Cross-Industry
Working Team

Managing Access to Digital Information:

An Approach Based on Digital Objects and Stated Operations

May 1997

3Com
Alcatel Telecom
American Management Systems
Apple Computer
AT&T
BBN
Bell Atlantic
Bellcore
BellSouth
Cisco
Citicorp
Compaq
Corning
CyberCash
Digital Equipment
EarthLink Network
Electric Power Research Institute
Ericsson
Fujitsu
GTE Laboratories
Hewlett-Packard
Houston Associates
Hughes Network Systems
IBM
Intel
InterTrust
Lucent Technologies
MCI Communications
Motorola
NEC USA
New York Times
NIST
Nortel (Northern Telecom)
Novell
Philips Research Briarcliff
Prodigy Services
QuantumLink
Science Applications International Corporation
Silicon Graphics
Southwestern Bell
Sprint
Sun Microsystems
Texas Instruments
USWest
West Group

XIWT

The Cross-Industry Working Team (*XIWT*), is a membership organization consisting of a diverse group of communications, computer system, information and service providers who have joined together to develop a common technical vision for the National Information Infrastructure (NII).

Among our activities, *XIWT* publishes White Papers intended to improve the quality and accelerate the evolution of the NII by establishing common understanding about technical issues among those involved with its development and use. White Papers will evolve along with our understanding and be reissued from time to time. Subsequent papers will delve more deeply into many of the issues identified herein.

XIWT activities have a technical focus, and may have broader implications. Hence we expect this series of papers will be of interest to policy makers, to others contemplating activity in the NII, and to the general public, and we invite comment and suggestions.

To obtain reports or for more information about *XIWT*, please contact:

Cross-Industry Working Team
Corporation For National Research Initiatives
1895 Preston White Drive, Suite 100
Reston, Virginia 20191-5434

Tel: 703-620-8990 Fax: 703-620-0913
Email: info-xiwt@cnri.reston.va.us
Web: http://www.xiwt.org

Charles N. Brownstein, Executive Director
Email: cbrownst@cnri.reston.va.us

Ira Richer, Director, Networking Research
Email: richer@cnri.reston.va.us

Pamela Memmott, Member Services Coordinator
Email: pmemmott@cnri.reston.va.us

Stephanie Kim, Secretary
Email: skim@cnri.reston.va.us

Cross-Industry
Working Team

Managing Access to Digital Information:

An Approach Based on Digital Objects and Stated Operations

Contents

1.0 Introduction

The deployment and widespread use of global information systems like the Internet may dramatically reduce the production and distribution costs usually associated with information dissemination. With digital technology, anyone can become an information provider, able to generate and distribute ideas at little or no cost. This technology facilitates dynamic and efficient forms of creativity or innovation, such as the integration of various digital materials to manifest sounds, images, graphics, or industrial designs – all linked in interesting, innovative, or entertaining ways. It offers wider, more dynamic forms of collaboration. For example, works of literature, music, or art converted to digital form, or initially expressed in some digital format, can now be worked on by large numbers of collaborators separated by time and space. New Works can be produced in record time; and scientific theories or problems can be proposed, decomposed, simulated, and worked on in parallel almost in real time by researchers around the world.

In the past, there was a relative shortage of creative work. A network environment may change this situation. In an open, accessible computer network environment, even the smallest voice can be widely heard. The result will be new dynamics for the economics of content production and distribution. Without the ability to control access to information in a network environment, however, intellectual property may have little value.

Although the future "networked digital world" holds promise for greater societal good, it presents new challenges with respect to existing legal systems. Information expressed in various digital formats is easy to reproduce, perform, and disseminate with nearly perfect accuracy at low cost. Digital information can be made immediately accessible to everyone without regard to location. Further, information technology allows for more interactivity. Links between works can be dynamically made and broken; and composite objects and works can be rapidly composed, nested, and/or transformed almost effortlessly (except for the intellectual energy expended).

Many laws apply to digital information, including the laws of copyright, patent, trademark, libel, slander, defamation, contract, and communications – not to mention the First Amendment to the U.S. Constitution. While copyright, patent, trademark, and communications laws are among the more important bodies of law in this context, there will also be

instances where legal provisions in such areas as contracts, taxes, securities, banking, insurance, and trade arrangements come into play. Legal provisions often interact, and, occasionally, overlap or even conflict in practice. Storing, manipulating, accessing, and distributing digital objects and other digital resources, and executing new types of operations on digital material, bring to bear a wide variety of laws and regulations. Thus, while it is important to understand the implications of each of these legal systems individually, as a matter of public policy, it is necessary to consider the combined effects of the various elements in light of new technological developments.

Emerging technical capabilities – especially efforts to develop data structures for use in a digital environment – may, in fact, advance public understanding of the relevant legal implications. Thus, for example, business models are being developed around the concept of a "container" or "package" that may embody digital information subject to various rights or interests or that, when processed, may manifest such "content." ln this paper, we refer to such data structures as **digital objects**. Conceptually, a digital object is a logical entity or data structure whose two principal components are digital material ("data"), plus a unique identifier for the material and other information pertaining to the data ("metadata").

Emerging cryptographic and agent-based technologies may make it easier to manage rights such as copyright by (1) providing more effective enforcement through cryptography, secure hashing/digital fingerprints, and certificates; (2) facilitating more efficient payment through digital cash and micropayments; and (3) providing efficient means for monitoring and detecting infringements through the use of intelligent agents. Cryptography can be used to give each digital object a unique digital signature; combined with steganographic technology, it can be used to imbed hidden or invisible markings or fingerprints. These digital object fingerprints then can be used to test for authenticity. This technology enables digital marks and digital signatures to be placed on digital objects in such away that they cannot be copied or removed without detection. When misapplied, however, these technologies may discourage and inhibit the very sharing and cross-fertilization they are meant to encourage.

These developments do not diminish the importance of intellectual property protection. ln fact, there is a growing need to encourage new forms of authorship or discovery that do not just replicate or mirror old

forms, but that reconceptualize what it means to be a creative work or invention. It is important, however, not to lose sight of the cost factors associated with the creative process. While much new information may now be made accessible in a network environment, it may actually offer little in the way of real creativity, inventiveness – or even interest. It will be increasingly important to find ways to reward those who add significant value to the store of human knowledge, who entertain, or who collect and disseminate information, and to encourage them to share their work widely with others.

This paper addresses various issues surrounding the management of rights and permissions in the digital environment. It introduces, in particular, the notion of digital objects (sometimes referred to as packages, containers, or structured bit sequences) and their supporting technologies as a means of enabling new business opportunities and protecting intellectual property in a computer network environment.

2.0 Digital Objects

Digital objects provide a means of organizing and identifying "content" – i.e., underlying data – for purposes of storage, access, or distribution. A digital object is not merely an unstructured sequence of bits or symbols from an alphabet. Rather, it has a structure that allows it to be identified and its content to be organized and protected, as appropriate. As described by Kahn and Wilensky (1995), a digital object may incorporate (or be interpreted to manifest) not only the content, but also the unique identifier of the digital object and other metadata about the digital object and its content. The metadata may include restrictions on access to digital objects, notices of ownership, and licensing agreements relating to underlying content.

A digital object may also be viewed as information in its own right, with its own intrinsic rules and procedures, and may itself be packaged in other digital objects. The packaging of a digital object within another may occur, for example, where agent software is charged with accessing information on behalf of a user, or collecting and organizing information that it presents to a user. Digital objects may be stored in repositories which, in turn, may be structured as digital objects – i.e., logical entities containing multiple digital objects.

The notion of a digital object as a container that incorporates protected information may facilitate the development of flexible and efficient mechanisms for managing rights and interests in protected information within a network environment. There will probably be at least two different categories of digital objects – those that come with meaningful restrictions and those that do not. Many commercial digital objects may come without any meaningful restrictions; others may be heavily encumbered.

Defining a digital object infrastructure allows business models to be developed that can be based on communications law and other bodies of law. It is anticipated that these legal systems will provide an adequate basis for managing access to digital objects in order to perform "stated operations" and provide related services.

2.1 Agents as Digital Objects

Software agents are a particularly interesting technology for managing rights and executing tasks in the network environment. When configured as digital objects, they may act on behalf of rights-holders to protect works embodied in such objects, and they may interact with other agents and systems to carry out a wide range of tasks in the networked digital world.

Briefly, software agents are computer programs that may be mobile in a network environment and can act as intermediaries providing information about rights and permissions. Agents can be used to control the distribution of material, discover infringements of rights and interests in intellectual property, and negotiate licenses in a network environment. They can be more than mere transport mechanisms for connection purposes. For example, they can also combine, filter, index, rearrange, interpret, and transform digital information. They could serve as a researcher's assistant – reading the works of others, and then rearranging and reinterpreting them, rather than merely reporting and regurgitating the works verbatim.

2.2 Some Issues for Further Exploration

A variety of questions arise with respect to digital objects and their contents in a network environment. These fall into four general categories – incentive issues, legal issues, business issues, and technology issues. A sampling of the key questions within each of these categories follows.

2.2.1 Incentive Issues

There are several questions that need to be addressed to make sure that producers, consumers, and network service providers are comfortable with this new means of information access. As Esther Dyson notes: "... everybody can get up on the Net, sing their own songs, write their own poetry. You no longer need a publishing house to get a book published. So economics would say that since the supply of content is increasing, the costs of duplication and distribution are diminishing and people have the same amount of time or less, we are all going to pay less" (Dreifus 1996). Of particular concern is the extent to which a balance is struck between intellectual property protection and the needs of users to work effectively in this environment. Some issues that may arise in this context include the following:

1. Will network users be able to browse information contained in digital objects (or that may be manifest when such objects are processed) as easily as readers have been able to peruse books at their favorite bookstore?

2. How will network users be able to "borrow" or otherwise use digital objects stored in repositories? Will there be restrictions on who may access such information?

3. Will authors and other information providers be vulnerable to the loss of significant potential royalties on their works as millions of network users armed with these new capabilities manipulate, disseminate, and interact with their works; or will a digital object infrastructure promote the development of a valuable new market for their information?

4. How will broadcast, cable television, satellite, and other conventional audio and video programming services be integrated in or associated with digital object information services?

2.2.2 Legal Issues

Works and other material configured as digital objects may be produced collaboratively in new and novel ways – for instance, emulating how a motion picture production company handles the various contractual relationships with contributors. Such collaboration may lead to more democratic and effective interaction, e.g., shared learning and discovery,

with wider distribution of ideas, and fewer limitations and constraints on communication. Computer networks permit greater and more rapid access to ideas and contributions, and, when combined with new implementations of business rules and practices, may lead to new kinds of businesses and increased employment. The activity raises many questions, however. For example:

1. What constitutes a public performance for copyright purposes in a digital environment? Where digital objects are disseminated over a computer network, should this activity be covered by the copyright right of distribution; and, if so, what should be the scope of this right?

2. How should running a computer program with creative inputs be treated from an intellectual property perspective? Is it a public performance to execute a digital work (such as a video game computer program) that is structured as a digital object?

3. What if such a program is embedded in a compound digital object where its performance is made more popular in its new context?

4. When one contributor provides added value through overlays or the morphing of someone else's intellectual property, at what point in the processing chain does the original work cease to be identifiable, or become sufficiently watered down to bring its link to the final product into question? How will such collaborative efforts relate to current intellectual property law?

5. Should a digital object be treated like a television program for purposes of regulation under communications law? If so, is it necessary to broaden existing communications law concepts of unauthorized interception of a program-carrying signal and the divulgence or publication of its contents for communications law purposes to cover unauthorized access to perform stated operations on digital objects, including repositories structured as digital objects? What stated operations should normally require prior authorization?

6. What constitutes a protected process when providing access to digital objects? What does it mean to communicate a performance of a copyrighted work embodied in a digital object by means of a patented device or process, whereby a bit sequence is received beyond the place from which it was sent?

7. With respect to digital objects, how can we track who owns what and in what contexts? Does "ownership" of digital objects make sense? Would a focus on access to a digital object information service or repository be a flexible starting point in analyzing possible legal implications?

8. How can information owners be adequately compensated when their works are expressed in various digital formats that may be accessed, manipulated, interpreted, and aggregated where such works are configured as digital objects?

9. How should the concept of access to information be applied with regard to confidential and privileged information that has been structured as digital objects?

10. How is denial of service to be addressed? Is this sort of interference an infringement of intellectual property rights? Does this violate communications law or antitrust law? Should denial of service be disallowed and/or protected against?

Several technical solutions and new business models may be introduced that could enable some or all of these activities without sacrificing the interests of individual contributors or dampening their motivation or enthusiasm for sharing their knowledge with society.

2.2.3 Business Issues

Another set of issues arises when planning and implementing business models to develop packages of information in various digital formats. New forms of business will need to evolve in the networked digital world to support the use of digital objects and other digital resources. Some issues to be addressed in this context include the following:

1. How should digital objects and other similar digital resources be identified?

2. Will automated licensing mechanisms be developed within a network environment to facilitate access to digital objects and their contents?

3. What will be the range of services that repositories of digital objects may provide, and what are acceptable rules of procedure and other terms and conditions for accessing such repositories? Will third-party services such as indexing and archiving services arise to facilitate access to these repositories?

4. Will the information contained in a digital object influence the rules for accessing it in a repository; and, if so, how will this be handled in practice?

5. What will be the liability of a certifying authority when authenticating information resources structured as digital objects? ln the event that different repositories are subject to different regulatory environments, what impact will this have on security arrangements?

2.2.4 Technology Issues

Many aspects of technology could be selected for discussion here, but we focus instead only on those issues relating to agent technology. This technology represents one of the newest and, in many ways, most interesting and controversial areas of technology. Specific questions that arise in connection with intelligent agent technology include the following:

1. How does the use of agents structured as digital objects that operate on information affect intellectual property? Is the output from such an agent a new work? Where is the boundary, if any, between the old work and the new work?

2. Should such agents have rights? Under what circumstances may they negotiate licenses on behalf of users?

3. Are the agents themselves to be viewed as inventions with their own patent protection, trademarks, etc.? Are they also subject to copyright protection? How does, or should, communications law regulate their behavior?

4. How should highly intelligent agents, sometimes called knowledge-based systems, be treated from a legal and business perspective when they give advice that others resell? What are the issues associated with multiple nestings?

5. How should the transformation of one digital object into another be viewed from a rights perspective?

3.0 Key Infrastructure Requirements

Commercial rights management technologies typically require one or more infrastructure services. Usually, these services involve repository management, data processing, or similar capabilities. Some entail the provision of gateways between the rights management technologies and various general infrastructure services such as financial clearinghouses. Following are descriptions of key infrastructure components of an open architecture that supports digital objects.

- **Persistent unique identifiers –** Digital objects and other digital resources need unique identifiers that can potentially last indefinitely. ln fact, a key characteristic of a digital object is the presence of a unique persistent identifier in its metadata. Multiple identification schemes may be desirable in certain circumstances; however, there should be some widely understood methods for resolving these identifiers to permit access to information regardless of the source of the identification scheme. This is particularly important where digital object technologies used in rights management need to interact and collaborate.

- **Global resolution system –** A widely recognized global resolution system for identifiers will allow service providers to identify digital objects – even though based on competing technologies – as unique entities in information commerce. For example, a digital object protected using one technical approach may be located and retrieved by a software agent configured as a digital object using a different container technology. In this instance, the retrieved digital object may retain its original structure and unique identifier when incorporated in the second container for delivery to a customer.

- **Metadata standards –** Digital objects have associated metadata (such as “handles” that uniquely identify them) that may contain information regarding usage terms and restrictions, permissible operations, the sources and contributors of the underlying information components, the rights of each source, the kinds of permissions that must be updated, and how to obtain these rights. The metadata may also be used in negotiating special arrangements. For example, if a user wants additional rights beyond those stipulated in the metadata, there could be a link in the metadata to a person or entity identified as authorized to grant rights and permissions in order to negotiate an appropriate license. To ensure widest interpretation, however, metadata must be based on common standards.

- **Certificate authorities (CAs) –** The availability of certificate authorities is extremely important to the full development of efficient information commerce, especially regarding document management and security. Some companies offer to certify individual or organizational identities for purposes of given transactions. Others are willing to be the "root authority" for other certificate authorities. A central unresolved issue concerns possible liabilities a CA might incur. For example, if a CA certifies that a person is a patent attorney and he or she is not, and if that person harms an unsuspecting client, the CA may be held liable.

4.0 Potential Business Opportunities

New business models are likely to evolve to meet the needs of digital technology that may prove of great benefit to society. They may foster the spread of ideas, add value to existing information, provide new services, and generate revenue opportunities. While it is important to encourage these new business activities and their possible collateral value to rights-holders, there is a tradeoff between losing new potential business and value, and losing sources of revenue through information piracy. As Stefik (1996) notes. "the dream of universal digital access to high quality works dangles just beyond reach. Such works are not usually available, because of publishers' concerns that uncompensated copying will infringe and erode their ability to make a living."

To some extent, differing values are at issue here in determining the so-called public good – free speech, free exchange of ideas, profitability, cultural preservation, equal access, community values, to name but a few. There are bound to be conflicting values in all this, including different community values; technology, therefore, should be able to support not just one set of values, but be flexible enough to support different values in different circumstances.

Computer networking technology has the potential to provide all manner of new services, many not yet even imagined. These services may not intentionally violate the letter – or even the spirit – of intellectual property or other laws, but they may be perceived as doing so, leaving potential service providers with sufficient doubt or fear of liability that they will either not offer the service at all, or price it too dearly for it to be of much interest. Criteria should be developed that would permit a large

class of operations to be performed on digital objects and other digital resources without prior authorization. Similarly, other operations would be considered as requiring prior authorization under most, if not all, circumstances.

Many different pricing schemes may be implemented depending on the nature and scope of rights involved in any given context. A business model might rely on pricing for a dynamic digital object that is constantly updated and refreshed, and that can traverse myriad dynamically updated communications pathways, where each use generally will traverse a new path, often with new or updated information. Other business models might offer digital objects for free as an inducement for a customer to purchase hard copies (books, etc.) or to sign up for a more comprehensive service. Such digital objects may be regulated much like television programs today under communications law as well as, where appropriate, under patent and copyright laws. Focusing on the implementation of a digital object infrastructure from a communications law perspective may facilitate the evolution of rights management systems for any incorporated contents (Dunstan and Lyons 1994).

In this context, it may be helpful to have in mind an example of a type of business offering that could be provided today. Current technology enables vendors to provide some or all of the following services, several of which are now under development (Bock 1996; IBM infoMarket 1995; and Sibert et al. 1995):

- linking content providers to those who want content;
- providing content or content-related services;
- acting as a repository for digital objects;
- providing abstracts and indices;
- searching content;
- employing encryption and related techniques to manage rights and interests and to ensure the integrity of digital objects and their contents;
- delivering information on disks or CD-ROMs, or providing network access via e-mail, browsers, etc.;
- keeping information protected until the digital object is opened (e.g., in order to open an object, the user must contact a clearinghouse to handle the payment); and
- operating somewhat like a bookstore (e.g., understanding content, generating abstracts, and selling digital objects to the public).

5.0 Access to Digital Objects

To learn about a digital object's contents, or to interact with an object to obtain some service, the object's data must be processed. In this regard, "processing" refers to those operations that manipulate content and those that only act on the container. The latter may be considered as "content-free operations." Simple actions such as rendering – whereby a digital object is interpreted to manifest its contents – or identification – whereby a digital object is interrogated to determine its unique identifier rather than its contents – would both normally constitute processing. In the case of a simple digital object (i.e., one that does not contain other digital objects), however, only the latter action would typically be a content-free operation.

More complex actions might include those that deal with multiple digital objects such as those that access content to transform one object into another; or those that merely aggregate multiple digital objects into composite structures, but that do not actually access their contents. Again, both of these would normally constitute processing, but only the latter would typically be a content-free operation.

Many types of operations can be performed on digital objects. One way to categorize these operations is with an a priori listing of the various types. Another way is via a computer-interpretable language or set of languages that can be used to specify the operations or their types. A third way is via computer programs possibly contained within the digital objects themselves that can become active agents in negotiating rights and permissions for the objects and/or their underlying contents at various locations in a network environment. By delineating specific types of operations that may he performed on digital objects – that is, **stated operations** – a basis may emerge for orderly management of rights associated with digital objects and their contents. These stated operations may dictate the terms and conditions under which digital objects may be stored, accessed, manipulated, communicated, and otherwise shared.

In drawing up any such list, or in delineating types of operations more generally, care should be taken to avoid undue specificity at this early stage so as not to impede the development and potential of this new capability. Further, a simple listing of types of operations does not rule out more complex subsets of each type, as well as the composition of various types in interesting new ways. Through careful deliberation and

realistic experimentation, those categories of stated operations associated with digital objects that require prior authorization should be distinguished from those that do not. Many operations on digital objects – typically those of a commercial nature – appear to have overt effects on rights-holders. For example, operations on a digital object may be subject to specific terms and conditions in licensing agreements set forth in an object's metadata or elsewhere, or simply a requirement that appropriate attribution of authorship be given and that the integrity of the material be respected.

A consensus may emerge on the types of operations that should be permitted outright, or the conditions under which they would be permissible without prior authorization may be delineated. Efforts in this direction appear advisable. A few examples of categories of operations that may be performed on digital objects are given below. This list is necessarily incomplete, and its further development could benefit from additional study and experimentation.

- **Processing –** Normally, processing of a digital object so as to manifest its contents – i.e., to interpret a digital object for the purpose of using the underlying information in another system or communicating it by some means either directly or indirectly to another person – would not be considered a permissible operation without express authorization. It would also be impermissible if processing entailed deleting or otherwise rendering unintelligible the terms and conditions or other information associated with a given digital object; or deleting or destroying a stored digital object from a repository without authorization.
- **Distribution –** Distribution of a restricted digital object without authorization would usually not be considered a permitted operation. On the other hand, denying access to a digital object where there are no restrictions placed on operations that may be performed on the object and/or its underlying contents, e.g., inhibition of service via methods such as jamming servers or communications pathways, should be proscribed.
- **Replication –** This operation refers to the replication of digital objects for ease of use and/or reliability. Replication is often a critical system function that adds value and may not necessarily involve intentional violation of intellectual property rights.
- **Compression** – Many compression schemes, both lossless and lossy, are based on content. While the use of compression may offer value in some circumstances (such as lossless compression), it does not

necessarily result in an infringement of intellectual property rights. Indeed, in many cases, compression can actually increase the value of intellectual property by enhancing the ease, timeliness, and cost effectiveness of its distribution.

- **Packaging –** Many digital information services are not intended to access the contents of digital objects but merely to assist in packaging or repackaging them. Packaging techniques might include adding formatting information, encrypting information, moving information from one container to another, or reordering discrete digital objects contained within a given digital object. In many cases, there may be no natural order specified for the multiple components of a digital object, and the specific packaging choice may be at the option of the sender or the receiver (or both), provided that the contents are not otherwise changed.
- **Caching –** Another useful service is caching the information of others for local redistribution or sale. This may be especially appropriate for certain classes of digital objects, such as those that contain – or may be interpreted to manifest – information considered as digital money or registered bonds, where the object can only be transferred from one repository to another without alteration, and where only one original is deemed to exist logically in the system.
- **Carriage –** Intermediate carriers that provide point-to-point delivery based on the wishes of the originator and/or subscriber should be able to treat that operation much like traditional common carriage. Resale carriers, however, might have to be specifically recognized as such by law or regulation.
- **Aggregation and integration –** Aggregating and integrating streams of information coming from different sources provide too much value to be prohibited entirely, even though such operations make it more difficult to enforce rights. An example of such aggregation/integration is combining weather prediction data structured as one logical entity with another group's digital object embodying oil storage and distribution plans, and presenting the resulting digital material in a structured form over a geographical information system.
- **Clearinghouse services –** Certain activities of rights and financial clearinghouses may be candidates for exemption from liability under relevant laws. Rights clearinghouses, for example, perform several useful intermediary functions, including encouraging rights-holders to put digital objects into repositories and attracting a larger potential customer base. As for financial clearinghouses, commerce in information "goods" or "services" – like commerce in anything else –

requires secure, efficient, timely, and accurate clearing of financial transactions. Rights-holders and other value chain participants want assurance of payment or receipt, but typically do not want to manage a large number of financial interfaces with widely dispersed customers. At the same time, users want to be able to pay for information goods or services – in a variety of ways – via a common, trusted interface. The parties to a transaction also need to be able to verify that a given exchange has occurred as it was mutually intended, and to preclude repudiation of the transaction by either party.

- **Reference services –** The explosive growth and increased accessibility of information, ideas, and concepts creates a demand for more and better indices, catalogs, and contexts in which they can be placed. In a networked digital world, technology permits myriad indexing and cataloging schemes and contexts to be developed quickly and efficiently, as well as linked to a dynamically updated worldwide information mesh of digital objects and other digital resources. Libraries and similar information providers may furnish a variety of future information services, e.g., locating intelligence in the network; launching agents to perform research tasks; translating in multiple contexts; and providing security, authenticity and the building of network environments from disparate resources tailored to user needs. Some of these operations may be permitted without prior authorization. For example, cataloging and indexing digital objects for the purpose of delineating the collection for subsequent access may be permitted, while performing such actions for the purpose of describing the contents of a collection in substantial detail may not.
- **Brokerage services –** Organizations may wish to act as brokers for digital objects owned by others without authorization, provided that they do not make available the digital objects themselves. An example of such an offering might be the generation of digital objects called **meta-objects**, whose primary purpose is to provide references to other digital objects. Brokerage activities may require the use of minimal amounts of information from the digital objects, such as their names, titles, etc. Such services may be restricted.
- **Maintenance –** These services may require access to repositories of information for diagnostic or repair purposes. Any legitimate access to digital objects for such purposes, or for improving system availability, would likely be considered a permissible operation without authorization.

- **Authentication –** Authentication services may require access to the contents of digital objects for the purpose of watermarking, certification, and/or time stamping. Whether, and under what circumstances, such services are exempt from liability for their operations is an important area for discussion.

- **Transformation/browsing –** Transforming and browsing digital objects are two of several different kinds of processing actions that merit further discussion regarding permissibility. For example, transforming one digital object into another (i.e., morphing) may leave no perceptible trace of the former but still not yield an exact replica of the latter. To what extent is there a remnant of the former resident in the result? A related example involves the stripping out of selected portions of a digital object during some intermediate operation such as morphing. And what about searching and/or browsing some portion of a collection of digital objects for the purpose of locating a specific object or identifying material of interest – should this be considered similar to searching or browsing in a bookstore, where the full content is not actually digested?

Various other operations come to mind in a network environment such as reporting (via agents), traffic analysis or forecasting services that can reconcile various operations previously taken on digital objects or those involving specifications for billing and payment, and accessing the metadata of a digital object to determine the terms and conditions governing its contents.

6.0 Reflections on Rights Management Technologies

What should a rights-holder (reasonably) be required to do in order to protect his/her rights in a digital environment? If terms and conditions that cannot be removed or modified can be easily incorporated within a digital object's metadata, would a user be justified in presuming that the only constraints on access are those found in the metadata, and contact the owner only if he or she wants different terms and conditions? Should independent parties who add value to original works be permitted/required to add their own terms and conditions to the business rules and procedures in metadata as the modified/augmented works are passed down the value chain?

The most technically advanced rights management systems will most likely be delivered in a powerful, flexible, and efficiently protected manner which supports a digital object infrastructure that allows appliances and devices of all kinds large and small to participate in information commerce. A distributed rights management system is that collection of technologies and processes that can assist in determining and enforcing rights and interests and in ensuring the persistence and integrity of information. It may be comprised of a single system whose components are distributed, or a collection of systems that have well-defined and open interface standards. A digital object may itself be an active component in a rights management system, carrying along with it the terms and conditions for its access or enabling dynamic negotiation of rights and permissions. A list of some general business considerations and infrastructure requirements for distributed rights management appears in Appendix A.

A range of technologies are already deployed or will be in the marketplace shortly for digital rights management in the network environment. Several noteworthy examples of these technical capabilities are described in Appendix B. In one way or another, they all depend on protecting digital information mapped into analog signals (i.e., continuous waveforms) at different levels of granularity. Communication of digital information from storage media or over networks (and other pathways) requires detection of bits from analog signals. Further, in a digital world, bits may be encrypted in a wide variety of ways for storage or communication. Inherently, this distinction enables structured digital information to be distinguished as a logical entity from the waveform for purposes of rights management.

Rights management systems may make use of certain current and future enabling technologies – technologies that do not, as such, manage rights. Various technical approaches for rights management have been deployed; others are now under development. Two important technical approaches that should be addressed in a rights management context are discussed below.

6.1 Securing the "Pipe"

A basic rights management technique focuses on protecting the entire set of signals transmitted over a communication pathway between a user and a server. This, in effect, protects the entire interaction with an information source. It may be seen as directly protecting the "pipe" rather than the initial, ultimate, or any intermediate container or underlying content. Typically, an entire protected interaction (after some preliminary

exchanges) between an information provider and a customer would be encrypted or scrambled.

In an open environment such as the Internet, someone intercepting an encrypted signal may not easily access the unencrypted bit sequence, much less any incorporated digital objects or underlying content. This technique ensures a certain degree of confidentiality, so that unauthorized parties cannot necessarily determine any material aspect of the information interchange, such as which content was being provided. It also allows for a degree of security when passing credit card and other financial information. Once the signal is received by the customer, however, it will generally be decrypted and its underlying structure made available to the end user. Some of these structures, such as individual digital objects, may be in the clear or they may be separately encrypted.

6.2 Protected Containers

A protected container approach, on the other hand, emphasizes the individual package that incorporates information that may itself be encrypted or embedded in another container. A simple example would be the lock/unlock approach used by a publisher or other distributor that encrypts specific content for delivery – in encrypted form – to a customer. Lock/unlock systems typically include a financial clearinghouse service for processing payments; these may also report some usage information to rights-holders. Once the customer has paid for the digital information service, he or she can decrypt the content (by first getting a key or password).

Most encryption systems do not provide for ongoing control, metering, and billing capabilities; others provide these features by requiring the customer to run a dedicated application each time he or she uses a digital property. Thus, the information service is often not widely available for general use by typical PC applications. These services usually ensure that rights-holders are paid upon delivery, and sometimes on a pay-per-use basis.

A more sophisticated approach for providing protection is based on the idea that it is possible to create a data structure ("digital object") that allows portions of the structure to be identified and separately protected. As a general matter, any digital object may be protected through the use of encryption. A variety of different symmetric and asymmetric encryption systems can be employed, with each having a distinct role in protecting a digital object and/or its contents – or, in some cases, the rights management information delivered with the content. Such encryption

capabilities enable a more complex rights management approach, and raise the threshold for those who would attack a container. A container may hold unencrypted fields for titles, abstracts, thumbnails (abbreviated or low-resolution images), or any other information the provider may wish to present to the customer or potential customer. An application on the user's machine opens the container and makes the content available to the customer, sometimes only within the context of that application, or more generally (e.g., an Internet browser or agent software).

Some protected container systems are "clearinghouse-centric": they require a conversation with some central server in order to purchase and use the content. This model reflects a client-server orientation in which large central servers provide most of the important functionality to less capable client software. Rights management capabilities are typically limited to securing distribution and ensuring that rights-holders are paid for the use of information. In this scheme, a customer may be permitted to further distribute the protected container and its contents to any number of people, each of whom may contact the information distributor's clearinghouse to effect payment and purchase. Typically, the customer cannot modify any of the controls associated with the content, nor can permissions and prices not originally distributed with the content be efficiently obtained.

Other protected container technologies go beyond server-centric rights management models. These allow each enterprise in a value chain to contribute business rules under the control of more senior participants, thus enabling flexible implementation of the broadest range of business models. By enabling the creation of chains of title, these advanced rights and information commerce technologies enable both traditional business models and new, as-yet-undreamed-of models, to emerge in cyberspace (Bock l996; and Sibert et al. i995). These systems support the notion that consumers can act not only as peer-to-peer distributors, but that, if authorized, they can contribute their own business rules and procedures. This capability allows consumers of business, educational, entertainment, and other information resources to become value-added resellers.

A brief example demonstrates the point. A scientist at a for-profit research company writes a long review article, and packages it in a secure container along with a licensing agreement that (1) restricts others from modifying the content, and (2) sets a one-time charge of $1 to read or print the article. Having obtained any necessary permissions, the scientist also incorporates two related articles in the same digital object.

Each of these articles could carry a similar set of conditions regarding modifications and pricing. Readers of the first article are not required to access the two additional articles. However, for the convenience of providing the additional articles, the researcher marks up each by 10 cents. So, if someone opens this container and views all three articles, the researcher would receive $1.20 and each of the authors of the other two articles would be paid $1.

7.0 Conclusions and Recommendations

This paper addresses several important issues about managing access to digital information. It highlights the overlap of legal and technical concerns, and introduces certain important concepts that may facilitate the development and evolution of network-based information services, in particular, rights management systems. One such concept is that of a **digital object**, i.e., a data structure for identifying and organizing information for access over a communication network. Another concept described here is **stated operations**, that is, the types of operations that may be performed on digital objects. Stated operations are a useful construct in helping value-added service providers and other users of protected information understand the scope of their liabilities.

Key infrastructure requirements in pursuing new business opportunities using network-based digital information are also discussed, and various rights management technologies introduced. It is highly advisable to gain experience with these capabilities so that their implications may be better understood and the resulting systems and techniques refined. Some guiding principles for the evolution of the field are introduced. Of these, the most important are the focus on digital objects as packages of structured digital information (encrypted or not) for provision of information in the network environment and the use of rights management techniques such as the incorporation of terms and conditions in a digital object's metadata, together with a capability of negotiating additional permissions with a rights-holder, or a means of determining where such information may be accessed.

The new capabilities described in this paper may require a new or revised legislative framework. Before laws are revised or enacted, or new regulations issued, however, additional experimentation and experience are needed with digital objects in the marketplace. This will let nascent

markets develop without undue regulation, provide a base of experience to guide the formulation of new laws, and suggest where change is – or is not – justified. In particular, and as noted earlier, overlaps in existing laws, such as copyright, patent, and communications law, should be exploited to facilitate a more contoured and textured approach in dealing with issues of protection and liability than is possible through reliance on any single body of law.

A guiding principle in interpreting existing laws and regulations – and in formulating any new provisions – should be as follows:

> If an operation does not restrict or impair a rights-holder's revenue stream or existing rights or interests, is not explicitly restricted by the rights-holder in the stated terms and conditions of use that are linked to or included within a digital object, or is not otherwise explicitly restricted by law, then the operation may be presumed to be permitted. This principle should apply independently of the technology used to realize or convey a digital object, or the means used to transact business.

Public policy should foster and support an environment that promotes experimentation, enhances understanding, and encourages the development of pilot projects and new business practices. And, for the duration of such efforts, limited immunity under antitrust law and certain intellectual property laws may be desirable. For their part, the projects thus supported by public policy and legal immunity should be aimed at developing and deploying new technology and infrastructure to facilitate the conduct of business in a digital environment, including, in particular, unique identifiers and resolution systems for digital objects, protocols for access to digital objects, and public key cryptography as well as certification and authentication infrastructure that meets the legal requirements for U.S. domestic commerce. Public policy should also promote the development and voluntary use of an open architecture, including open standards and common business practices to support these efforts.

References

Bock, G.E. 1996. “InterTrust Commerce Architecture and Developer’s Kit.” In Distributed Computing Monitor. p. 3. Boston: Patricia Seybold Group.

Dreifus, C. 1996. “The Cyber-Maxims of Esther Dyson.” The New York Times, July 7: 16-18.

Dunstan, J.E., and P. Lyons. 1994. “Access to Digital Objects: A Communications Law Perspective.” In 1994 Annual Survey of American Law, pp. 363-82. New York University School of Law.

IBM infoMarket. 1995. “IBM Cryptolope Containers.” ≪http://www.infomarket.ibm.com/ht3/crypto.htm≫.

Kahn, R.E., and R. Wilensky. 1995. “A Framework for Distributed Digital Object Services.” ≪http://www.cnri.reston.va.us/home/cstr/arch/k-w.html≫. Reston, VA: Corporation for National Research Initiatives (CNRI).

Sibert, O., D. Bernstein, and D. Van Wie. 1995. “The DigiBox: A Self-Protecting Container for Information Commerce.” Proceedings of the First USENIX Workshop on Electronic Commerce, p. 171. New York, NY: USENIX Association.

Stefik, M. 1996. “Letting Loose the Light.” Internet Dreams, p. 221. Cambridge, MA: MIT Press.

Appendix A

Following is a short list of some of the most desirable attributes of a rights management system from a business perspective – that is, capabilities that facilitate protected information commerce and rights management.

- **Associated terms and conditions –** A key idea is that terms and conditions can be associated with specific digital objects, as well as with their underlying contents and that a rights management system may assist in enforcing these provisions. Among the terms and conditions applying at the digital object level are the "stated operations" described earlier. Permissions for access to a digital object or its contents may be included within a digital object's metadata, or may be delivered independently. The most sophisticated rights management systems will allow rights-holders to describe access terms and conditions for different models and contexts. For example, a property could be delivered with two sets of rules: one for pay-per-use and another that specifies a larger one-time fee for unlimited use. A property could also be associated with rule sets for different contexts, so that different pricing models or permitted operations could be granted based on whether the user were, for example, a student or a government employee.

- **Assured integrity –** Rights management systems also need to protect digital properties against loss of integrity through alteration or substitution of one work for another. Consumers may need assurance that the work they purchase or rent has not been altered; and rights-holders need assurance that their brands will not be undermined by unauthorized modifications or fraudulent recreations of their properties.

- **Chain of operations and value management –** Flexible rights management systems will support the ability of each distinct entity in the value chain – author, publisher, aggregator, repackager, payment method provider, customer, etc. – to contribute independently the business rules and other conditions that reflect its individual rights and interests. Some of these contributions may be under the control of more senior participants in the chain. For example, authors may permit their publishers to modify their works, but not permit others in the distribution chain to do so. Publishers may offer discounts to aggregators who, in turn, can mark up the price of the work.

- **Efficient and tamper-resistant –** Rights management technologies vary in their defenses against sustained attacks. Of course, not all digital information has to be made completely secure. Rather, the protection has to he high enough that the cost of breaking the security is disproportional to the value of the property being protected.

- **Flexibility –** Business, educational, entertainment, and other types of information are "consumed" using a variety of devices and appliances large and small. While some material is made available over a computer network, a variety of information resources are delivered on physical media – for example, motion pictures may be delivered on digital video disk. Rights management systems must incorporate technologies that support devices of varying sizes and capabilities as well as huge numbers of transactions. Further, an advanced rights management system must be able to support the broadest possible range of business models on an enterprise-by-enterprise, category-by-category, or even property-by-property basis. Such models refer not only to pricing strategies, such as "one-time purchase" or "pay per use," but also to the relationships among value chain participants. Value chain participants should readily be able to create ad hoc business and rights relationships, and dynamically change them in response to market or business conditions.

- **Payment methods –** Rights management systems must ensure that rights-holders and other distribution chain participants are paid appropriately for those properties that carry a price. In doing so, however, rights management systems should not impose undue economic burdens on the commerce being protected. For example, the cost of providing infrastructure services such as financial clearinghouse services must not be disproportionate to the value of the commerce being transacted. Many payment methods now exist, and more are likely to emerge. The best rights management systems should provide users, rights-holders, and others in the distribution chain with the broadest range of cost-efficient payment methods.

- **Persistent protection of digital information –** Some of the earliest rights management solutions delivered digital information in encrypted form, but made the unencrypted version available in unprotected form after payment. Advanced rights management technologies should be able to provide rights-holders with more persistent protection, if that is what they want.

- **Security and trust –** An obvious, but essential, requirement of a rights management solution is that it be trustworthy and secure. And a trusted system is only as secure its weakest link. While existing

security problems on the Internet – and on intranets – are well-known, much of the current focus has been on securing the "pipe." In contrast, advanced rights management systems should be capable of protecting both the digital object and/or its contents. Once encrypted (e.g., with protected keys), the sealed package as a whole (or discrete portions thereof) is protected. Rights-holders may want to enable some operations on their properties but to forbid others. As rights management systems become fully integrated with standard applications, controls will become increasingly fine-grained, thus providing rights-holders with many options.

- **Support for advertising models –** It is envisioned that there will be many different models of repositories, e.g., serving as a bank, as an advertiser, as a video distributor, or as a broadcaster. Many business models for digital information commerce will depend on advertising for some or all of their revenue. Thus, rights management technologies should support many advertising models.

Appendix B

Several basic technologies are now available that could be used successfully in advanced rights management systems. Some of the most promising are described below.

Encryption

Encryption is primarily used to make information secret or confidential so that only those who possess a certain key can access it. This information might be a digital work, rights management controls or pricing information, or other element. The key is simply a number. Advanced rights management systems make use of two different kinds of encryption technology: symmetric, or secret key, and asymmetric, or public key. **A symmetric key system** uses the same key to both encrypt and decrypt information; consequently, it is important to keep this key protected. **An asymmetric key system** uses a pair of keys that share certain mathematical properties. In an asymmetric system, if information is encrypted with one of the keys, it can only be decrypted by the other. As in symmetric key systems, one of keys – the private key – is usually protected. The other key – the public key – can be made available publicly without compromising system security, since the private key's value cannot be determined from that of the public key. Anyone can use the public key to encrypt information, but only the holder of the private key can decrypt it.

Digital Signatures

Digital signatures provide very strong indicators of integrity and authorship, and thus can be very important to rights-holders, value chain participants, and customers. For example, stockholders may need to know that a financial report has not been modified accidentally or intentionally. Digital signatures make that knowledge possible; they also can provide a reliable way of ensuring that rights are exchanged based on enforceable licensing agreements.

A digital signature can be generated using the cryptographic method called the **one-way hash function**. The hash is a calculated number that reflects the content of a particular digital object. If even one bit is changed, the value generated by the one-way hash function will also change. And, conversely, it is extremely difficult to change a digital object in such a way that corresponds to a particular hash value.
These features allow a person to "sign" a particular digital object using his or her private key. First, the person who wants to sign an object calculates the hash value using a one-way hash function. and then encrypts this hash value using the private key. Anyone who has the signer's public key can then decrypt the value, recalculate it, and compare the two numbers. If they are the same, the recipient knows that the digital object is unchanged and that it could only have come from the person with the corresponding private key. This protected hash method is even stronger than the one-way hash since it involves encryption.

Certification

Asymmetric key systems can also be used in conjunction with "certificates" that attest to or warrant some fact about the owner of a public/ private key pair. These certificates are issued by a "certificate authority" (CA), a service that performs varying degrees of fact checking before issuing a certificate. Among the kind of facts that can be certified are individual identities or membership in a particular class or organization. Certificates can also attest to the authenticity of a digital object and/or its content. For example, a CA may create a message that contains a structured factual statement that the public key in a given message belongs to John Q. Public, or that the person using a specific public key was born on April 19, 1960. The CA then encrypts the information with its private key. As with the digital signatures described above, this procedure allows those people who have the CA's public key to decrypt the message, and – assuming they trust the authority – to accept the facts conveyed as true.

In the best rights management systems, certificates can also convey contexts for rights usage. For example, a publisher may wish to offer discounted or free goods or services if customers can provide a certificate

attesting to the fact that they are affiliated with an institution of higher education, or a certificate indicating that they are affiliated with a not-for-profit research organization. Similarly, the rights management system may enforce one set of conditions on prices, taxes, and currencies in the United States, and another set in France, depending on which certificate covering jurisdictional issues is provided by a customer.

Fingerprinting and Watermarking

Steganography is the science of hiding messages in communications and is the basis of various so-called fingerprinting and watermarking techniques. For example, the location of marks on a page can be adjusted in minute ways so as to encode hidden information. Certain pixels of a digital image can be manipulated for the same purpose. Such hidden messages may be difficult to detect and difficult to remove by anyone who does not know how they were applied in the first place.

Advanced rights management systems can make use of fingerprinting in several ways. First, these methods can be used to encode copyright information such as property title and other identifying information (e.g., who owns the copyright and the year of first public availability). Second, when content is released out of a controlled environment – usually for a fee – a fingerprint can be added to many kinds of properties indicating who exported the property and when. The fingerprint can be used to indicate, or at least suggest, the initial source of the information in the event of infringement.

Other Security Measures

Software-based rights management systems can protect against overall system defeat and unauthorized access to digital information. The goal is to ensure that the cost of defeating the system is disproportionately larger than the value of the properties protected by the system. Some rights management systems are able to make use of secure hardware when it is present. This hardware may be a microprocessor and memory on a PCMCIA card, a tamper-resistant co-processor on the motherboard, or recently introduced advanced microprocessors. Secure processors help ensure that the digital properties will continue to be protected from all but the most dedicated and sophisticated attacks. More importantly, secure processors can provide strong protection for the rights management information that keeps the system operating correctly. This protection allows more processing of rights-related information on users' systems, which lightens the load on central servers and opens up new opportunities for user-initiated commerce. Until secure silicon is widely available, and perhaps beyond, software-only solutions can do a good job of protecting a broad range of digital information.

X I W T

Corporation for National Research Initiatives
1895 Preston White Drive #100 Reston, VA 22091