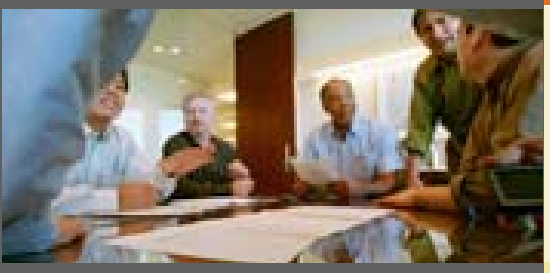
FENWICK & WEST LLP



Intellectual Property Rights on the Internet

by Stuart P. Meyer

FENWICK & WEST LLP

About the Firm

Fenwick & West LLP provides comprehensive legal services to high technology and biotechnology clients of national and international prominence. We have over 250 attorneys and a network of correspondent firms in major cities throughout the world. We have offices in Mountain View and San Francisco, California.

Fenwick & West LLP is committed to providing excellent, cost-effective and practical legal services and solutions that focus on global high technology industries and issues. We believe that technology will continue to drive our national and global economies, and look forward to partnering with our clients to create the products and services that will help build great companies. We differentiate ourselves by having greater depth in our understanding of our clients' technologies, industry environment and business needs than is typically expected of lawyers.

Fenwick & West is a full service law firm with "best of breed" practice groups covering:

- Corporate (emerging growth, financings, securities, mergers & acquisitions)
- Intellectual Property (patent, copyright, licensing, trademark)
- Litigation (commercial, IP litigation and alternative dispute-resolution)
- Tax (domestic, international tax planning and litigation)

Intellectual Property Group

Fenwick & West's Intellectual Property Group offers comprehensive, integrated advice regarding all aspects of the protection and exploitation of intellectual property. From providing sophisticated legal defense in precedent-setting user interface copyright lawsuits to prosecuting arcane software patents, and from crafting user distribution arrangements on behalf of high technology companies to implementing penetrating intellectual property audits, our attorney's technical skills enable the Firm to render sophisticated legal advice.

Our Offices

Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel: 650.988.8500
Fax: 650.938.5200

Embarcadero Center West
275 Battery Street
San Francisco, CA 94111
Tel: 415.875.2300
415.281.1350

For more information about Fenwick & West LLP, please visit our Web site at: www.fenwick.com.

The contents of this publication are not intended, and cannot be considered, as legal advice or opinion.

FENWICK & WEST LLP

Intellectual Property Rights on the Internet

Prepared for Computer Law and the Internet '97
March 20-21, 1997, Denver, Colorado

Table of Contents

I. Introduction

The number of adults using the Internet, in the United States alone, increased from 27 million in January, 1996 to 35 million in September, 1997. *Random Notes*, 1 CYBERSPACE LAWYER, January 1997, at 12 (citing recent poll by Lou Harris & Associates). In a number of ways, this "hockey stick-like" growth of the Internet has brought a sea change in intellectual property law, *i.e.*, the law concerning copyrights, trademarks, patents, and trade secrets.

This paper will highlight some of the more important aspects of intellectual property rights as they relate to the Internet, and discuss the manner in which intellectual property law is evolving with the increased use of the Internet in society.

United States law provides four general types of intellectual property protection relevant to Internet technology: patent, copyright, trademark and trade secret. While these four categories of intellectual property overlap to some degree and coexist with other related rights not discussed in this paper, one can generally consider the four categories separately as follows:

1. **Copyright.** United States copyright law protects works of original authorship from unauthorized duplication, modification, and distribution. A maxim of United States law is that copyright protects the expression of ideas, but not the ideas themselves. Since United States accession to the Berne Convention in 1989, very few formalities are required for copyright protection to come into play; mere creation of a work gives rise to substantial rights. However, placement of a copyright notice on the work and registration of the work with the Copyright Office of the United States Library of Congress provides more complete protection. Copyright protection may last 75 years or more, depending, *inter alia*, on whether the author is a natural or legal person. Through a series of treaties, a United States copyright provides some degree of protection worldwide.

2. **Trademark.** Trademark law in the United States protects words, names, or symbols that are adopted and used by a company to identify its goods and distinguish them from those manufactured or sold by others. Unlike United States patent and copyright protection, which is derived purely from federal statutory law, trademark law obtains from both federal and state law. As with copyright law, some protection arises immediately upon adoption of a trademark, but state or federal registration is required to obtain the maximum protection. Federal trademark registration with the United States Patent and Trademark Office may be made only for marks that are currently in use or that are anticipated to be used in the near future. Assuming that periodic renewals are obtained and that the mark does not become generic, trademark protection under United States law may be perpetual. Registration of a

mark in the United States does not provide rights in other countries; such rights must be obtained separately in the countries where protection is desired.

3. **Patent.** United States patent law protects inventions that are novel, useful, unobvious and fit one of the statutory categories for patentable subject matter, *i.e.*, processes, machines, articles of manufacture, and compositions of matter. United States patent applications must be applied for in the name of the true individual inventors. The patent prosecution process in the United States Patent and Trademark Office typically takes two or three years, and a United States patent is valid for 20 years from the date the patent application was filed. A United States patent provides exclusionary rights by which others are restricted from making, using, or selling the claimed invention in the United States, but a United States patent does not confer any positive right to practice the invention upon the patent owner, nor does it confer rights in other countries.

4. **Trade Secret.** A trade secret is any device or information that is used in a business and that gives the owner an advantage over others who do not know or use it. Trade secret protection is a creature of state, rather than federal, law. While the laws of the states vary significantly, most of the states have adopted a uniform law of trade secrecy. No formal filings or registrations are required, or are even available, for trade secret protection. Trade secret protection may last indefinitely, but is lost when the information becomes generally known to the public. Because civil trade secret law is not provided on a federal basis, protection does not extend beyond the borders of the United States. A recently enacted federal criminal statute provides broader protection for certain types of economic espionage relating to commercial trade secrets.

II. Internet-Related Intellectual Property Issues

The facilities provided by the Internet, *e.g.*, international, extra-organizational electronic mail and the World Wide Web, have generated a plethora of new issues in intellectual property law. These new issues have sparked scholarly debates, various lawsuits, major legislative action, and even multinational treaty negotiations. One need only review a sampling of the recent literature to understand that Internet legal issues are currently the subject of a great deal of thought and discussion. *See, e.g., Special Issue: Harvard Conf. on the Internet and Society*, 10 HARVARD J. LAW & TECH. (Fall 1996).

A. Copyright Issues Related to the Internet

The technology of the Internet provides a new medium for dissemination of information, and this new medium presents numerous challenges to traditional norms of copyright law.

Most fundamentally, the Internet provides a means of nearly effortless and essentially perfect duplication and dissemination of works such as texts, pictures, audio-visual

material, and other authorship for which copyright law provides certain exclusive rights to owners. Like the videotape recorder and photocopier technologies that preceded it, the technology of the Internet has led to widespread revisitation of the public policy underpinnings of copyright law.

1. The White Paper

The 1992 Clinton/Gore presidential campaign had as one of its goals the promotion of a National Information Infrastructure, more commonly known by nicknames such as the "Information Superhighway" or the acronym NII. In essence, the backbone of the NII was envisioned to be, and remains, the Internet. In order to promote this aspect of the President's agenda, a working group was formed by the late Secretary of Commerce Ron Brown. The group was headed by Commissioner of Patents and Trademarks Bruce Lehman, and was charged with informing Executive Branch decisionmaking on issues pertaining to intellectual property and the NII. The culmination of this group's work was the White Paper, actually entitled INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE, which was released in its final form in September, 1995.

Although purporting to cover the whole gamut of intellectual property issues pertaining to the NII, the White Paper devotes 135 of its 237 pages to copyright analysis, compared with only ten pages for patents, five for copyright, and four for trade secrets. The remainder of the White Paper addresses issues such as technology, education, and recommendations.

The need for a document such as the White Paper is aptly demonstrated in the White Paper by reference to forebears who also had to deal with difficult intellectual property issues. The White Paper cites, for instance, an 1841 opinion by Justice Story characterizing intellectual property not only as "subtile," but as the metaphysics of law. The White Paper also quotes Thomas Jefferson on the danger of allowing intellectual property law to remain stagnant in changing times: "We might as well require a man to wear still the coat which fitted him when a boy . . . ."

There is general agreement that a detailed treatment of computer copyright such as is found in the White Paper would be helpful in these changing times, but the particular analysis provided in the White Paper has been the subject of heated debate. It has widely been suggested that the White Paper reflects more Mr. Lehman's views as a former lobbyist for the Software Publishers Association than a neutral analysis of what the law should be.

There is little question that the White Paper favors copyright holders. For example, the treatment it provides of the "fair use" doctrine that allows copying in some circumstances gives scant recognition of the seminal Supreme Court case of *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), and only grudgingly admits that this decision adopted the "substantial noninfringing use" test from patent law to consider whether Sony was a contributory infringer by providing the machine (the Betamax videotape recorder) for

copying. The White Paper's primary citation to the *Sony* case is for the ancillary proposition that copying for commercial uses is presumptively unfair.

Similar treatment is given to the first sale doctrine, which allows parties purchasing a copy of a work to subsequently transfer that work, such as by selling a book at a garage sale. The White Paper suggests that such doctrine should not apply in Cyberspace (*i.e.*, the environment provided by the Internet), because the mechanism of transfer inherently involves some reproduction of the work, however fleeting. Thus, under the approach advocated by the White Paper it is impermissible to electronically transfer one's copy of a software work to another even if the original owner does not retain any copies, although a transfer of the work by "sneaker-net" (*i.e.*, by personally delivering the disk containing the work) would be allowable.

Another issue addressed by the White Paper is whether online service providers should be held liable for copyright infringements caused by their subscribers' postings. The White Paper answers in the affirmative, reasoning that "They, and only they, are in the position to know . . . their subscribers and to stop unlawful activities." The White Paper concludes that, "Between these two relatively innocent parties [providers, authors], the best policy is to hold the service providers liable." A number of decisions during the past year, some of which are discussed below with respect to defamation issues, have shown that this is an area of extensive debate, with one side seeing as perfectly reasonable what the other sees as draconian.

Aside from its analysis of copyright law, the White Paper is interesting for its extended treatment of "steganography" and other mechanisms for "copyright management," *i.e.*, various technical methods of detecting and preventing copyright infringement. The White Paper suggests matter-of-factly that there should be legal prohibitions against obviating such protection schemes, but does not address the problems that would arise when copyright management mechanisms are used to prevent fair use copying, or copying of works in which copyright has expired.

Even presumably mild suggestions in the White Paper for an educational "Copyright Awareness Campaign" have met with criticism for being one-sided, ignoring the importance of teaching children to share their work with others, and suggesting that the notion of "fair use" is too complicated to be taught until later in a child's education.

The premise of the White Paper is that the Internet provides a machine made to copy, and that copyright owners therefore need enhanced protection. Whether this premise is right or wrong, and regardless of whether the White Paper is neutral or biased, it has provided an unparalleled engine for debate among legal scholars and industry participants.

Among the recommendations provided by the White Paper is a suggestion that copyright law be updated in various ways to reflect the importance of the NII to society. Specifically, the White Paper advocates the establishment of a new "distribution" right for electronic transmission, in addition to thecopying/distribution/public display rights provided under current law. The White Paper also recommends extending the notion of "publication" to include electronic distribution rather than just distribution of tangible copies as is presently the case. Other recommendations include the prohibition against obviating copyright management schemes as discussed above and other suggestions concerning, *e.g.*, the extent to which libraries may make copies, and incentives for making special versions of works for the visually impaired.

2. The WIPO Negotiations

In late 1996, the United States sent Patent Commissioner Lehman to a diplomatic conference of the World Intellectual Property Organization (WIPO). The diplomatic conference lasted for most of the month of December, included representatives of approximately 160 countries, and was specifically intended to address issues of how the Internet and other digital technologies impacted copyright law. The conference resulted in adoption of two proposed treaties and likely consideration in the near term of a third, and will be the subject of intense scrutiny and debate in the United States and abroad over the coming year. *See, e.g.*, 11 WORLD INTELLECTUAL PROPERTY REPORT (February 1977) at 55.

The WIPO Copyright Treaty adopted at the conference is particularly notable in its overall consistency with the approach taken by the White Paper. For instance, the treat explicitly recognizes computer programs as literary works, provides protection for compilations of data, and declares the right of a copyright owner to control electronic distribution of the owner's work to the public.

However, there was some dissension with the U.S. proposals. For instance, a proposed article extending a copyright owner's rights to "reproduction . . . whether permanent or temporary" was deleted. Such a provision arguably would allow copyright owners to prevent licensees from using third parties (known as Independent Service Organizations or ISOs) to perform maintenance on their systems, and also could be construed to limit "web-surfing," *i.e.*, browsing World Wide Web sites. *See, e.g., MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993) (temporary copy made in RAM by unauthorized maintenance provider was infringing). The measure was deleted despite the objection of the United States, but the U.S. was able to include in the conference records a statement of agreed understanding on this point, so it is likely to be revisited either at the treaty level or in national legislation. Interestingly, there does not appear to be consensus on this issue within the United States, as legislation has recently been proposed that would specifically allow computer owners to have ISOs perform such maintenance without fear of infringement. See, Computer Maintenance Competition Act of 1997 (HR72), Cong. Rec., January 7, 1997 at E21 (sponsored by Representative Knollenberg). As to Web browsing, even

if copies made in the course of such browsing are determined to be subject to copyright law, the doctrines of fair use and implied license will in many cases prevent copyright owners from asserting that such browsing constitutes actionable infringement.

The other adopted treaty, known as the Performance and Phonogram Treaty, also included some departure from the U.S. position. For example, rights under this treaty are to be granted not only to performances but to the performers of such performances as well.

A third treaty, known as the Database Treaty, involves the protection of database contents. WIPO was unable to adopt this controversial treaty during this conference, and it has been held for future consideration. This treaty, if put into place, would significantly change U.S. copyright law, which does not currently extend protection to the factual matter in databases per se, although the selection, arrangement, and coordination of such data may be protected.

Full details concerning these treaties can be found at the WIPO Web site, http://www.wipo.org.

3. Legislative Developments

Debate on legislation to implement some of the changes proposed in the White Paper commenced in February 1996 and is ongoing. No doubt, developments at the WIPO diplomatic conference will impact such legislation. As of this writing, no bill has yet been presented to the President for signature, but some amendment to the copyright act in the coming year is likely according to many commentators. *See, e.g.*, John Gibeaut, *Zapping Cyber Piracy*, 83 ABA JOURNAL, February 1997, at 60; Rory J.O. O'Connor, *Tech Debate Takes New Turn*, San Jose Mercury News, January 13, 1997, at 1E.

4. Lawsuits

Numerous legal actions have been brought involving Internet issues, and the pace seems to be accelerating. Of particular interest is a set of copyright actions recently brought by software publishers against Internet service providers (ISPs) and Internet users. *See, Let the Litigation Begin: Software Publishers Go to War Against the Internet*, 4 INFORMATION L. ALERT (October 25, 1996) at 1. As reported therein, the Software Publishers Association, on behalf of Adobe Systems, Claris, and Traveling Software, has filed suit against Web companies whose users allegedly provide means for software piracy over the Internet. Such means include serial numbers that will make operable commercial software otherwise protected from use by non-licensees, programs that obviate such protection schemes, and links to Internet "FTP" sites where piratical versions of commercial software are available. These actions apply a theory of "contributory" or "vicarious" liability for copyright infringement, in which the defendant may not be the person who directly infringes a copyright.

The issue of contributory infringement for ISPs and bulletin board operators has been addressed before, with the result that in some circumstances, these parties may be held liable for infringement if they knew that infringing works were being uploaded on their systems and refused to remove them. *See, e.g., Religious Technology Ctr. v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995), *Sega Enterprises Ltd. v. MAPHIA*, 857 F. Supp. 679 (N.D. Cal. 1994); *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993).

B. Trademark and Related Issues

It is now becoming general knowledge that people, businesses and other organizations are accessible to one another over the Internet by particular email or World Wide Web addresses, known as "domain" names. Because of the unstructured nature of the Internet and particularly the Web, users often locate organizations by searching for domain names that correspond to the organization's name. For example, most Web addresses for U.S. businesses begin with the prefix http://www. and end with the suffix.com . Thus, one looking for the Web site for International Business Machines Corporation might try looking at the address http://www.ibm.com. It has also become common practice for businesses to use addresses that describe the products that they sell. For instance, a manufacturer of canoes might adopt the address http://www.canoe.com or the like.

Not surprisingly, numerous disputes have arisen where companies with similar names, or manufacturing the same types of products, have wanted to adopt similar or identical domain names. This development has recently catapulted the organization responsible for registration of Internet domain names, InterNIC, and Network Solutions, Inc. ("NSI"), a company under contract with the National Science Foundation to operate InterNIC, to the forefront of a very heated and public debate. As a result, InterNIC made revisions to its policy for name registrations to require applicants for a domain name to assert that they have a legal right to use that name. This may help to resolve some disputes, such as arose when Hasbro Inc., the manufacturer of the "Candy Land" game sought and obtained injunctive relief against Internet Entertainment Group, which was using candyland.com for adult entertainment. *Hasbro, Inc. v. Internet Entertainment Group, Ltd.*, 40 U.S.P.Q.2d (BNA) 1479 (W.D. Wash. 1996). Unfortunately, the InterNIC registration policy may not address issues that arise where two similarly named organizations desire the same domain name, as in the case where Fry's Electronics in California and Frenchy Frys in Washington went to battle for the domain name frys.com. *Fry's Electronics v. Octave Systems*, C95-2525 (N.D. Cal., filed July 13, 1995).

The tensions caused by the InterNIC registration policies have resulted in several lawsuits being brought against NSI. *Roadrunner Computer Systems, Inc., v. Network Solutions, Inc.*, Civ. Dkt. 96-413-A (E.D. Va., filed March 26, 1996); *Data Concepts Inc. v. Digital Consulting Inc. and Network Solutions, Inc.*, 96-CV-429 (M.D. Tenn., filed May 8, 1996); *Giacalone v. Network Solutions, Inc.*, C96-20434 (N.D. Cal., filed May 30, 1996). Much more exhaustive

treatments of these trademark issues are provided in numerous sources, *e.g.*, Note, *Trademark Law Lost in Cyberspace: Trademark Protection for Internet Addresses*, 9 HARV. J. L. & TECH 483 (1996) (authored by Kenneth Sutherlin Dueker). Here, we will explore but two of the more interesting areas: trademark dilution and the development of related defamation and objectionable communications standards.

1. Trademark Dilution

The *Hasbro* decision mentioned above relied in part on a recently enacted federal law that prevents the "dilution" of certain marks even in the absence of "likelihood of confusion" (a prerequisite for conventional trademark infringement liability). The Federal Dilution Act protects famous trademarks from being used in a manner that "causes dilution of the distinctive quality of the famous mark." 15 U.S.C. § 1125.

Application of this law, or of equivalent state laws, to domain name disputes has been made in several subsequent cases. For example, in *Intermatic Inc. v. Toeppen*, 40 U.S.P.Q.2d (BNA) 1412 (N.D. Ill. Oct. 3, 1996), the court held that defendant's registration of the domain name intermatic.com with the intent to sell it to the plaintiff or some third party was a commercial use that diluted the value of the plaintiff's Intermatic trademark. In addition, the court held that the mere existence of this mark on defendant's Web pages "inexorably" would have an adverse effect on plaintiff's mark. The court not only enjoined defendant from using the domain name, but in an extraordinary move ordered that the domain name be transferred to the successful plaintiff. The same defendant was enjoined from using the domain name panavision.com based on similar reasoning by another court. *Panavision Int' l L.P. v. Toeppen*, 938 F. Supp. 616 (C.D. Cal.), *summ. j. granted in part*, 945 F. Supp. 1296 (C.D. Cal.); *summ. j. granted* , 41 U.S.P.Q.2d (BNA) 1310 (C.D. Cal. 1996). That court additionally recognized that such use of domain names taken from famous trademarks injures consumers by making it difficult to find the trademark owner's Web site.

Still another case involving dilution of trademark over the Internet came about when the domain name adultsrus.com was registered and used to sell sexual devices over the Internet. The plaintiff, owner of the "R US" family of trademarks (*e.g.*, Toys R Us) prevailed in obtaining an injunction against defendants use of this domain name. *Toys "R" Us Inc. v. Akkaoui*, 40 U.S.P.Q. 2d (BNA) 1836 (N.D. Cal. 1996).

The use of domain names similar to trademarks has been dubbed "Cybersquatting." *See, e.g., New Dilution Act Used to Evict ëCybersquatters'* , NAT. L. J., January 27, 1997, at C3. The Cybersquatting problem has been exacerbated by the fact that, unlike the provisions of trademark law allowing different types of products to carry the same mark, generally there is only one entity that can use a particular domain name. While different types of organizations can use different suffixes to distinguish otherwise similar domain names, such distinction is extremely limited. For example, U.S. businesses generally must use the suffix .com as their

"top level domain name," and the other registrable top level domain names, such as .edu (educational institutions), .org (organizations such as non-profits), .mil ((military); .gov (government) and so forth are not available for businesses. Thus, there can be only one fenwick.com domain name, even if there are numerous businesses with the term "Fenwick" prominent in their name. This situation may be ameliorated in the near future, as the Internet Ad Hoc Coalition has announced that seven new top level domain names will be put into use in coming years. Those include .firm (for businesses or firms), .store (for businesses offering goods to purchase), .web (World Wide Web related activities), .arts (arts and entertainment), .rec (recreation), .info (information services), and .nom (individual or personal nomenclature). Further information is available through the IAHC web site at http://www.iahc.org.

2. Defamation, Offensive and Indecent Communications

In a related area, the increased use of email and the World Wide Web in recent years has led to a widely publicized increase in distribution of offensive communications. A sociological phenomenon, now the subject of renewed interest with the advent of Cyberspace as a popular communications medium, is that moral norms in interpersonal relationships tend to deteriorate as the mode of communications becomes less intimate. For example, it is well recognized that the tone of email communications is much more cavalier, and oftentimes less circumspect, than corresponding face-to-face communications would be. A new verb, "flame," has even developed concerning such communications that are particularly harsh. Thus, the law firm of Canter & Siegel was flamed by thousands of Internet users after it posted an advertisement for its services on the Internet. Brian G. Gilpin, *Attorney Advertising and Solicitation on the Internet: Complying with Ethics Regulations and Netiquette*, 13 JOHN MARSHALL J. COMPUTER &AMP INFO. L. 697 n.7 (Summer 1995). For whatever reasons, common courtesies typically exhibited in face-to-face discussions are often ignored in non-verbal electronic communications.

Regardless of the cause, the growing use of the Internet as a communications medium has resulted in increased litigation concerning defamation and other types of objectionable communications. A particularly vexing issue involves the liability of ISPs and other online service providers for the acts of their users.

For defamation to be found, the speaker generally must be found to have an intent to defame. Damage to the injured party is typically presumed, and the burden is upon the speaker to prove the truth of the statement to avoid liability. Distributors of defamatory material are liable only if they know or had reason to know that the material was defamatory before distributing it. *See, e.g., Auvil v. CBS "60 Minutes"*, 800 F. Supp. 928, 931-32 (E.D. Wash. 1992). Publishers, however, are deemed liable for defamatory material published either with knowledge of falsity, or with reckless disregard as to truth or falsity. *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964). Thus, publishers are traditionally held to a higher standard than are distributors in defamation cases.

A difficult decision for courts in recent years is whether online service providers should be treated as distributors or publishers for defamation analysis. In *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp 135 (S.D.N.Y. 1991), the court agreed with defendant's argument that it was more like a distributor than a publisher, since it exercised no control over content. However, another court faced with a similar situation in *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct., May 24, 1995) held that another online service provider, Prodigy, should be treated under the more strict standard of a publisher.

Partially in response to the *Stratton Oakmont* decision, Congress included as part of the recent Communications Decency Act ("CDA") a "good Samaritan" provision mandating that online service providers not be treated as publishers, and further protecting online service providers from any liability that might result from screening or blocking objectionable content from their facilities. CDA § 230(c), Pub. L. No. 104-104, 110 Stat. 133 (1996), to be codified at 47 U.S.C.

The CDA is but one portion of a much more comprehensive piece of legislation known as the Telecommunications Act of 1996, signed into law by President Clinton on February 8, 1996. The Telecommunications Act brought about many sweeping changes in U.S. telecommunications law, including changes in telephone, cable and broadcast laws. The CDA portion of the Act is particularly relevant as it prohibits obscene transmissions and displays over the Internet by means of interactive computer devices and telecommunication devices and is widely viewed as Congress's response to public uproar over pornography available on the Internet. Enforcement of portions of the CDA has now been blocked by injunctions from lawsuits brought by the American Civil Liberties Union and others; the Supreme Court has agreed to hear this issue. *Reno v. ACLU*, 117 S.Ct. 516 (1996); *Shea v. Reno*, 930 F. Supp. 916 (S.D.N.Y. 1996).

C. Patent Law and the Internet

Unlike the copyright and trademark issues brought to the fore by the rising popularity of the Internet, fundamental patent law norms are not subject to challenge by the Internet. To be sure, the Internet's popularity has spawned tremendous interest in certain patents related to enabling technology for the Internet, but the emergence of this new medium is generally considered as something that the patent law can take in stride. For example, the White Paper did not propose any changes to the patent law to address technologies related to the National Information Infrastructure. The primary development in Internet-related patent issues has come not from the courts or legislature, but from the Patent and Trademark Office. Specifically, the PTO has revised its guidelines for examination of computer-related inventions and has also issued guidelines for handling "design" patent applications for computer display icons (*e.g.*, the icon of a trash can that is used to discard or delete unwanted files). These developments bode will for increased protection of Internet-related inventions.

1. The New PTO Guidelines for Computer-Related Inventions and Design Patents

The United States Patent and Trademark Office recently issued new guidelines for its patent examiners to follow in handling computer related inventions. The new guidelines were formally adopted in February, 1996 in response to federal court decisions upholding the patentability of software. Software that demonstrably controls or configures some computer hardware is patentable, regardless of whether it includes significant mathematical processes.

The PTO has also changed its policy for design patents on computer icons and user interfaces. Under new guidelines issued in March, 1996, computer generated icons or screen displays qualify for design patent protection. This should significantly increase the number of applications for design patents in this area.

Several key points are addressed in the new software guidelines. First, claims for software must specifically indicate how the software controls the operations of a computer or configures structural features such as the organization of memory, stored data, or the like. It is the combination of software with its material transformation of the hardware or certain data that is patentable.

The second key theme is that the patent application must provide sufficient, detailed information that allows others in the field to practice the invention. Patents are required by law to provide an "enabling disclosure" in return for the right to prevent others from using the invention, and the guidelines direct examiners to focus on this.

Third, the new guidelines specify that incorporating mathematical processes into claims for software is not fatal. The emphasis is squarely placed on identifying the overall operation or structure of the claimed invention, not merely its computational details. Further, there are now specifically defined "safe harbors" (features in the claims that help ensure that the claim is patentable), including features that manipulate specific hardware, employ specific data not otherwise required by underlying mathematical equations, or employ computational results in specific applications.

Fourth, the guidelines indicate that patent protection is available for data structures in combination with some form of computer readable memory. However, data structures as merely logical arrangements of information are likely not patentable.

Fifth, the guidelines formally accept that software can be claimed as an article of manufacture, for instance, a CD-ROM or floppy diskette. This allows patent holders to sue those who ship infringing software for direct infringement, rather than for more complex "contributory infringement" or "inducement."

Finally, the PTO is attempting to quicken the pace of the examination process. All defects of a patent are to be identified by the examiner in the first analysis of the patent application. Examiners are specifically instructed to provide suggestions for changes to the patent claims to make the invention patentable.

One area of considerable interest for some software companies are patents on financial software packages. The PTO has typically rejected software in this area as merely performing "a method of doing business." The new guidelines explicitly state that methods of doing business are to be treated like any other process, and not singled out for rejection.

The guidelines discussed above are specific to utility patents, which cover processes, machines, articles of manufacture and so forth. Design patents are generally granted for any new, ornamental design for an article of manufacture. For a number of years, the PTO refused to grant design patents on icons and other screen displays on the grounds that the icons were merely unpatentable pictures or illustrations.

In March, 1996, the PTO issued new guidelines for examining design patents for computer generated icons, such as file or document icons. The design patent guidelines state that icons are subject to patent protection so long as they are illustrated as part of an article of manufacture, such as a computer terminal or other display device. The icon must be novel and non-obvious, so it is not likely that anyone will get design patents on file folders, trash cans, or other conventional icons. Further, the icon must be ornamental, and not purely functional, such as merely indicating the progress or state of an operation (*e.g.*, battery level icons).

Even so, many companies do create interesting and new icons for their software, which are often related to product or company names. Design patents on such "branded" icons complement trademark and tradename protection and should be seriously considered.

2. Other Patent-Related Issues

The growth of the Internet has provided certain new tools for patent research and analysis that were not previously available. For instance, IBM provides a publicly available Web site at which users can, at no charge whatsoever, search for and review all U.S. patents issued in the past 25 years. Such tools provide invaluable benefits for patent practitioners, as well as technical personnel looking to learn about particular areas of technology. In addition, countless Web sites provide discussion about various patents, their relative strengths and weaknesses, the terms on which they have been licensed to others, and the like. Prior to such information being available on the Web, it was much more difficult for potential licensees to estimate the value of a patent license that was being urged on them by a patent owner.

In addition, the Internet provides a fantastic vehicle for "prior art" searches. These searches are routinely performed by companies accused of patent infringement, in order to determine whether the patent at issue should be held invalid based on some earlier known technology that may not have been brought to the attention of the patent examiner. Even the Patent and Trademark Office can make use of such facilities in performing their examination searches. However, one failing of this technique is that the authenticity of information found in this manner is not immediately certain.

D. Trade Secret Law Developments

The law of trade secrets continues to have strong application in Internet-related industries, but the very nature of the Internet makes maintenance of trade secret information inherently difficult. Since information can be disseminated over the Internet almost effortlessly, once information finds its way onto the Internet it will be extremely difficult to claim trade secrecy for such information. For example, In *Religious Technology Ctr. v. Lerma*, 908 F. Supp. 1362 (E.D. Va. 1995), the court held that although a person who originally posts trade secret material on the Internet may be liable for trade secret misappropriation, reporters who merely downloaded such information from the Internet were not liable, since that information was publicly available once put onto the Internet. Similarly, another court in *Religious Technology Ctr. v. Netcom On-Line Communications Servs. Inc.*, 923 F. Supp. 1231 (N.D. Cal. 1995) held that posting works onto the Internet makes them generally known such that they can no longer be considered secret.

How, then, can companies gain the benefits of the Internet without losing the benefit of trade secret protection? Encryption programs are now available that allow messages to be securely transmitted over open channels with little threat of useful interception. In addition, secure "firewalls" to internal company facilities known as "intranets" permit company personnel to move back and forth between secure intranet sites and non-secure Internet sites.

Due in part to the recognition that increasing use of the Internet makes possible wholesale misappropriation of corporate trade secrets, Congress enacted the Economic Espionage Act of 1996 ("EEA") and National Information Infrastructure Protection Act of 1996 ("NIIP"), amending title 18 of the United States Code to provide federal criminal liability for theft of trade secrets and for "anyone who intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage." See 18 U.S.C. § 1030 et seq. These were signed into law by President Clinton on October 11, 1996. The NIIP has sometimes been referred to as the "Anti-Hacker Act" and now applies to any computer used in interstate or foreign commerce or communications. Even though these new laws are criminal in nature they are nevertheless quite important to civil trade secret appropriation issues as well.

The EEA concerns two types of trade secret thefts. Section 1831 of the EEA deals with "economic espionage"—the theft of trade secrets for the benefit of any foreign government, foreign instrumentality or foreign agent. Section 1832 concerns the theft of trade secrets generally as opposed to the theft of trade secrets for the purpose of economic espionage. Both Section 1831 and Section 1832 use similar language to define the crimes of economic espionage and trade secret theft.

Section 1831 provides, in part, as follows:
(a) Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense any offense described in any of paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in any of the paragraphs (1) through (4), and one or more of such persons do any act to effect the object of the conspiracy.

For violations of Section 1831, individuals may be fined up to $500,000 or imprisoned for up to 15 years, or both; organizations, on the other hand, may be fined up to $10 million.

Section 1832 applies to anyone who, "with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly" performs any of the acts set forth in paragraphs (1) through (5) above as to the trade secret information. It does not require for liability that there be any foreign beneficiary. The penalties for Section 1832 violations are less than the escalated penalties for Section 1831 violations covering foreign economic espionage. For violations of Section 1832, individuals may be fined up to $250,000 or imprisoned for up to 10 years, or both. Organizations committing violations of Section 1832 may be fined up to $5 million.

In addition to other penalties, the EEA also allows a court to order violators to forfeit to the United States any property or proceeds resulting from the violations or used in commission of such violations.

This statute also specifically provides for the protection of the trade secrets at issue during the prosecution of any offenses. Under Section 1835, the court is required to enter such orders and to take such other actions as may be necessary to preserve the confidentiality of trade secrets. Furthermore, any order of a district court authorizing or directing the

disclosure of any trade secrets is subject to interlocutory appeal. This provision was included because Congress expressed concerns about the efforts taken by courts to protect the confidentiality of trade secrets. According to a congressional staff member statement, the provision was included in part so that legitimate owners of trade secrets would not be discouraged from using the EEA. In particular, the legislative *Manager's Statement* accompanying the passage of the EEA provides the following guidance with respect to the protection of trade secrets by courts handling EEA cases:

It is important that in the early stages of a prosecution the issue whether material is a trade secret not be litigated. Rather, courts should, when entering these orders, always assume that the material at issue is in fact a trade secret. (Emphasis added).

In passing this legislation Congress has indicated, through the *Managers' Statement*, that existing civil remedies under state law to protect trade secrets may not be adequate to the task and a Federal civil cause of action may be necessary. Senator Arlen Spector has indicated that he intends to consider legislation in 1997 to enact civil remedies for the misappropriation of trade secrets.

The EEA also allows the United States to seek civil injunctive relief against any violation of the statute and allows the United States to prosecute conduct outside the United States if the offender is a natural person who is a citizen or permanent resident of the United States or an organization organized under the laws of the United States.

The EEA does not preempt or displace any other remedies. Thus, this statute is not intended to preempt any claims based on state law or under federal law, including the Federal Copyright laws.

A very important aspect of the EEA is the definition of trade secret that it provides. Section 1839(3) defines "trade secret" as meaning: all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, programs, devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes whether tangible or intangible, and whether or how stored, compiled or memorialized physically, electronically, graphically, photographically, or in writing if . . . (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public;

Though the EEA definition of trade secret generally corresponds to the definition of trade secret in Section 1 of the Uniform Trade Secrets Act, the EEA definition more fully describes the forms and types of trade secret information, as well as the manner that such trade secret information is stored, compiled and memorialized in today's information systems.

The definition of "owner" in the EEA should also be noted. Section 1839(4) defines the owner of a trade secret as "the person or entity in whom or in which rightful legal or equitable title, to, or license in, the trade secret is reposed." Thus, both owners and licensees are protected by this statute.

There may be some benefit to using the EEA definition of "trade secret" or adaptations of this definition in connection with the confidentiality clauses companies use in various forms of agreement. Current forms of agreement should be reviewed with the EEA in mind. By more closely tracking the statutory definition of trade secret, companies may be in a better position to demonstrate the applicability of the statute in the event of trade secret theft.

The EEA provides a very strong criminal remedy for combating trade secret theft. The EEA needs to be considered very carefully in the analysis of, and plans for, any trade secret enforcement action. Since the EEA does not displace any other federal or state law cause of action criminal prosecution may be considered in addition to any other civil claims for the misappropriation of trade secrets.

The EEA may also have a positive deterrent benefit that should be considered. It may serve to help discourage employees and others from stealing trade secrets. Company education programs on intellectual property should include specific information concerning the EEA so that all employees know the potential liability associated with the theft of trade secrets and fully recognize the gravity of the offense of trade secret theft. Trade secret programs need to appreciate the potential significance of the EEA as a deterrent and potential remedy.