facto* and formally recognized standards. Once standards begin to emerge or become established, the major operating systems developers will incorporate or support them at the operating system level. Thus, solutions developed to address the needs and concerns of users, content providers, service providers and carriers will evolve and become integrated into the infrastructure of the NII.

Over time, point-to-point solutions will become established as standards and/or incorporated into operating systems. When this happens, uniform means for identifying the author of a work, authenticating the contents of an information object, ensuring the secure transmission of information objects between remote sites, and authorizing subsequent use of information objects after the first transfer, will be possible. At this point, however, given the nascent state of the NII, it would be inappropriate to suggest that a comprehensive system could best be devised from a central planning perspective.

Interoperability and interconnectivity of networks, systems, services and products operating within the NII will enhance its development and success. Standardization of copyright management (standardized header information and format, for instance), as well as technological protection methods (such as encryption), may also be useful. The question of whether any standards should be established, either through government regulation or industry consensus, however, is not within the purview of this Working Group. The issue of what those standards should be, if established, is similarly outside the scope of the area of inquiry of the Working Group.[526] If a standard is established, however, protection of intellectual property rights used in that standard is of concern to this Group.

The intellectual property rights implications of the standards-setting process are not new with the development of the NII. The Federal Communications Commission, for instance, has established standards in related areas without interfering with the legitimate rights of intellectual property rights owners.[527]

The Working Group finds that in the case of standards to be established, by the government or the private sector, the owner of any intellectual property rights involved must be able to decline to have its property used in the standard, if such use would result in the unauthorized exercise of those rights. If the rights holder wishes to have its intellectual property as part of the standard, an agreement to license the necessary rights on a nondiscriminatory basis and on reasonable terms may be required. In the case of *de facto* standards, arising out of market domination by an intellectual property rights holder, the antitrust laws may provide a remedy for anticompetitive uses of the standards.

[526] The IITF Committee on Applications and Technology has responsibility for addressing the issue of standards.

[527] Recently, the FCC adopted technical standards that define a patented system as the AM radio stereophonic transmitting standard in the United States. *See* 58 Fed. Reg. 66,300 (daily ed. Dec. 20, 1993). The FCC conditioned the selection of the patented system as the standard on the agreement of the patent owner to license its patents to other parties "under fair and reasonable terms." *Id.* at 66,301.