Journal of Technology Law & Policy

Volume 3 | Issue 2 Article 4

January 1998

Property Rights on an Intranet

Scott S. Kokka

Journal of Technology Law & Policy
Volume 3 Spring 1998 Issue 2
Published by Students at the University of Florida College of Law

Return to Table of Contents | Comment on this Article

Property Rights on an Intranet

by Scott S. Kokka

Cite as: Scott S. Kokka, *Property Rights on an Intranet*, 3.2 J. TECH. L. & POL'Y 3 <http://journal.law.ufl.edu/~techlaw/3-2/kokka.html> (1998).

TABLE OF CONTENTS

I. INTRODUCTION

{1} In a world which is becoming increasingly reliant upon the Internet and information infrastructures, widespread use of "cyberspace" [1] is creating extensive decentralization of the Global Information Infrastructure (GII). One of the most prized attributes of the Internet is its free flow of information to all parts of the world supplied by a telecommunications infrastructure. However, the Internet's greatest characteristic is also its darkest threat: ready access by anyone, anywhere. With the explosion of e tronic commerce looming on the horizon, many companies are beginning to look for ways to control this anarchy and prevent the chaos of unregulated access on the Internet from spreading to their internal computing networks. If a corporation or organization wants to maximize its efficiency and productivity through the use of information technologies, it must assert control over content, activity and access. One of the tools which can help keep the anarchy of cyberspace under control is an intranet. [2] Operating on the same technologies as the Internet, an intranet makes it possible for large-scale corporations to implement protected internal computing networks for organizing data and information. Intranets are changing the way information is used, managed and disseminated within an organization. Increased productivity, centralized management of large projects, heightened efficiency and higher returns on investment (ROI) are some of the immediate benefits of implementing an intranet. There are distinct differences between the Internet and an intranet in terms of application which are especially apparent in the realm of proprietary rights.

{2} Proprietary rights on the Internet have been especially difficult to define, particularly since there are no geographic boundaries or borders to cyberspace. The inherent nature of the Internet does not recognize territorial limits; it expands to where the telecommunications infrastructure will allow it. The "Information Superhighway" is anarchic in nature, like a freeway without lane dividers, police or a directed flow of traffic. It has virtual off-ramps which lead to smaller communities of self-contained information known as "websites." These sites are increasingly taking the form of secure, encapsulated intranets to stabilize much of the anarchy of the free-flowing general Internet. Additionally, by employing a secure and organized means of accessing the Internet, corporations and individuals can maximize the benefits of electronic commerce. The essential qualities of an intranet which make it significantly different and appealing from the Internet is that it can provide structure, organization and security to cyberspace as discussed below. Intranets are a secure means of using the Internet and can simultaneously provide answers to previous questions of jurisdiction and choice of law in resolving proprietary rights disputes in cyberspace. By using an intranet, a corporation or entity can predict with a fair degree of certainty how issues regarding the use of patents, copyrights, trademarks and other proprietary rights should be resolved in cyberspace.

II. WHAT IS AN INTRANET?

{3} In 1994, Dr. Steven Telleen of the Amdahl Corporation first coined the phrase "intranet" in a paper entitled IntraNet Methodology. [3] This is the earliest known use of the term and is generally credited as the first written description of the technology. [4] However, the technology is not new; it has been around as long as the Internet and the World Wide Web. [5] An intranet is an internal network of

computers, servers, routers and browser software designed to organize, secure, distribute and collect information within an organization. [6] They operate on the same technologies as those used for the general Internet. However, intranets are different because they can be completely isolated from the Internet by means of a protective shield which prevents access via hardware or encryption/authentication software or through a combination of both elements. The protective shield is known as a "firewall" and is used to effectively isolate the internal network from the Internet at large. [7] The secure nature of intranets is changing the way information is organized and managed within the workplace, and "firewall" security is the most essential component to ensuring the greatest benefit from using the Internet, particularly in areas such as the growing field of electronic commerce. [8] Valuable key features of intranets which make them appealing to goods and services providers alike are the ability to deploy security and encryption measures.

{4} Intranets are bringing an entirely new set of benefits to the workplace, especially in organizations which have a high level of decentralization in their operations and subdivisions. These internal networks increase efficiency and productivity, yield a high ROI, provide decision-makers and executives instant access to real-time information and data, and allow project managers to coordinate input from a decentralized computing organization. [9] Intranets are tailored to the specific needs of an organization and can be described in five distinct categories of evolution. [10] All five categories are in use by a wide-range of organizations, depending on the scope of information organization, distribution and efficiency. An emerging enterprise, intermediate manufacturing company or a multi-national company will each require a different level of intranet. These levels are defined as: Basic, Publishing Library, Collaboration, Transactions and Extranets. [11]

A. Levels of an Intranet

{5} Not every organization has the same requirements for structure, access or security with regard to using the Internet, but an intranet is designed and deployed to meet specific needs and scope. The first level of an intranet is the "basic intranet" which is a small website designed for the use of an individual or a small collection of users. [12] The key reason for using a basic intranet is to provide information for the education of the individual members of the organization. [13] At the next higher level of organization is the "publishing library," which is used for corporations or organizations which operate off of a common database, such as using general, company-specific forms. [14] These types of intranets are the most commonly used in organizations or businesses which are confined to small-scale operations. [15] Organizations with a much higher level of complexity and decentralization will require greater services and will need to use either a "collaboration" or "transactions" intranet. [16]

{6} Large organizations such as educational institutions, intermediate level manufacturing facilities and multi-departmental companies deploy collaboration intranets. [17] This level of intranet provides a wide range of services including e-mail, project management and directory services. Many corporations have deployed collaboration intranets and they fulfill data and information management requirements. Usually, a collaboration intranet is used by a large organization which requires the use of information among several departments located on a single site, such as a university or large manufacturing site. Finally, large organizations which require greater capabilities for coordinating data and information among geographically independent offices or departments are deploying transactions intranets.

{7} A "transactions" intranet is useful when extensive projects with a wide range of users, such as research and development or financial services, need to be organized. At Netscape Communications Corporation, the largest supplier of internet/intranet servers, over 50% of all sales were for transactions intranet applications. [18] Transactions intranets are capable of fully-integrating corporate functions

with the databases and systems of the organization. The transactions intranet extends to all levels of operations and is used to maximize efficiency through real-time project management, electronic mail and information coordination. It can also employ a wide range of applications across all levels of an organization, using inter-operability languages such as Java and Active-X, which allow compatibility across several different types of platforms, i.e. running the same program simultaneously on an Apple MacIntosh as well as an IBM PC. [19] Finally, the last level of evolution for an intranet is the "extranet;" a mammoth internal network designed to manage and coordinate the operations and information of large organizations on a global scale. [20] This is referred to as "inter-enterprise" networking and represents the largest evolutionary version of an intranet. [21] It is deployed only by corporations which require the full-service capabilities of a transactions intranet and the added ability to handle electronic commerce and manage global projects. [22] However, an intranet's efficiency and effectiveness is directly proportional to its degree of control and management. Some of the primary concerns in terms of control are resolving issues of access and use, which require the implementation of protective measures to defend the internal network from the "anarchic" nature of the Internet. An uncontrolled intranet, especially one with poorly managed firewalls and access is no more efficient than the general Internet itself. This means lowered protection and security which will jeopardize any proprietary information stored within an intranet. This can be particularly damaging where the use of trade secrets is the primary form of protection for intellectual property.

B. Firewalls and Encryption

{8} An intranet is similar to the Internet in that it transmits packets of information rapidly to various locations along its length, depending on access to the available telecommunications infrastructure. An intranet is similar to the Internet in that it enables intra-organizational information to be freely available and accessible, but only within an internal network. It is also difficult, if not impossible, to determine a geographic location for any piece of information on the Internet. This creates significant problems for resolving conflict of laws issues for cyberspace disputes. These difficulties are still being resolved by the World Trade Organization (WTO), World Intellectual Property Organization (WIPO) and the International Telecommunications Union (ITU) in terms of defining proprietary rights on the Internet. [23] However, intranets may provide answers to these difficult problems through the use of old technologies in a new fashion. What makes an intranet different is its ability to isolate itself from the general Internet through the use of "firewalls," gateways and encryption programs. Access through an intranet creates a situation where there are two distinct parties: the owner/operator of an intranet and the external/internal user.

{9} A "firewall" is a protective barrier comprised of hardware and software which represents the first line of defense against penetrations into or out of an intranet. [24] Security is the primary concern in preventing or controlling access and activities within an intranet. [25] Sensitive information, such as corporate trade secrets, contained within an intranet require protection from disclosure or misappropriation. Computer fraud and break-ins represent losses in millions of dollars every year. As a result, corporations spend over $6.3 billion on intranets and security systems. [26] This is estimated to increase to $13 billion given the explosive growth of electronic commerce within the next year. [27] Firewalls and encryption technology represent some of the major security instruments which can protect corporate intranets and websites as well as ensure safe and rapid expansion of electronic transactions in cyberspace.

{10} Encryption software is used to supplement firewalls by providing a protective barrier against unauthorized or indiscriminate access from the Internet. Encryption is a highly controversial subject in terms of cyberspace applications, however it is extremely useful and important for establishing intranet

security. The debate centers around whether this technology, which is used to encrypt and decrypt data, should be regulated and, if so, to what extent. There are two principal types of encryption methods: public and single key. [28] Public key encryption relies on having two separate keys, one to encrypt and the other to decrypt data or messages. [29] Without both keys, only one of which is publicly revealed, the data is incomprehensible. [30] Under the single key approach, only one key is needed but it is not publicly disclosed. [31] Both types require the use of a secret encryption key to decode data. These secret keys are the subject of past, present and future attempts at enacting legislation and regulations on encryption. [32] The government is concerned that by not being able to gain access to these keys it will lose the ability to intercept, monitor or impose surveillance upon suspected or known criminals who may be using encrypted messages or electronic mail to communicate or perpetrate crimes. [33] This concern extends beyond the domestic sphere and has a multitude of ramifications upon the issue of national security. Proposed plans include either a form of "key escrow" or a trusted third party system in which the secret encryption key would be registered with the government to allow decrypting at will. [34] Industry leaders, educational institutions and technology developers are strongly arguing in favor of self regulation instead of government intervention which may force mandatory registration of encryption keys.

{11} Just about every sector of business is concerned with the security and privacy of electronic messages and mail in cyberspace, on the Internet and within an intranet. Employers are concerned that proprietary information or sensitive corporate trade secrets are being divulged or misappropriated and employees are mutually concerned about privacy and integrity in communications. However, the benefit of an intranet is that encryption can protect highly sensitive areas from within as well as prevent unauthorized external intrusion. Trade secrets and confidential information can be encrypted to prevent unauthorized access. Encryption can also provide virtual privacy between the sender and receiver of electronic mail and messages. The debate is left in further disarray by the question of how to balance constitutional concerns with the national security. [35] An area of the Internet law which is still widely debated is how to resolve previous constitutional issues such as the First Amendment right to freedom of speech or jurisdiction under the Fourteenth Amendment without sacrificing the concern of protecting the security of the nation.

{12} Whether a communication on the Internet or on an intranet is protected by the First Amendment can largely be answered by a traditional analysis of whether the electronic message falls into one of the unprotected categories of speech. [36] Under the standard developed by the Supreme Court in *Brandenburg v. Ohio*, there are very few classes of unprotected speech. [37] The technology involved with Internet/intranet communications does not provide any substantial reason why this traditional analysis and rule should be invalidated. In fact, the *Brandenburg* standard has been used in addressing television and radio communications as well. [38] Rapid changes in technology do not require a subsequent alteration of legal standards and norms.

{13} Intranets also answer many of the questions surrounding jurisdiction by providing the location of "where" a cyberspace event occurs. Access to users can be subject to consent to specific terms prior to entering an intranet. Such terms can include forum selection clauses which specifically delineate the particular forum where disputes or litigation will be addressed. In the event an intranet firewall does not have a forum selection clause, penetration of the firewall should be the point at which a user enters the "loci" or place. Under a territorial approach to the conflict of laws, this is known as the "lex loci fori" or the law of the forum, which is defined as the geographic area where the intranet servers are located. [39] This generates the nexus of contacts which courts may find sufficient to assert jurisdiction over a particular party as a result of their particular Internet activities. Jurisdiction, the First Amendment and the national security are only three of the major concerns which are involving government legislators

and industry officials in regulatory debate over the Internet and cyberspace in general.

{14} As an interim measure to address national security concerns in 1994, President Clinton, citing the International Emergency Economic Powers Act (IEEPA), declared that encryption technology represents an emergency and has placed it on the U.S. Munitions List as a prohibited item for export. [40] This action, under Executive Order 12,924, is mitigated by the transfer of agency cognizance from the U.S. Department of Defense to the U.S. Department of Commerce for oversight purposes. [41] The current state of affairs is still unresolved and to address the Constitutional questions and details of encryption would take this article well beyond its intended scope and subject matter. Nonetheless, encryption is a fundamental and critical component to deploying an intranet because it provides security and places an identity to a computing network which is useful in resolving disputes over intellectual property rights in cyberspace. With the predicted growth of electronic commerce and the digital economy looming on the horizon, the ability to conduct secure transactions is absolutely necessary.

III. COMMERCIAL POTENTIAL

{15} A growing segment of the Internet industry designs and constructs intranets, known as "outsourcing," tailored to the specific needs and requirements of the customer in a market. [42] Requirements for size, security, access and scale of operations can be incorporated into the construction of an intranet. Internet content, service and goods providers are relying on large telecommunications and computer software companies to manufacture entire systems tailored to meet their particular requirements. [43] Inter-enterprising networks are becoming increasingly popular with organizations which are deploying intranets to take advantage of the growth of electronic commerce. Many types of organizations such as financial, governmental and educational institutions, law firms, hospitals and pizza delivery services as well as technology developers are turning to the use of intranets as a means of maximizing the Internet medium. Additionally, other industries, besides information technology sectors, are becoming increasingly reliant upon the use of intranets.

{16} Manufacturing industries are particularly well-suited for deploying intranets to track project development and management. Intranets maintain real-time tracking on daily output, expected delivery shipments and other operations which can be improved through an increased flow of information. [44] Design teams can place models and plans on a corporate intranet and allow every member of the team to access the information with the expectation that it is the latest updated version. Executives and decision-makers also benefit by referencing the real-time "information state" of the company. Intranets gain the most benefit when they are used by a corporation looking to use the Internet to sell goods and services in electronic commerce. The tremendous growth of electronic commerce makes intranet deployment desirable in addition to its capabilities for project management, increased productivity and improved efficiency. [45]

A. Electronic Commerce

{17} The predicted value and benefits of electronic commerce vary greatly. Most surveys and analyses can only project a few years past the turn of the millennia and those that venture further are probably more speculative than analytic. [46] However, it is undisputed that electronic commerce is a tremendous and potentially vast source of revenue. In the United States, current indicators estimate that electronic commerce will reach in excess of $327 billion by the year 2002. [47] In 1997, over 33% of the Gross Domestic Product (GDP) was generated from information technology industries alone. [48] Consumers and businesses spent over $282 billion on information technology products, goods and services, not including electronic commercial transactions. [49] Internet/Intranet server sales are yielding accurate

trend information about electronic commerce. In 1997, more than 50% of all web servers sold were for intranet applications. [50] By the turn of the century, this figure is expected to increase dramatically, with intranet servers exceeding 90% of all sales. [51] In the extranet software market alone, sales are anticipated to grow, reaching an estimated $400 million by the turn of the millenium. [52] In light of these apparent indicators, electronic commerce is growing at a rapid rate and there is an enormous demand for technology components which will allow access to these markets.

{18} Telecommunications, Internet telephony and on-line goods and services are gradually coming together to provide "one-stop" shopping for consumers from a single supplier. Digital convergence will expand the National Information Infrastructure (NII) and the GII, providing the public with greater access to goods and services, further enhancing the appeal of electronic commerce. This will significantly alter the global trade, commerce and communication infrastructure. Since the enactment of the U.S. Telecommunications Act of 1996, markets in competing technologies such as cable, telephony and information services have begun to open. [53] Traditional cable companies are cooperating with technology firms to provide combined television programming and high-speed Internet access. [54] If this trend continues, eventually a single utility or service company will be able to provide cable, telephone services, electronic mail and Internet access via a single device or "set-top" box. [55]

{19} Although convergence is still in its infancy, it is driving the developers of information technology to create new markets for electronic commerce by means of devices other than personal computers. New consumer markets will open from the intersection of the television, cable, telephone and telecommunications industries. Electronic commerce is expanding beyond its reliance on Internet access via computers alone. The growth of electronic commerce will require corporations to be more sophisticated in the use of information for organization, management and production. An intranet is an ideal tool for accomplishing these objectives and generates an extremely impressive ROI in the process.

B. Return on Investment (ROI)

{20} Corporations and organizations which require efficient tools for communication, collaboration and knowledge-building recognize the inherent benefits of deploying an intranet. [56] Cost savings are among the major benefits of an intranet and are factored into calculating the return on investment (ROI). Important factors in calculating the ROI include the cost of maintaining and administering an intranet and personnel costs. In fact, the most significant costs associated with deploying an intranet are not the actual hardware or software, but the training and hiring of support personnel to manage the intranet. [57] However, despite these costs, the value added and ROI from deploying an intranet are significant enough to justify building one. [58]

{21} The high ROI is calculated by tabulating the costs of hardware, software, personnel, training, implementation and maintenance. [59] These are compared against the benefits and savings in time and money, which are calculated in terms of the time saved per employee in a standard work day. [60] Although individual employee savings might be insignificant, a corporation with several thousand or even a few dozen employees might find that several hundred work-hours per day may be saved as the result of deploying an intranet. In a study conducted by the International Data Corporation, the average ROI appears to be generally high enough to recover the costs of deployment within six to twelve weeks. [61] Large multi-national corporations with decentralized operations were found to have exceptionally large savings and ROIs. Corporations such as Lockheed Martin and the Amdahl Corporation realized ROIs in excess of 1500%, given the relatively low cost of implementing an intranet to manage extensive and decentralized manufacturing operations. [62] With over 170,000 employees, of which 140,000 of whom use an intranet, Lockheed Martin, the world's largest developer of military aircraft, experienced a

tremendous amount of savings in terms of increased efficiency and overall information management. [63] After calculating three years of expenditures for hardware, software, training and personnel for the intranet which totaled $1.9 million, the total savings was in excess of $28 million. [64] Generally, the larger the intranet, the greater the return on investment.

IV. ATTRIBUTES OF THE INTRANET

A. Benefits and Costs

{22} Deploying an intranet creates risks, but these are quickly overrun by rapid gains in increased efficiency, cost savings and a competitive edge. The immediate benefits are gained in improved real-time project management and increased productivity. [65] Once implemented, an intranet provides immediate organizational and improved management benefits of data and information. However, savings are not initially realized due to the costs incurred in implementation and personnel training. These immediate costs are known as "ramp-up" expenses which include not only the purchase of hardware and software, but also training and personnel. [66] Over a longer period, however, the increased efficiency derived from an intranet assists the corporation in gaining a competitive edge. [67] Real-time project management and the rapid flow of information are significant factors in gaining a leading edge over competitors, especially in manufacturing processes and research and development organizations. The two largest areas of risks which diminish these benefits are access and security. [68]

B. Access

{23} Access is the primary concern in terms of maintaining control over an intranet. The risks involved with widespread use of an intranet are usually associated with either internal or external unauthorized access to data and corporate information stored on an intranet. These risks are more easily managed on an intranet than on the Internet because of the ease of managing an enclosed structure compared with an anarchistic collection of uncontrolled and unrestricted information. [69] One of the major characteristics of the Internet which has generated tremendous debate is its free-flow of information and whether the uncontrolled access that accompanies it is an asset or risk. [70] Some argue that the tremendous availability and freedom of information is a wonderful asset, while others, usually institutions or organizations who want to use the Internet for commercial purposes, assert that the anarchy and lack of control is a major security risk for all involved. On an intranet, the external problem can be resolved through the use of firewalls and encryption technology which provide containment barriers. Controlling access ensures the integrity of an intranet and creates a single, cyber-identity for purposes of determining jurisdiction and conflicts of laws. Intranets are fundamentally different in so far as they make it possible to determine a forum, from which a distinct body of law can be chosen and applied. Deciding what jurisdiction will apply will determine what body of intellectual property laws will be used as well. By allowing access to an intranet, contract formation can be used to answer these questions through the use of "web licenses" or access agreements prior to entry. [71] The internet permits access to anyone with the requisite elements of a telecommunications infrastructure. Once enabled with access to the Internet, there is no control mechanism for governing the activities of users, other than denying basic access or filtering the content of materials placed on it. Activities within intranets can be governed by existing contracts law, by providing access contingent upon acceptance of the corporation's terms of behavior while using it. [72] Coase's basic economic theory supports this notion that the contracting parties will reach the most economically efficient result, with the user providing guarantees on her behavior in return for the opportunity to view the information or content within the intranet. [73] This is dramatically different from the Internet in that it is much more difficult, if not impossible, to determine a single point or place where a contract was formed. In general, determining "where" and "how"

information is accessed is extremely difficult on the Internet, i.e. a user in Australia who gains access through an Internet Service Provider ("ISP") in Germany and then enters the general web page of the U.S. Library of Congress is indistinguishable from a user performing the same activity from the District of Columbia. An intranet is distinct in that it is not an amorphous river of information without boundaries. It is an internal organizational network which has been designed, implemented and administered for a single entity. System administrators acting on behalf of the corporation can control access, enforce security, track users, and form contracts with external users to permit access and gain certain promises in return. In addition to access, intranet security is the second major asset which distinguishes intranets from the Internet.

C. Security

{24} Security on the intranet is modeled after the U.S. Department of Defense Trusted Computer System Evaluation Criteria. [74] The Trusted Computer Criteria, also known as the "Orange Book," lists detailed guidelines for specific levels of security within an internal computing network. [75] Although the standards were created in 1985, the "Orange Book" has been an effective model for intranet security in the private sector. Access should be limited to a few key personnel in the most sensitive areas of an intranet. For example, in a software development firm, the chief technology officer or operating officer may have an A(1) rating which permits wide, but controlled access. [76] On the other hand, external users or customers of an intranet may be restricted to a lower rating of C(1) or C(2) which would permit only limited control of personal or private information entered during the course of the transaction. [77]

{25} Trade secrets, confidential material and projects can be closely guarded by implementing graduated levels of security. To protect proprietary information, external users should be strictly limited to areas which are required for electronic commercial transactions. Large-scale operations such as global intranets and multi-national networks are more susceptible to unauthorized breach because of the high degree of decentralization and increased number of external and internal users. [78] Comprehensive policies should incorporate measures for external/internal use, physical security and access to proprietary information. [79] Intranets are an important organizational tool, and with electronic commerce they become profitable as well, especially when valuable intellectual property can be managed so as to increase its utility and productivity.

V. INTELLECTUAL PROPERTY ON AN INTRANET

{26} Understanding the value of protection of intellectual property provided by an intranet requires a different approach than the Internet. The self-contained nature of an intranet allows the use of forum selection clauses to establish a choice of law through contractual arrangements which, unless agreed to by both parties, will determine how to resolve conflicts. [80] A fully developed intranet firewall using encryption, information questionnaires and security validation measures provides a means to determine when and where a user accesses it. From a geographic "real space" perspective, it would be similar to crossing through a customs inspection station, i.e. "Identification, please? Where are you going? What is the nature of your visit? Have a nice day." Once passing through the wall, private laws or rules of the corporation will determine the outcome of any acts or disputes which occur within it. An intranet is an ideal means of further protecting intellectual property in cyberspace.

A. Patents

{27} The state of the law with regard to patents and computer-related inventions, which includes the Internet and intranets, is vague and ambiguous in terms of what is permissible and what is not. In 1972,

the U.S. Supreme Court ruled that mathematical algorithms are not patentable under § 101 of the Patent Act. [81] In the cases that followed *Gottschalk v. Benson*, additional guidance for defining the patentability of computer-related inventions was not clear. However, where a physical process appears to interact with the algorithm, and the mathematical formula is not wholly pre-empted, then patentability may be permissible. [82] The nature of Internet technology is intangible and, with the exception of the hardware components, non-patentable subject matter under § 101. However, although an intranet relies upon the same technologies as the Internet, it is fundamentally different in that there are physical aspects to an internal network.

{28} An intranet is a system or method of operation which, as defined by § 101 of the Patent Act, is patentable. [83] Outsourcing technology development firms are manufacturing entire intranets which are tailored to meet the individual needs of a specific corporation, organization or consumer. [84] These custom-made units incorporate hardware components along with the necessary software to generate an organizational system to manage information and databases within the corporate network. If the outsourcing developers are able to satisfy the conditions of patentability under the Act, such as utility and novelty, then it would be possible to obtain patents for the various models or types of intranets. This is not achievable for the Internet since it would be impossible to embody the entire GII and resolve inventorship issues. An intranet is designed as a self-contained virtual network and is physically embodied in servers, browsers and other web architecture components which are patentable.

{29} However, patentability does not extend much further than to the actual system or process of an intranet. Apart from the overall system and its individual components, it would be unlikely to obtain patentability for data or information stored on the databases or software applications used within the network. In fact, in light of the *Benson* prohibition placed on mathematical algorithms and object code, software patents would be difficult to obtain without some sort of physically interactive process or transformation. [85] For these "intangible" components of an intranet, copyrights should be sought for protection.

B. Copyrights

{30} Copyright law is another unsettled area of intellectual property law with regard to the Internet. However, the Copyright Act may be the only source of protection for software applications which are not physically embodied or interacting with a transformation process. Unlike the Patent Act, there are specific regulations codified to deal with computer programs and software. [86] Copyright protection for software is statutory, providing for specific remedies and damages. [87] There is also a statutory period of protection which, under certain conditions, can be extended. [88] Copyright law is more flexible than patent law in terms of protection for software, however, there are problems in this area as well.

{31} An intranet is a system or method of operation, used as an organizational tool to enhance project management, increase productivity and improve efficiency. As a method of operation, an intranet would be expressly prohibited from copyright protection under § 102 (b) of the Copyright Act. [89] The software applications and computer programs used to coordinate and organize the internal network can be protected as "literary works" under the Act. [90] However, the components of an intranet such as application software which employ menu command hierarchies are non-copyrightable in light of the decision in *Lotus v. Borland*. [91] Menu command hierarchies which are used as graphical user interfaces with an intranet firewall would fall under that preclusion to copyright protection. In *Lotus*, the Court of Appeals for the First Circuit ruled that menu command hierarchies were not protected under the Copyright Act. [92] Thus, as Judge Boudin suggests in his concurring opinion, an alternative form of protection such as the Patent Act should be chosen over existing copyright laws. [93]

{32} With regard to databases and information files stored on an intranet, a minimal degree of creativity must be established to meet the test as defined by the Supreme Court's decision in *Feist v. Rural* in order to afford protection under the copyright laws. [94] Intranets with user interfaces might be able to meet this standard if the data were stored in such a way as to convey originality. In *Feist*, the Court found that not every selection or arrangement of data and information would be copyrightable, reinforcing the extinction of the "sweat of the brow" doctrine. [95] In order to find that copyright protection does extend to a database or factual compilation, there must be some minimal degree of creativity or originality in authorship which would meet the spirit of the requirements under § 102 of the Act. [96] Keeping in mind that copyright protection can be extended to individual portions of intranet software which meet the "original works of authorship" requirement of § 102 (b), corporate projects and research and development efforts might be protected under these categories.

{33} Confidential information and projects often represent the most important and valuable work product of a corporation, especially in industries such as aerospace, defense, computer, information technology and automotive. Protecting information on an intranet such as confidential project information is permissible under the Copyright Act, provided the minimum level of creativity is met. [97] However, where this information represents significant financial interest to the corporation, protection may be better suited under the law of trade secrets. The tension between copyrights and trade secrets is such that information on an intranet can be protected under both forms without actually disclosing the trade secrets. [98] There is no requirement to choose between either trade secrets or copyrights, but caution should be employed when considering whether to disclose valuable confidential information to anyone outside the trusted parties within the corporation. [99] The theft of copyrighted material is becoming an increasingly reliable area of the law.

{34} On December 17, 1997, President William J. Clinton signed the No Electronic Theft (NET) Act which, once effective, imposes criminal penalties for the theft of copyrighted material by using the Internet as the medium for the crime. [100] The Act imposes a sliding scale of penalties of imprisonment and fines, regardless of whether the person(s) who commit the crime profit from it. [101] For corporations and organizations that deploy intranets to organize and protect valuable information or trade secrets, this Act is a powerful tool to prevent theft. Some individuals and groups have argued that this legislation could also have the effect of limiting the fair use doctrine. [102] The "fair use" doctrine enables courts to determine whether a particular use of a copyrighted material is infringing based upon equitable factors. [103] However, unless the infringing use is found to be willful, the NET Act does not apply. [104] The full effect of the law remains uncertain until litigation is brought which challenges the scope of the NET Act.

C. Trade Secrets

{35} Under the Uniform Trade Secrets Act (UTSA), which has been adopted in all but a few states, state law governs what can be protected as a trade secret, as well as how to determine issues of infringement. [105] Security is critical to ensuring that the commercial viability of research and development projects is maximized by limiting the number of people who have access to the information. An intranet is an excellent form of protection for trade secrets and, if administered properly, can maintain tight and accurate security over internal confidential information. However, regardless of intranet security measures and policies, keeping valuable physical information such as flow-charts, indices and other research in a secure location is just as important as it was before the deployment of the network. [106] Even the most fervent advocates and developers of intranet technology support physical security measures for extremely sensitive documents. [107] There are a significant number of components of an intranet which can be protected as trade secrets, such as encryption and software applications.

{36} Encryption programs coupled with physical devices and hardware meet the "transformation" test set forth under *Gottschalk* [108] and can achieve patentability. The transformation test is used to establish patentability for an invention by determining whether the invention reduces an article from one state to another. [109] Encryption programs transform intelligible information such as messages and data into nonsensical numbers and letters and vice versa. If the object of the patent application is written in such a way as to incorporate a system or method of operation which is physically embodied in a hardware component such as a server or networking computer, then the chances are good that it can achieve patentability. However, even if patentability were achievable in this manner, it is still subject to determining a physical element and there must be an election as to whether to use trade secrets or patent protection. Patents and trade secrets cannot be used together or to supplement each other.

{37} An invention must be sufficiently disclosed so as to meet the descriptive requirements of § 112 of the Patent Act. [110] The disclosure of the invention is made to the People of the United States and, in return for the statutory monopoly, the inventor donates his information to the public. A patent monopoly can only protect that which is disclosed. This runs contrary to the underlying theory of trade secrets, which requires that in order to maintain protection, the commercial information which derives independent economic value must be maintained as a secret. [111] In short, intranet projects and confidential information should be protected under either patents or trade secrets, relying on subsidiary uses of copyrights and trade secrets for comprehensive protection. Intranets make the use of trade secrets more viable and less risky in light of its firewalled isolation from the Internet and general disclosure in cyberspace.

{38} Finally, for any software application which is used on an intranet, by either internal employees or external users or customers, a license, web-license or some other form of virtual agreement can be used to preclude the possibility of discovering trade secrets through reverse engineering. [112] The nature of an intranet provides a clearly defined party which is able to enter into contract and licensing agreements for trade secrets protection. Unlike the Internet, an intranet provides a means for establishing a contract between parties which can ultimately determine how disputes will be resolved through clauses which provide for conflicts of laws, jurisdiction, alternative dispute resolution and mandatory arbitration. The Internet cannot do this because there is no single point or frame of reference to determine where or who is participating in a transaction. This is troublesome when trying to establish liability for actions occurring on the Internet, in terms of who is involved and what the intent was in forming the original transaction. [113] However, with improved recognition of the need for international cooperation and greater use of intranets, it may be possible to establish some form of trans-national framework to regulate cyberspace in its entirety. [114] This need for uniform application of laws is especially visible in the area of trademark law.

D. Trademarks

{39} Trademark law is particularly applicable in the areas where goods are being sold from the intranet in electronic commerce such as software downloads. Trade and service marks can be applied to these goods, indicating a mark-good association. However, the nature of cyberspace makes it difficult to determine whether there is a general acceptance that a good sold on the Internet is actual commerce. Some courts have found that Internet content resides in the stream of commerce and this is becoming a more commonly accepted theory. [115] Another unique area of trademark law which is applicable to intranet deployments is the registration and use of domain names, which are used to locate particular websites.

{40} A domain name is a label such as "www.kokka.com" which is matched with a series or sequence of

numbers which serves as an Internet address and are used to locate specific websites. [116] Intranets are internal networks which are composed of a collection of individual web pages and web sites which can be located by these domain names. The use and registration of domain names is an especially difficult area of trademark law for a number of reasons.

{41} Domain name registration is a very unsettled area in Internet law. The current registration process is controlled by a private corporation, Network Solutions, Inc. (NSI) which functions under a contract with the National Science Foundation. [117] NSI registers domain names on a first come-first serve basis for a nominal fee, which entitles the owner to exclusive use on the Internet. This contract and registration system will expire on March 31, 1998, with national responsibility being given to a non-profit organization which will be established from April to September, 1998 and international responsibility being assumed by the International Telecommunications Union (ITU). [118] Web page domain names for sites within an intranet are registered under the corporate entity with NSI.

{42} The registration process is used in conjunction with existing trademark law to resolve disputes under the Lanham Act [119] for the use of domain names. Intranets do not pose any new challenges or significant problems to existing trademark law, but it may ease some of the debate by focusing industry efforts to find a solution to the registration dilemma. The increasing use of intranets is demonstrative of the fact that the Internet is becoming an increasingly viable means of conducting business. Other areas of the law such as trademarks and domain names must be resolved or the potential will be lost. Disputes which involve two or more competing organizations using or seeking to use the same domain name can be resolved by looking at the nature of their intranets. Intranets aid in the resolution of these problems by enabling courts to resolve trademark infringement claims. Intranets provide a specific entity to evaluate for similarity. The use of an intranet can help the fact finder decide whether the nature of their transactions are similar enough to warrant a finding of infringement. [120] Potential problems will rise under the domain name dispute which are beginning to assume international proportions with the impending expiration of the NSI registration system. Furthermore, intranets help provide a foundation upon which to develop and adopt uniform standards for the protection of intellectual property and regulation in cyberspace.

VI. REGULATION OF CYBERSPACE

A. Approaches to Regulation

{43} Regulatory proposals for cyberspace, the Internet, and intranets are framed in three different categories: governmental, self, and no regulation. Governmental regulation tends to be found in countries where the rate of growth of the information infrastructure and penetration rate to the population are fairly low. Third world nations are particularly susceptible to extreme forms of governmental regulation due to political instability or weak economies which are barely able to support existing telecommunications services and infrastructure. Self-regulation is industry driven, relying on competition in open markets to ensure that activity and content in the marketplace are being driven by consumer desires. This relies on the assumption that parties operating in cyberspace, such as owners of corporate intranets, will ensure unwanted content and activity are suppressed to prevent interference with market operations. [121] Finally, a no-regulation scheme seeks to impose no controls or restrictions on access or content and allows the free-flow of information on the Internet to continue.

B. Types of Regulation

{44} There are two principal forms of regulation in cyberspace: content and activity. [122] Content

regulation refers to the control of the subject matter placed in cyberspace. [123] This is usually accomplished through the use of filtering programs or government censorship in countries which impose strict regulatory schemes upon their information infrastructures, such as Singapore and Vietnam. [124] Activity regulation targets the specific conduct which occurs in cyberspace by prohibiting undesirable transactions from occurring. [125] Unwanted content is filtered out by locating its source and then placing a prohibition or technological barrier to access. [126] This is a preferable form of regulation which can be used in jurisdictions without the capability or resources to prevent unwanted content from being placed on the Web.

{45} Protective firewalls and encryption allow an intranet to control access to and from the Internet, eliminating unwanted activity or content. Network administrators can also ensure that certain categories of transactions occur within a specified level of access as defined by security policies and personnel responsibilities. [127] Content can also be monitored to ensure that undesirable material is either filtered or removed from the intranet. It is possible to ensure compliance with corporate policies through contractual employment agreements and forum selection clauses. [128] The use of existing forms of contracts law can be used to regulate activities and content within an intranet.

C. U.S. Approach to Regulation

{46} The United States has adopted a regulatory scheme that relies heavily on industry self-regulation. In light of the rapid rate of technological change, the U.S. balances government rules with industry self-regulation since developers are better suited to anticipate and understand the needs of the technology. Already industry leaders are working to take measures against unwanted content on the Internet. [129] However, Congress may no longer be comfortable with a secondary role to industry self-regulation, as evidenced by the passage of the NET Act. [130]

VII. INTERNATIONAL OUTLOOK FOR THE INTRANET

A. International Agreements or New International Legal Regime?

{47} In the European Union, a similar approach has been adopted, mixing governmental and self-regulation. There is a stronger tendency towards governmental regulation within the EU which has a central body for dealing with regulatory matters, the European Commission, which administers and adjudicates disputes, including those which might deal with the telecommunications and information technology. [131] On the other hand, although some countries do not have legislation which addresses the growth of information technologies, they are rapidly moving towards enacting laws which facilitate protection. For example, the Argentine Supreme Court recently upheld a lower court ruling which stated that existing copyright laws in that nation did not protect software. [132] However, pressure from high technology firms has brought rapid attention to the passage of new legislation to govern software. [133] A new copyright law which governs software has passed the lower house and is before the Argentine Senate awaiting passage, with reassurances of strong support from President Raul Granillo Ocampo. [134]

{48} There have been several international agreements which indirectly affect cyberspace and intranets. For example, in February of 1997, the WTO Agreement on Telecommunications Services was negotiated to open national telecommunications markets around the world to privatization and foreign investment, encouraging development of the GII. [135] The development of a telecommunications infrastructure and services will allow a greater penetration rate of Internet access in the international realm. None of the existing agreements directly confront intellectual property issues of the Internet

directly. [136] The North American Free Trade Agreement (NAFTA) of 1993 and the General Agreement on Tariffs and Trade (GATT) of 1994 do not provide guidance for resolving specific intellectual property issues in cyberspace, with the exception of the Trade-Related Aspects of Intellectual Property Rights (TRIPs). [137] Intellectual property rights are not significantly altered by these agreements, since the Agreement and existing laws can be used to coordinate international protection. International organizations are beginning to understand the issues involved with the Internet and, rather than create an entirely new body of law, discussions have been opened for treaty negotiations to establish uniform treatment of intellectual property rights on the Internet. [138] The WTO, which negotiated the Agreement on Telecommunications Services under the General Agreement on Trade in Services (GATS), will address the impact of telecommunications services, digital convergence and the Internet on intellectual property rights. The next round of negotiations will be a significant attempt to provide uniform standards for Internet services and regulations. During these negotiations, the WTO will confront several important issues concerning trade regulations, the Internet and the growth of electronic commerce. Other international organizations such as the World Intellectual Property Organization (WIPO) and the ITU are also struggling to provide rules and regulations for other aspects of cyberspace, including intranets.

{49} In 1996, the WIPO met in Geneva, Switzerland to address issues concerning copyright infringement over the Internet. [139] Unfortunately, differences in the application of copyrights to electronic databases between the United States and the European Union led to an inability to reach an agreement. [140] The conference ended without resolution and today the subject of whether to extend copyright protection to electronic databases is still unresolved. [141] Another example is the ITU, which assumed overall responsibility for resolving the international Domain Name System (DNS) registration dispute in 1997. [142] The Generic Top Level Domain Name Memorandum of Understanding or GTLD-MOU is the agency responsible for establishing a new international framework to replace and expand the original system created by NSI. [143] It faces a difficult task, especially in light of the fact that two previous agencies were dissolved after their failure to reach a proposal. [144]

{50} The pressure is increasing with the expansion of electronic commerce and very little progress has been made toward establishing international cooperation in terms of providing some manner of uniform treatment of cyberspace. Various international bodies are struggling with individual issues of cyberspace, but a single international governing body needs to be appointed to supervise these efforts. The United Nations or NATO have been proposed bodies in the areas of patents and copyrights, but the imbalance in intellectual property rights between the U.S. and the EU create unique tensions. [145] However, intranets can provide a different aspect on the technology and allow existing laws to govern cyberspace, rather than attempt to create an entirely new regime. If a new international legal regime were to be created, by whose or what nation's norms would the standard be set? [146] If a form of cyber common law were established, what would guarantee virtual compliance in the international context or determine whether a particular nation would look to this law rather than its own? National governments would tend to rely upon existing domestic laws to handle disputes which fall within its "borders," using intranets and forum selection clauses to resolve conflicts of law. "Cyberalty" would add to the already intolerable chaos, creating more problems by introducing a new body of law rather than focusing existing laws and clarifying their application to new technologies.

{51} Continued inflexibility in drafting international agreements to help resolve conflicts of law will only stifle the economic and social potential of the Internet. Intranets facilitate these agreements because they provide entities which can be held accountable for specific actions in cyberspace. The creation of another legal regime might extend an already chaotic situation by forcing other nations to either adopt or refuse to recognize this new form of law. Given the current trend of Internet law, the latter position is

more likely to occur. The difficulty and impracticality associated with creating a new form of law and jurisprudence for cyberspace, much in the same way as admiralty is the law of the sea, is enormous. The rapid growth of telecommunications infrastructure, information technology and the Internet will not abate thus requiring, at a minimum, an international regulatory framework for cooperation. The law cannot keep up with the rate of change of technology. It is almost unconscionable to think of changing the law with every new or major shift in technology which affects society as deeply as the Internet has. Without predictable applications of existing national laws, the potential of the Internet will be prevented from reaching its maximum success.

VIII. CONCLUSION

{52} Intranets reduce the anarchy of the Internet by providing certain outcomes and parties. The explosive growth of electronic commerce and intranets are transforming the Information Superhighway into a cyberspace ocean with virtual islands everywhere. These islands are the intranets, representing businesses, organizations and individuals selling, buying or offering goods and services on the Internet. Soon the islands will grow to the size and scope of continents, connected by the countless strands of the Internet. Although it is founded on Internet technologies, an intranet does not represent many of the same concerns as to conflicts of law or how to effectively protect on-line intellectual property. Existing forms of contracts and torts law, using employment and licensing agreements, "web-wrap" licenses and forum selection clauses settle the uncertainties of the Internet. Employing intranets provides particular locations and parties for transactions to be conducted on the Internet. There is no uncertainty in determining where a transaction took place or who was a party to the action itself. Although the technology may alter the shape of the Internet in the years to come, it is certain that intranets will be an integral part of it.

{53} Ultimately, the disparity between the intellectual property laws of the United States and the European Union must be resolved. An international oversight committee must be appointed and the GII must be built from existing national telecommunications networks. It appears to be a mammoth task, but electronic commerce has guaranteed that the Internet is here to stay with the foundations of the Next Generation Internet. The fundamental task of governing cyberspace is no more difficult than it was for the advent of telecommunications, broadcast television or the airplane. Intranets will help make the task easier by understanding the patterned effects of a new technology rather than by trying to study the minutiae of the technology itself. With the proper perspective and proper objectives, international cooperation and a uniform application of laws, the legal regime of cyberspace can be reduced to a stable, reliable source of freely exchanged ideas and information.

ENDNOTES

[1] "Cyberspace" is a term used to describe the medium of the Internet, which was first introduced in the science fiction novel, NEUROMANCER 51 (1984), by William Gibson. It is now used to refer commonly to the Internet and the electronic information medium.

[2] *See* Robert E. Calem, *Injecting Order Into Anarchistic Global Intranets*, INTRANET WORLD (last modified March 1, 1996) http://internetworld.com/print/1996/03/01/intranet/injecting.html.

[3] Steven L. Telleen, *IntraNet Methodology* (visited Nov. 28, 1997) http://www.amdahl.com/doc/products/bsg/intra/concepts1.html.

[4] *See* RANDY J. HINRICHS, INTRANETS, WHAT'S THE BOTTOM LINE? 11-12 (1997).

[5] *See Reno v. American Civil Liberties Union*, 117 S.Ct. 2329, 2334 (1997), *aff'd* 929 F.Supp. 824 (E.D. Pa. 1996).

[6] *See* G. Burgess Allison, *A Primer on Intranet Methodology*, AMERICAN BAR ASSOCIATION (last modified August 1996)

[7] *See* HINRICHS, *supra* note 4, at 79; *see also Firewall & Virtual Private Network*, UNIVERSITY OF OKLAHOMA (last modified Nov. 1, 1997) http://www.busn.ucok.edu/tips/info_hrd/firewall.htm.

[8] *See Id.*

[9] *See Id.*; *see also*, Allison, *supra* note 6; *What the 'Intranet' Really Means*, SUNWORLD ONLINE (last modified July 1, 1996) http://www.sunworld.com/sunworldonline/swol-07-1996/swol-07-connectivity.html; H. Waverly Deutsch et al., *Computing Strategies* (last modified July 1, 1996) http://access.forrester.com/index-bin/d?s%29%3Akind%29%29&TYPE=reportX#toclink1.

[10] The term "evolution" refers to the level of complexity and not to historical developments.

[11] *See* HINRICHS, *supra* note 4, at 12-13.

[12] *See Id.*

[13] *See Id.*, at 13.

[14] *See Id.*

[15] *See Id.*

[16] *See Id.*

[17] *See Id.*

[18] *See Intranets Redefine Corporate Information Systems*, NETSCAPE INTRANET WHITE PAPER, (visited Nov. 11, 1997) http://home.netscape.com/comprod/at_work/white_paper/indepth.html.

[19] *See* HINRICHS, *supra* note 4, at 13.

[20] *See Id.*

[21] *See Id.*

[22] *See Id.*

[23] *See* BRUCE A. LEHMAN, INTELLECUTAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 130-131 (1995); Lee Tuthill, *GATS Negotiations and Future Telecom Services* (visited Oct. 3, 1997) http://www.globalcomms.co.uk/interactive/development/legal/56.html (senior staff member of WTO discussing upcoming GATS negotiations in 2000 regarding market access for telecommunications and Internet services); *Geneva WIPO Copyright Conference Winding Down Amidst Disagreement Over Cyberspace Reproduction Rights*, Dec. 23, 1997, *available in* WESTLAW, Text and Periodical Library,

West's Legal News File.

[24] *See* HINRICHS, *supra* note 4, at 118-119.

[25] *See Id.*, at 115.

[26] *See* Adam L. Penenberg, *Info-Terror*, FORBES DIGITAL, (last updated Oct. 10, 1997) http://www. Forbes.com/tool/html/97/oct/1010/colb.htm.

[27] *See Id.*

[28] *See* G. A. Keyworth, II and David E. Colton, *The Computer Revolution, Encryption and True Threats to National Security*, (last modified June 1996) http://www.townhall.com/pff/encry.html.

[29] *See Id.*

[30] *See Id.*

[31] *See Id.*

[32] *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution* , 143 U. PA. L. REV. 709, 764-767 (1995). (author discusses several previous legislative and regulatory attempts to specifically control encryption, including the Escrowed Encryption Standard, or EES, and the Clipper Chip, the failed federal encryption chip).

[33] *See Id.*, at 735.

[34] *See Id.*, at 736.

[35] *See Id.* at 812.

[36] *Accord Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969).

[37] *See Id.*

[38] *See DeFilippo v. National Broadcasting Co., Inc.* , 446 A.2d 1036, 1039-1040 (R.I. 1982); *see also Weirum v. RKO General, Inc.* , 15 Cal.3d 40 (1975).

[39] *See* Matthew R. Burnstein, Note, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 VAND. J. TRANSNAT'L L. 75, 93 (1996).

[40] International Emergency Economic Powers Act of 1977, 50 U.S.C. § 1701 et seq. (1991).

[41] Exec. Order No. 12, 924, 59 Fed. Reg. 43,437 (1994).

[42] *See $600M To Double NASDAQ Capacity*, WIRED NEWS, Nov. 20, 1997, at http://www.wired.com/news/business/story/8678.html. (The NASDAQ stock market contracted for an intranet outsourcing development project for a 6-year upgrade of the network to be able to manage 4 billion shares of trading in a single day).

[43] *See Id.*; *see also*, David Bank, *Netscape to Buy 'Extranet' Concern for $180 Million*, THE WALL STREET JOURNAL, Nov. 25, 1997, at B9.

[44] *See Engineers Take Virtual Tinkering to Next Level*, WIRED NEWS, Nov. 7, 1997, at http://www.wired.com/news/news/technology/story/8392.html.

[45] *See* HINRICHS, *supra* note 4, at 41.

[46] *See* Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L.& PUB. POL'Y 475, 478 (1997).

[47] *See Andreessen: Netscape Browser Slide Will Stop*, WIRED NEWS, Dec 2, 1997, at http://www.wired. com/news/news/business/story/8891.html.

[48] *See National Telecommunications and Information Administration (NTIA) Information* (last modified Oct. 1997) http://www.ntia.doc.gov/ntiahom/about97.htm. (statistical compilation of data regarding information technology industry and expected growth of electronic commerce, domestic and international).

[49] *See Id.*

[50] *See Intranets Redefine Corporate Information Systems*, NETSCAPE INTRANET WHITE PAPER (visited Nov. 11, 1997) http://home.netscape.com/comprod/at_work/white_paper/indepth.html.

[51] *See Id.*

[52] *See* Bank, *supra* note 43, at B9.

[53] *See generally* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat.56 (to be codified at scattered sections of 47 U.S.C.). (Further discussion of the effect of privatization, the Telecommunications Act of 1996 and topics such as long-distance and local carriers cross competing is held off in that this represents an independently significant topic which is tangential to the present discussion.)

[54] *See* David Bank, *TCI in Talks Over new Cable-TV Boxes*, THE WALL STREET JOURNAL, Dec. 15, 1997, at A3. (Microsoft, a large technology and software company, is attempting to provide computer and Internet access via cable systems, refining the focus on convergence).

[55] *See Id.*

[56] *See* George McGrath and Anthony Schneider, *Measuring Intranet Return on Investment*, INTRANET COMMUNICATOR, June/July 1997, at http://www.intrack.com/intranet/ireturn.html.

[57] *See Id.*

[58] *See* Ian Campbell, *The Intranet: Slashing the Cost of Business*, INTERNATIONAL DATA CORPORATION (visited Nov. 30, 1997) http://home.netscape.com/comprod/announce/idc/summary.html.

[59] *See Id.*

[60] *See Id.*

[61] *See Id.*

[62] *See Lockheed Martin Corporation ROI Survey*, INTERNATIONAL DATA CORPORATION, (visited Nov. 30, 1997) http://www.highsoft.com/Netscape/WHITEPPR/Roi.htm.

[63] *See Id.*

[64] *See Id.*

[65] *See* HINRICHS, *supra* note 4, at 37-41.

[66] *See Id.*

[67] *See Id.*

[68] *See Id.* at 115.

[69] *See* Calem, *supra* note 2.

[70] *See Id.*

[71] *See* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1029 (1994).

[72] *See Id.*, at 1029-30.

[73] *See generally* Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).

[74] *See* HINRICHS, *supra* note 4, at 117.

[75] TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA, U.S. DEPARTMENT OF DEFENSE (last modified Dec. 26, 1985) http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html.

[76] Id. at § 4.1.

[77] Id. at § 2.1.

[78] *See* HINRICHS, *supra* note 4, at 115.

[79] *See Id.* at 116.

[80] *See* Hardy, *supra* note 71, at 1028.

[81] *Gottschalk v. Benson*, 409 U.S. 63 (1972); *see also* Patent Act of 1952, 35 U.S.C. § 101 et seq. (1952).

[82] *See Arrhythmia Research Technology, Inc. v. Corazonix Corp.* , 958 F.2d 1053 (Fed. Cir. 1992).

[83] *See* 35 U.S.C. § 101.

[84] *See What is E-Business?* (visited Feb. 13, 1998) http://www.ibm.com/e-business/what/.

[85] *See Diamond v. Diehr*, 450 U.S. 175, 184 (1981).

[86] Copyright Office Regulations, 37 C.F.R. § 202.20 (1977).

[87] *See* 17 U.S.C. § 504.

[88] *See* 17 U.S.C. § 304.

[89] 17 U.S.C. § 101 et seq. (1976).

[90] *See* 17 U.S.C. § 102 (a).

[91] *Lotus v. Borland*, 49 F.3d 807, 815 (1st Cir. 1995); *aff'd by equally divided court*, 116 S. Ct. 804 (1996).

[92] *See Id.*, at 815.

[93] *See Id.*, at 819.

[94] *See* 499 U.S. 340, 349 (1991).

[95] *See Id.* (The "Sweat of the Brow" doctrine was originally designed to provide a proprietary interest in facts by rewarding authors who labored to compile facts, such as large collections of statistics. However, the doctrine is considered ineffectual in that copyright protection is given under the standard of original authorship which may include the selection and arrangement of facts, but not the facts themselves).

[96] *See Id.*

[97] *See Id.*

[98] *See* Copyright Office Regulation, 37 C.F.R. § 202.20 (1977).

[99] *See Id.*

[100] *See Clinton Signs Law Closing Electronic-Theft Loophole*, THE WALL STREET JOURNAL, Dec. 18, 1997, at B12; *see also Industry 1, Academics 0: Clinton Signs Copyright Bill, WIRED NEWS*, Dec. 17, 1997, at http://www.wired.com/news/news/email/other/politics/story/9236.html.

[101] *See Id.*

[102] *See Id.*

[103] *See* 17 U.S.C. § 107.

[104] *See* 17 U.S.C. § 506 (a).

[105] *See* GALE R. PETERSON, TRADE SECRETS IN AN INFORMATION AGE § 2.1 (1997).

[106] *See* HINRICHS, *supra* note 4, at 118.

[107] *Accord Id.*

[108] *See* 409 U.S. at 70.

[109] *See Id.*

[110] 35 U.S.C. § 112.

[111] *See* PETERSON, *supra* note 105.

[112] *See ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1452 (7th Cir. 1996). (shrink-wrap licenses are enforceable subject to standard contracts law provisions).

[113] *See generally* Lawrence Lessig, *Symposium: Emerging Media Technology and the First Amendment: The Path of Cyberlaw*, 104 YALE L. J. 1743 (1995). (Proposing that cyberspace should be allowed time to evolve before courts apply strict analogy to other legal areas).

[114] *See* David R. Johnson and David Post, *Law and Borders-The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1372-1373 (1996); *see also* A Proposal to Improve Technical Management of Internet Names and Addresses (draft Jan. 30, 1998) http://www.ntia.doc.gov/ntiahome/domainname/dnsdraft.htm (proposed rule promulgated by the U.S. Department of Commerce to be published in the Federal Register calling for the creation of a non-profit organization to manage the domain name registration system. The proposal calls for global representation from various Internet address groups to be appointed to the Board of Directors).

[115] *See Intermatic, Inc. v. Toeppen*, 947 F. Supp. 1227, 1239 (N.D. Ill. 1996); *But see, Lockheed Martin Corporation v. Network Solutions, Inc.* , 985 F.Supp 949 (C.D. Cal. 1997).

[116] A Proposal to Improve Technical Management of Internet Names and Addresses (draft Jan. 30, 1998) http://www.ntia.doc.gov/ntiahome/domainname/022098fedreg.htm (Domain names are identified by their particular components. For example, the .com component of a domain name is known as a generic Top Level Domain Name or gTLD. The "kokka" of "kokka.com" is referred to as an SLD or second level domain name. Currently, there are only six gTLDs in use, .com, .net., .org, .edu, .mil, and .gov. The last two are used exclusively by the federal government to designate military and government organizations. Current proposals under the Proposal or "Green Paper" call for the creation of five new gTLDs by September 30, 1998).

[117] *See* Network Solutions, Inc. Home Page (visited Dec. 16, 1997) http://www.internic.net.

[118] *See The Generic Top Level Domain Memorandum of Understanding*, (last modified Dec. 16, 1997) http://www.gtld-mou.org/; *see also supra*, note 116.

[119] 15 U.S.C. § 1051 et seq. (1995).

[120] *Accord Intermatic, Inc. v. Toeppen*, 947 F. Supp 1227 (N.D. Ill. 1996).

[121] *See generally* Thomas E. Weber, *Internet Plans Self-Regulation of the Industry*, THE WALL STREET JOURNAL, Dec. 1, 1997, at B16.

[122] *See* Timothy Wu, Note: *Cyberspace Sovereignty?-The Internet and the International System*, 10 HARV. J.L. & TECH. 647, 649-650 (1997).

[123] *See Id.*, at 649.

[124] *See Id.*, at 655; *see also* David Case, *Big Brother is Alive and Well in Vietnam-And He Really Hates the Web*, WIRED, Nov. 1997, at 164, 168.

[125] *See Wu, supra* note 111, at 655.

[126] *See Id.*

[127] *See* TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA, U.S. DEPARTMENT OF DEFENSE § 2.1-2.2.

[128] *See* Burnstein, *supra* note 38, at 101.

[129] *See* Weber, *supra* note 110.

[130] *See supra* note 91.

[131] *See* Catherine Curran Butcher, *Telecommunications in the European Union*, 48 ADMIN. L. REV. 451, 455 (1996).

[132] *See* Jonathan Friedland, *Software Makers Assail Argentine Piracy Ruling*, THE WALL STREET JOURNAL, Feb. 6, 1998, at A17.

[133] *See Id.*

[134] *See Id.*

[135] Agreement on Telecommunications Services (Fourth Protocol to General Agreement on Trade in Services), Feb. 15, 1997, World Trade Organization, 36 I.L.M. 367 (1997).

[136] *See* e-mail letter from Lee Tuthill, senior staff member for Telecommunications of the World Trade Organization to Scott Kokka (Oct. 31, 1997) (on file with author).

[137] *See* HENRY H. PERRITT, JR., LAW AND THE INFORMATION SUPERHIGHWAY § 14.2 (1996).

[138] *See* Robert Gurrola, *U.S. Info Technology Group Proposes Hi-Tech Copyright Protection Alternatives at Geneva WIPO Meeting*, Dec. 12, 1996, *available in* WESTLAW, News Library, West's Legal News File.

[139] *See Id.*

[140] *See Geneva WIPO Copyright Conference Winding Down Amidst Disagreement Over Cyberspace Reproduction Rights*, Dec. 23, 1996, *available in* WESTLAW, News Library, West's Legal News File.

[141] *See Id.*

[142] *See The Generic Top Level Domain Memorandum of Understanding, supra* note 117.

[143] *See Id.*

[144] *See Id.*

[145] *See* Rick Brennan & R. Evan Ellis, *Information Warfare in Multi-Lateral Peace Operations*, April 18, 1996 (visited Dec. 1, 1997) http://sac.saic.com/SOMALIA.HTM. (case study prepared for the U.S. Secretary of Defense which addressed the need for international cooperation and uniformity in establishing the GII).

[146] *See* Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1408 (1996) (Professor Lessig actually adopts the opposite viewpoint of this author, however he ignores the issue of who, how and on what model will "cyber common law" be formed?).
