

AMERICAN BUSINESS MEDIA

The Association of Business Media Companies

Legal Issues Relating To Publishing In New Media

March 1999

by Dana Shilling, J.D., ©1999, by American Business Press (ABP)

Table of Contents

I. Introduction

II. Copyright Issues

- A. Exceptions to Normal Copyright Requirements
 - 1. Public Domain
 - 2. Fair Use
 - 3. Scene a Faire
- B. Registering Copyrights
 - 1. Special Rules for On-Line Works
- C. The *Tasini* Case
- D. Using Sound on the Web
 - 1. Digital Performance Rights
- E. Protection of Data
- F. Kinds of Infringement

III. Legal Problems of Domain Names

- A. Trademark Basics
 - 1. Trademark Registration
- B. On-Line Trademark Problems
 - 1. Registering a Domain Name
 - 2. NSI Dispute Resolution
- C. Linking, Framing, and Caching

IV. Patent Issues

V. Liability Issues for On-line Publishers and Distributors

- A. Content Regulation
- B. Defamation

VI. Important Recent Registration

- A. Digital Millennium Copyright Act
- B. Y2K Information and Readiness Disclosure Act
- C. Internet Tax Freedom Act
 - 1. Basic Sales Tax Principles

VII. Protection of Consumers

- A. Privacy Protection
 - 1. FTC Measures
 - 2. EU Directive
- B. False Advertising
- C. Credit Card Fraud
- D. Securities Fraud
- E. Spam
- F. Click-Wrap Agreements

VIII. Jurisdiction: Where You Can Be Sued Based on On-Line Activities

The author wishes to thank Ron N. Dreben and Karen Butcher of Morgan, Lewis & Bockius LLP for their contribution to an earlier version of this paper.

NOTE: The purpose of this article is to provide basic information about U.S. intellectual property law as it relates to electronic media. However, it does not represent individualized legal advice. You should contact your own attorney for individualized compliance strategies.

I. Introduction

There are already plenty of legal rules in existence to straighten out copyright, patent, trademark, trade secret, obscenity, defamation, and unfair competition issues--issues that relate to intellectual property (IP). Unfortunately, most of those rules date back long before the World Wide Web was accessible to much of the U.S. population. Some of the rules reflect the mind-set of the nineteenth-century bureaucrat who suggested closing down the Patent Office because everything useful had already been invented.

Our legal system is struggling to come to grips with emerging technologies. It's tough enough to monitor unauthorized copying of copyrighted works when the infringer had to own a printing press. The task got much tougher when photocopying became practical--and is almost insuperable when "copies" can be distributed on the Internet instantly, at very little cost. However, the practical ease of infringing on a copyright doesn't reduce the legal validity of the copyright.

In the past, it was perfectly clear who would get in trouble if government censors deemed a publication to be obscene, libelous, or seditious: secondarily the author, but primarily the printer and publisher (who were usually one and the same). Today, there are many more parties involved, including Internet Service Providers (ISPs), Website designers and operators, and individuals who post information to Websites. A body of law is gradually emerging to sort out the various liabilities (including who gets into trouble if securities fraud occurs on-line).

Similarly, trademarks evolved as a local phenomenon, then a nationwide registration system was

created (but did not entirely replace the local system). Today, companies that want to register a domain name may find that a name they confidently thought of as their own must be shared with other businesses using the same or a similar name. See Part III for a discussion of some of the IP problems of naming a Website.

The legal system (including the Internal Revenue Code) is just beginning to cope with the concept of "software" as a special kind of intangible property. But there are many differences between a software program (such as Excel or PeopleSoft) and a Website, which is a method of displaying and transmitting content such as words, images, music, and videos. It has not yet been resolved whether the Internet is a "public" place (e.g., for deciding if material has been "published," whether there has been a "public performance" of music or dramatic works, or whether a Website is a "public accommodation" which is required to meet handicap-accessibility requirements). The main Internet probably is "public" for this purpose, but there are even greater problems created by intranets.

The Internet, of course, connects the entire world, so sites originating within the United States are very likely to be accessed in other countries. Not only does that create language barriers (and currency barriers, if the site can be used for transactions), but it creates potential for conflict between U.S. "community standards" of taste and those of other countries-an image of a woman clad in shorts and t-shirt would be inoffensive in the United States, but extremely offensive in much of the Islamic world, for instance. Furthermore, the United States copyright law is not the same as the law for the rest of the world, and in some respects the European Union offers more protection to authors and publishers (for instance, "moral rights" preventing alteration of a creator's work are recognized, and royalties are payable on library sales). The EU privacy rules are also much stricter than the U.S. rules, and may result in the on-line equivalent of trade embargoes of U.S. sites.

There is a whole body of law about radio and TV stations, including their licensing, the frequencies they can use to broadcast, and how they pay licensing fees for programming. As the Internet's use of multimedia becomes more sophisticated, it may in effect be possible for almost anyone to have a personal "radio station" or "TV station"; it will have to be determined the extent to which telecommunications law will apply to these "micro-stations."

II. Copyright Issues

The author of a work, or an employer that has commissioned a work as a "work for hire," becomes the "copyright proprietor." The entire subject of copyright is often thought of as a "bundle of rights," which is an important concept for several reasons. It is possible to sell, give away, or assign all of the rights involved in a copyright-and also to enter into exclusive or non-exclusive licenses affecting only some of the rights, or to transfer some but not all rights. A person or business that wants to use copyrighted materials in some way (unless an exception to the normal requirements applies: see ¶II.A) needs permission to exercise the appropriate rights. Furthermore, each right must be obtained from the party who actually owns it-and it's not always clear who controls which rights, at what time.

Although we usually think of copyright in terms of written materials, many other kinds of things can be copyrighted: photographs, movies, musical compositions, and recordings of musical compositions, for instance. Some of the toughest legal problems on the Web deal with the fact that a Website can involve "multimedia"-e.g., combinations of items, involving different rights, and whose rights are held by different people.

Some material cannot be copyrighted: U.S. government publications, for instance. Ideas can't be

copyrighted. Neither can titles (although it may constitute unfair competition to misappropriate a title associated with someone else). What is copyrighted is a particular expression, so, for instance, romance paperbacks can be copyrighted despite compelling similarities in their plots and characters.

Creators of copyrightable works automatically have a copyright as soon as the works are created and "fixed" in a tangible form (e.g., written down; photographed), even before they are published, and even if no steps are taken to register the copyright. However, certain remedies against infringers (those who violate the copyright) are only allowed if the copyright was registered, and if the work was published with a notice indicating who owns the copyright. The creator can sell or assign the copyright-typically, to a publisher, movie studio, or similar business. Commissioned works can be "works for hire"-i.e., the contract between the commissioning business and the creator clearly indicates that the copyright will belong to the business and not to the creator of the work.

One of the most important rights in the "bundle" is the right to control "derivative works," such as sequels and works using the characters of a work of fiction in other contexts. As long as a work is in copyright, only the copyright proprietor can determine how its characters will be used. You can write a novel about Hamlet marrying Alice in Wonderland (because those works are in the public domain; see ¶11A(1)) but you'll need the consent of Paramount and Disney to publish a story (whether print or on-line) about Luke Skywalker/Ariel the Little Mermaid nuptials. Many Websites include copyrighted images and "fanfic" (fiction written by fans of a movie, TV show, etc.); unless prior consent of the copyright proprietor has been obtained, these sites are in violation.

Ability to control derivative works includes the ability to control changes and distortions in the work-for example, using Photoshop or other software to change a copyrighted photograph. It is not a defense to a charge of copyright infringement that you have altered the copyrighted image; even if the "new" image is not identical to the old one, it is a violation of the right to control derivative works.

Many copyrighted works consist of collections or compilations of other works-e.g., a short story anthology, and ¶201 of the Copyright Act permits copyrighting the compilation as a work in itself, based on the selection of items to be included and their arrangements. (Compilations also frequently include original material such as introductions and critical writing.)

As mentioned above, facts per se can't be copyrighted. A non-fiction book or article containing facts can certainly be copyrighted, although it is not an infringement for someone else to copy some of those facts and use them in a different expression. (It certainly isn't a good idea to encourage the writers of non-fiction to make up their own facts in the interest of creativity or copyright compliance!)

A. Exceptions to Normal Copyright Requirements

1. Public Domain

Copyright doesn't last forever: material "falls into the public domain" after the copyright expires. It's not always easy to say when it expires, however. For works copyrighted before 1978, material entered the public domain 75 years after its first publication. Between 1978 and 1998, the term of a copyright was the life of the author plus 50 years (or the life of the longest-lived author plus 50 years, if there was more than one). The Sonny Bono Copyright Term Extension Act of 1998, S. 505 (1/27/98) however, basically extends earlier copyright terms by 20 years. Note that this new law is a major boon to Disney and other large companies that have a large inventory of

copyrighted material, but may create additional difficulties for parties who want to use content that would otherwise have entered the public domain.

2. *Fair Use*

There are also some situations in which some kind of use can be made of copyrighted material without infringing on the copyright. One of the most important is "fair use": the opposite of unfairly taking someone else's work. For instance, it is a fair use to discuss the ideas in a book or article in another book or article, and even to quote short passages as part of a review, discussion, or comment. There are four major elements in fair use, as defined by Copyright Act §107 and a body of case law:

- How and why the material is used; non-profit educational use is much more likely to be considered fair than for-profit commercial use
- The nature of the work or trademark allegedly copied
- How much of the allegedly copied work is used-and what percentage of the whole it constitutes
- Whether the asserted fair use limits the commercial potential of the allegedly copied work

The last two factors were crucial in deciding recent cases where infringement was found when Playboy photographs were made available on the Internet without the magazine's permission, and when entire articles were posted without permission.

Even "freeware"-material that can be copied for personal use at no charge-is protected by the fair use doctrine, as the Northern District of Illinois decided in a July, 1998 case. Copying and re-selling a freeware game was held not to constitute fair use. The entire game was copied, not just a part; and even though the owner of the copyright did not sell the game (so it did not lose sales income as a result of the copying), it did sell a "key" that enhanced the success of game players, so the defendant's actions impaired the market for the key.

Title III of the Digital Millennium Copyright Act, discussed below, authorizes making copies of a computer program in the specific context of maintaining or repairing a computer; the copy must be destroyed as soon as the computer is ready for normal use again.

Parody is a special kind of fair use: some leeway is allowed for caricaturing copyrighted materials, especially if it's obvious that there is a parody and not just an imitation. However, it is more likely to be accepted by the courts if there is a parody of the copyrighted material itself (e.g., making fun of the film "Titanic") rather than using copyrighted material to parody something else (e.g., using images or caricatures of Kate Winslet's and Leonardo DiCaprio's characters to parody something other than the film "Titanic.")

3. *Scene a Faire*

Copyright law includes the "scene a faire" doctrine (this is a French phrase which more or less means "obligatory scene"). In other words, if two works in the same genre use the conventions (or cliches) of the genre, this doesn't mean that the later one infringes the early one, only that a final kiss is a basic part of the romance genre, shoot-outs are a basic part of the Western genre, and conflict among conspirators is a basic part of the thriller genre. A similar doctrine can be applied to functional elements of a computer program-just about any program is going to use menus and commands, so some similarities are inevitable.

Although case law hasn't yet caught up to the question of "look and feel" of Websites-and it's easy to copy an entire Website (because the HTML code can readily be accessed by clicking on the "Source" option in the "View" menu of the Web browser-courts would probably decide that imitating some of the design and functional features of another site is OK, because certain design elements are scenes a faire, but wholesale copying is probably unfair competition and possibly infringement of the copyright in the site as a whole. A distinctive look and feel might obtain secondary meaning as "trade dress," a trademark-like concept that applies to the overall design and packaging of a product.

B. Registering Copyrights

The basic procedure for registering a copyright calls for filling out a simple federal form, submitting it to the Copyright Office with a small fee, and "depositing" copies of the work. There are several forms; the creator of the work picks the appropriate form: TX for "literary works" (computer programs are considered to fall into this class), VA for paintings, drawings, photographs, and other visual works; PA for audiovisual materials; and SR for sound recordings (i.e., This is simple enough in the case of a book or music CD, tough in the case of a sculpture (you deposit plans or photographs), and hard to figure out in the case of a Website. You certainly can't "deposit" a site the same way you can a manuscript or printed book, but you can copyright it.

1. Special Rules for On-Line Works

The Copyright Office issued rules in November, 1997, called "Copyright Registration for Online Works." For a text-only site, obviously TX would be the right choice; an on-line art gallery would probably fall under VA. Most Websites, however, contain text in combination with a lot of images, and some include sounds, music, and/or video. So far, the Copyright Office doesn't have a separate registration form for multimedia works, much less on-line multimedia works; the creator of the work has the responsibility of picking whichever registration form covers the predominant content of the site.

The application requires the applicant to list the nature of his, her, or its authorship. The material should not be described as "Web site" or "user interface"; instead, more specific information such as "articles about race cars" and "digitized images of race cars" should be given. The description is crucial, because copyright protection extends only to copyrightable content (not public domain material) that is included in the copyright registration.

The next hurdle is "depositing" the copyrighted work. The basic procedure for the deposit of an on-line work is to submit a computer disk containing a copy of the entire site, plus hard copy, audiocassette, or videotape (depending on the nature of the material). For up to about 3-5 minutes of material, or five pages of text or graphics, hard copy of the entire work should be submitted; but if the whole site is larger, five pages that are a representative sample, or an equally representative three minutes of tape or video, should be submitted. Or, the creator of the work can deposit hard copy of the entire work, whatever length it is, in which case it is not necessary to deposit a computer disk.

The procedure is different if the site reflects material that has already been published as a hard-cover book. In that case, the creator should deposit two copies of the hard-cover book, but nothing from the site. Still another procedure applies to copyright a computer program or database (part of the data in the database, or the source code for the program, is deposited) and CD-ROMs (not only the whole CD-ROM, but its packaging, instructions and manuals, and operating software must be deposited).

The nature of a Website is that it isn't much good unless it stays current, so you should have a workable plan to keep refreshing the site. Unfortunately, this means you'll also need a copyright strategy, because every time you add new copyrightable material to the site, you have to re-register to maintain copyright protection. So far, the Copyright Office does not have a procedure for registering the start-up version of a site and all of its updates.

The Copyright Office is trying to drag itself into the twenty-first century, though. Since 1993, the agency has had a pilot project for performing copyright registrations on-line (whether or not the copyrighted material actually appears there). The Copyright Office Recording Documents System (CORDS; check acronym) allows copyright proprietors to register copyrights on-line rather than on paper, speeding up the service from four months (the average time for a paper registration) to 10-15 days (the best case scenario for on-line registration).

One interesting feature is that not only does the CORDS system include a registration form that can be filled out using a Web browser, but the registrant attaches a data file containing the work that is being registered. Once CORDS is fully developed, people will be able to access the actual work through the CORDS system, if the copyright proprietor allows them to do so (probably in conjunction with payment of a fee).

CORDS is working on one of the most serious problems for e-commerce: how can you "sign" an electronic document? CORDS, like many other commerce sites, uses private key encryption for digital "signatures." To use CORDS or learn more about copyright, check out the Copyright Office Website, <http://www.loc.copyright.gov>. (The Copyright Office is part of the Library of Congress, which explains the "loc."). You can subscribe to a free on-line newsletter that will alert you to developments in copyright regulation by e-mailing LISTSERV@RS8.loc.gov, using the message "Subscribe USCopyright."

C. The *Tasini* Case: Compilations and Boldly Going Where No One Has Gone Before

So far, *Tasini v. New York Times Company*, 972 F.Supp. 804 (S.D.N.Y. 1997) is the first and only case to tackle one important Internet copyright issue head-on. In this case, freelance writers' work was published in print. Most of the plaintiffs did not have written contracts; none of them had contracts with the initial publisher specifically granting electronic rights to the publisher.

The case arose when several publishers, including the New York Times agreed (and received fees for) to put some of this material on CD-ROMs and allow it to be included in the Lexis-Nexis information database. The writers did not receive any additional compensation for the re-publication.

The authors, not surprisingly, sued for copyright infringement-but lost. The court's decision was that the publishers had a valid compilation copyright in each entire issue of each publication (as distinct from the various individual articles in the issue). The copyright proprietor of a "collective work" has a right, under §201(c) of the Copyright Act, to revise that work. The Southern District of New York treated the activities of the publishers as revision of the collective work, not infringement of the authors' copyright in the underlying work.

However, even though so far there are no other cases specifically about the Web, there are plenty of cases (recent and otherwise) dealing with the impact of new technology on existing entertainment contracts. For instance, many movie contracts were negotiated long before home video was a possibility. It's hard to draw hard-and-fast rules based on these cases; relevant factors include whether all rights were transferred or only specific rights; if the technology was

contemplated (even though not in use) at the time of the contract; and which rights were retained by the creator of the work.?

For full protection, make sure that your contracts grant you comparable rights not only in technologies already in use, but those that may be developed in the future. Furthermore, if you want to electronically re-publish material that is in print as part of a collective work, make sure that you have permission of both the copyright proprietor of the individual element and of the compilation.

If you are commissioning work that will appear on your own site (e.g., artwork; writing) have the creator of the work sign a written work-for-hire contract that satisfies the requirements of the Copyright Act. If you are using "stock" elements, such as clip art or digitized photographs provided by a service bureau or software publisher, make sure that the fee you pay to buy or license the material entitles you to use it on a Web site. (You may have purchased only one-time rights, or the right to use the material in an in-house publication or intranet, but not on a publicly accessible Website.

In many instances, a Website contains some elements owned by the company that posts and maintains it, and other elements owned by the designer or design firm involved in the creation of the site. For instance, it is conventional for designers to retain the right to re-use software modules or code elements they themselves have developed, or to re-use graphics that they themselves created for the project. The commissioning company, however, will certainly want the right to a perpetual, royalty-free use of such graphics, and may insist on outright ownership of graphics created especially for their project, even if the graphics do not reflect their logo or corporate image.?

D. Using Sound On The Web

The copyright treatment of music is especially confusing. Once a piece of music has been composed, there are many things that someone other than the composer might want to do with it:

- Publish the sheet music
- Perform the music in public (for instance, at a concert)
- Record the music
- Play an existing recording in public (such as using CDs to provide atmosphere in a restaurant)
- Use an existing recording as part of another work-such as using a song as part of the soundtrack of a movie, or adding a sound clip to a Website.

It is not absolutely clear when, or whether, the use of music on the Internet constitutes a "public performance" at all. ASCAP and BMI naturally take the position that it always does, but the line may be drawn differently: Webcasting that is perceived in the same way at the same time by a large audience may be treated as a public performance, whereas downloading of music clips by individuals, at their own election, might not be.

The complexity comes in because each of the various uses involves different rights from the "bundle," and therefore different licenses, often issued by different parties. Furthermore, it's easy to apply for the wrong combination of licenses, or to contact a party who honestly believes that it controls the rights you need-or that dishonestly claims to control rights that actually belong to others.

In addition to these uses, which have existed about as long as sound recordings, the Internet makes an additional use possible: accumulating recordings on a Website, and allowing people to download them (whether for free or by paying a fee). The MP3 compression format is a convenient format for reproducing music, and transmitting it quickly. MP3 files can be played on the Diamond Rio player, a portable device that looks a lot like a Sony Walkman. (As an alternative, music can be transmitted using software such as Real Audio.)

The Recording Industry Association of America tried but failed to get an injunction that would have forbidden U.S. sales of Diamond Rio players. The RIAA's objection was that MP3 files are not copy-protected, so it is impossible to disable the files until royalty payments have been made. Therefore, although the Rio can be used legitimately (for public domain materials, or subject to scheduled payments), piracy is very easy.

The basic copyright rule, dating back to the days of player pianos, is that the copyright proprietor of a musical composition has an absolute legal right to determine who will make the FIRST recording of that composition (often, the composer him- or herself will exercise that right, or will let a favored performer put a definitive interpretation on record). But after that, a "compulsory license" structure goes into place. Anyone else who wants to record the work is allowed to do so, in return for agreeing to pay royalties to the copyright proprietor. Royalties are also due when copyrighted recordings are played in a public place, or synchronized with another work (as part of a sound track).

ASCAP (the American Society of Composers, Authors and Publishers) and BMI (Broadcast Music International) maintain clearinghouses so that those who record or use copyrighted music make regular reports to ASCAP or BMI on how many copies of recordings have been sold and how often copyrighted compositions have been played. Those who use the music make payments to ASCAP or BMI, who then divide the money among the various copyright proprietors whose works have been used. ASCAP uses EZ-Seeker, software created by Online Monitoring Services, to scan the Internet for Websites that maintain music archives or otherwise distribute music.

ASCAP has published an Experimental License Agreement for Computer Online Services, Bulletin Boards, Internet Sites and Similar Operations; BMI does not have a standard agreement for this situation. The ASCAP agreement imposes a basic charge of \$500 per year, and includes three payment schedules keyed to the site's revenue-which, of course, fails to cope with the numerous sites that (accidentally or by design) fail to generate revenue.

The right to record a piece of copyrighted music is known as a "mechanical" or "mech" license. The right to incorporate a piece of copyrighted music into another work (e.g., to add it to the soundtrack of a movie) is called a "synchronization" or "synch" license. It's hard to tell whether a Website that uses music will require one or both licenses. According to legal scholar Ronald Lubach, a mech license is not necessary if a temporary copy of the music is made during the uploading process, but probably is necessary if the end user retains a permanent copy of the music on his or her computer hard drive. If the end user controls the relationship between the music and the images on a site, the site's owner will probably not be obligated to get a synch license. However, if the site displays as an integrated work of art, with specified music accompanying certain images, a synch license will probably be required.

The settlement of a 1995 New York case, *Frank Music v. CompuServe*, led to a procedure for licensing copyrighted music. CompuServe users can get PIN numbers that allow them to request a "mech" license for digital transmission and copying of a particular piece of music.

1. Digital Performance Rights

In 1995, Congress passed the Digital Performance Right in Sound Recordings Act of 1995, P.L. 104-39, 17 U.S.Code Sections 114-116. Detailed rules for "use of sound recordings in a digital performance" can be found in the Code of Federal Regulations (a compilation of rules drafted by federal government agencies): see Title 37 Part 260.

This act extended the "compulsory license" concept to "digital subscription transmission services," which are narrowly defined to include digital transmission of audio over the Internet, but not conventional analog audio transmissions (i.e., ordinary radio broadcasting, already covered by copyright laws and licensing schemes), interactive digital transmissions, or digital transmission of audiovisual works. P.L. 104-39 was drafted at a time that it was expected that "pay per listen" "audio on demand" would become a major market segment, but that has not panned out as anticipated. You can find detailed rules at 63 Federal Register 25934 (5/8/98). You should be aware that sites are not allowed to publish an advance program or schedule of which music will be played, and only three selections from one record (and only two in a row) can be played during any three-hour period; only four different recordings by the same artist can be played within three hours.

The Digital Millennium Copyright Act copes with digital transmission of music over the Internet that uses streaming audio technology ("Webcasting"), which was not covered by the Digital Performance Right Act. Webcasts are called "eligible nonsubscription transmissions"-i.e., eligible to follow the statutory licensing procedure, even though they don't use the subscription business model that was contemplated in 1995. Eligible nonsubscription transmissions are noninteractive; part of audio programming for entertainment; and not used to sell, advertise, or promote goods or services. This time, the rules can be found at 63 Federal Register 65555 (11/27/98). Both the Digital Performance Rights Act and the Digital Millennium Copyright Act require the payment of royalties for on-line music performances.

Yet another group of problems arises from the fact that music can easily be "digitized" (saved in digital form), and digitized sound files can be downloaded from the Web and played on the user's computer, or saved on the user's hard drive or transferred to a CD. It is perfectly legitimate for a copyright proprietor to put digitized music on the Web, and to allow people to listen to it or copy it, if the copyright proprietor thinks that it will benefit in the long run from increased popularity of the music or its performers. But it is not legitimate for pirates (even if they do not profit themselves) to create on-line archives of copyrighted works to which they do not have rights.

The Recording Industry Association of America (RIAA) has been active in defending the rights of record companies against defendants who create archives of copyrighted music, and then encourage downloading by consumers. The organization's site, <http://www.riaa.com>, has details of the litigation.

In July, 1998, a European organization, SESAC, that acts much like ASCAP or BMI, sued a radio station, claiming that streaming audiocasts of copyrighted songs on the station's Internet site are unlawful, because they are unpermitted performances of the songs; but the case has not yet been resolved.

E. Protection of Data

Traditional copyright principles do not really accommodate databases. A compilation of facts that reflects original selection and arrangement can be copyrighted. See 37 Code of Federal Regulations 202.20(c)(vii) and Copyright Office Circular 65, "Copyright Registration for Automated Databases," for the Copyright Office's deposit requirements. For copyrightable

databases, compilations, and statistical compendia, the mandatory deposit is one copy of "identifying portions" of the work (the first and last 25 pages, printed out or otherwise reproduced in a form that can be read without a machine). "If the work is an automated database comprising multiple separate or distinct data files," the identifying portion consists of 50 complete data records from each data file (or the whole thing, if it's smaller than that). There are special rules for copyrighting updates to databases.

Even a database that is not entitled to copyright as such may be entitled to protection under state law, and you may be able to sue for the tort of misappropriation if anyone copies (without adding new creative elements) a database in which you have invested substantial funds, time, labor, or skill, and if this copying is commercially damaging to you. However, it is likely that you will succeed in court only if the copying is done by a direct competitor, and the court may require that the copied material be time-sensitive information that can be characterized as "hot news." Congress is considering legislation that would offer broader protection to databases of all kinds, even where there is no "hot news" involved.

One of the differences between U.S. and European Union copyright law-and one that has not been resolved yet-is the greater protection given to databases under EU law. The EU's Database Directive extends protection to situations in which the creator of a database has used significant judgment and made a substantial effort in deciding which data to include, and how to arrange them, within the database.

F. Kinds of Infringement

More than one party might be involved in copyright infringement, each playing a different role. The party actually responsible for initiating infringement is a direct infringer; other parties may have lesser liability as contributory infringers. See below for the Digital Millennium Copyright Act's procedure for excusing Internet Service Providers (ISPs) from liability for contributory infringement if they maintain a procedure for prompt removal of infringing content.

It is quite clear that direct infringement claims can be brought when copyright materials are placed on the Internet without permission and, if the owners of a Website or ISP take an active role in selling access to copyright images or encouraging uploading of copyrighted images by users (and are not merely passive conduits for copyright infringement by users), they can certainly be subjected to liability.

A 1994 case, dating back to before the Web was available, involved a BBS (Bulletin Board Service) whose operator encouraged BBS members to place copyrighted computer games on the BBS, so that other users could download them without paying the copyright proprietors. The BBS operator was charged with violating 18 USC §1343, the federal wire fraud statute, but was acquitted because he was merely a computer game enthusiast and BBS hobbyist; he did not earn financial profits from the operation.

Congress took advantage of a broad hint from the judge in this case, and passed a law, The No Electronic Theft Act (NET Act), P.L. 105-147 (12/16/97). The NET Act makes it a crime to copy and distribute (including by electronic means) copyrighted works with an aggregate value of \$1,000 or more, with additional penalties if at least 10 copies with a retail value of \$2,500 or more are distributed within a six-month period. Note that it is possible to violate this statute based on the value of the works that are copied-whether or not the copier derives financial benefit from the copying.

III. Legal Problems Of Domain Names

Although, technically, Websites are identified by their "IP Numbers"-a series of digits, separated by dots, that act much like a telephone number-nearly all contact with sites is initiated by using "domain names." (The communications network that handles the communication translates the domain name into IP number.) Most (although not all) domain names begin with "http://www," which indicates that the Hypertext Transmission Protocol (http), rather than one of several other possible transmission systems, is being used. "WWW" stands for "World Wide Web," which is the part of the Internet that uses graphical user interfaces.

Under the current system, all U.S. Websites are organized into several "top level domains" (TLDs): .gov for government sites, .org for sites run by non-profit organizations, .edu for educational institution sites, .mil for military sites, and the ubiquitous .com for commercial sites. Therefore, most Web addresses start with http://www and end in .com; it's the stuff in the middle that can cause problems.

During the early years of the Web, domain names were assigned by Network Solutions, Inc., a private company. NSI's contract with the federal government has expired, and another entity will take over; see 63 Federal Register 8825 (2/20/98) for details. The Internet Assigned Numbers Authority (IANA) wants a non-profit organization, the Internet Corporation for Assigned Names and Numbers (ICANN) to take over, and the Department of Commerce agreed on October 20, 1998, that this was a good idea (see 67 U.S.Law Week page 2252).

No two Websites can use exactly the same domain name, so if you want to use a name that has already been registered, you will probably have to get the earlier registrant's permission-which might be given for free, but will probably cost money (although, despite a few cases of large sums being spent for commercially valuable names, usually not a very large sum of money).

A. Trademark Basics

Under U.S. practice, a "trademark" is a name, picture, or logo (combination of name and picture) that identifies a kind of goods. A "servicemark" does the same thing for a service (e.g., auto repair). A business can claim a trademark by putting TM after each use (or SM for a servicemark)-and being careful to protest when others use the mark in other contexts. Failure to do can lead to "abandonment," and to the mark becoming "generic" and available to anyone making the same product or rendering the same service. For instance, "aspirin" used to be Bayer's trademark for acetylsalicylic acid tablets, but they abandoned the trademark and now anyone who makes that kind of over-the-counter pain relief tablets can refer to them as "aspirin."

Not all trademarks are equal. Because the purpose of the trademark is to identify a particular brand or source of goods, trademarks gain entitlement to a greater measure of protection if they acquire "secondary meaning": if consumers identify the trademark with a specific manufacturer's products. A strong trademark is an arbitrary one; a purely descriptive term cannot be registered as a trademark at all. For instance, "BlogBB" would be a very strong trademark for potato chips (whether anybody would buy potato chips with a name like that is a practical marketing question, not a legal one), but "Crunchy" would be a very weak trademark, and could not be registered unless it had secondary meaning, because all potato chips have to be crunchy, no matter who makes them.

1. Trademark Registration

Just as works are automatically copyrighted as soon as they are created-but it makes sense to register the copyright to put other people on notice-trademarks can exist and be enforceable even if they are not registered, but there is a useful registration process. The federal government maintains several registers, including a Principal Register for trademarks, a Principal Register for

service marks, and a Supplemental Register of words, shapes, and symbols that are capable of becoming trademarks.

Trademarks and service marks can be registered either based on their existing use in interstate commerce, or on Intent to Use (ITU) the mark in the future. However, ITU registrations will not be finalized until the registrant files a verified statement that the mark is now being used in interstate commerce. (In a sense, then, trademarks work in the opposite way from patents: you can't get real trademark protection unless you have used the mark and consumers recognize it; you lose the ability to patent an invention or process if you have already disclosed it to the public.)

When a federal trademark application is filed, an Examining Attorney in the Patent and Trademark Office checks the application against the existing registrations to see if it is deceptively similar to an already registered trademark, or could cause consumer confusion. To prevent wasted time and embarrassment, registrants usually perform their own searches first (or hire a specialty trademark research firm) to make sure that the desired trademark is not duplicative of an existing trademark.

Trademarks and service marks are organized into classes, based on the goods or services covered by the mark. If you want to register a trademark specifically for a site, you should be aware that the U.S. Patent and Trademark Office (PTO) does not consider Websites, or even text that can be downloaded from a computer network, to fall into International Class 16 ("printed materials"). Instead, the PTO thinks that International Class 42 should be used, on the theory that the publisher is offering the service of providing publications on a global computer network. If a whole publication (such as a magazine) is presented on a site, the primary service that qualifies for registration is providing the publication electronically.

Although trademarks are usually thought of in terms of names or logos, other things can qualify for trademark protection, if they are associated with a particular brand and therefore can cause customer confusion: for instance, the color of a product's packaging. This could have implications on the Web, if a particular background or banner color is associated with a particular site.

The Federal Trademark Dilution Act of 1995 gives the owners of "famous" trademarks (those with significant secondary meaning) the right to obtain an injunction preventing others from using the trademarks in a way that dilutes the distinctiveness (and thus the commercial value) of the marks.

It's important to protection of a trademark that, every time you use it, you include an indication of its status. Accompany the name or logo with TM (for trademark), SM (for servicemark) or ® (for registered trademark), and include a statement such as "### is a [registered] trademark/servicemark of *** Corporation, which explicitly prohibits its use without permission. Improper use of a trademark or servicemark violates state and federal trademark law." Be sure to protest on the record every time you see your trademarks or servicemarks mentioned without indication of their status. Of course, you should accord the same respect to other parties' trademarks or servicemarks if you mention them on your site.

In addition to federal registration of trademarks, most states have some kind of registration procedure for trademarks used in that state. Sometimes states offer broader protection than the federal system. Also, some trademarks are ineligible for federal registration because they are not used in interstate commerce, but can be registered in the state where they are used.

B. On-Line Trademark Problems

Very early in the commercial development of the Internet, it occurred to various people that if they reserved domain names that were the same as, or very similar to, famous trademarks, that sooner or later the owners of those trademarks would want to use the trademarks as domain names, and would have to pay to "buy them back.". (At that time, you could register a domain name without proving any connection with it.) This practice became known as "cybersquatting," and in appropriate situations, it can constitute trademark infringement or unfair competition.

Trademark dilution occurs when a trademark or service mark is "famous"; if its lawful owner uses it in commerce; that the alleged infringer is also making commercial use; and that the alleged infringement reduces the commercial value of the legitimate mark owner's use of the mark. This could cause problems for a start-up company that has not yet had time to make its marks "famous," or even start selling products and services.

A related problem is the practice of registering domain names that represent common misspellings or typographical errors of famous names: "IMB" or "Dinsey," for instance. The theory is that the owners of those domains will get a lot of traffic from people who are trying to reach the famous site, and once people reach a site, you can always try to sell them something.

"Meta tags" are part of the HTML code of a site, but are not readily viewable by site users. Meta tags are used by search engines and directories such as Yahoo ® and Infoseek ® to classify sites. Sometimes meta tags are used deceptively, e.g., including the name of a popular company or site so that people who do a search for that company will get references to the manipulative site instead. It has been held to violate a registered trademark to include it in the meta tag of an unrelated site, without consent of the trademark owner.

Sometimes so-called "rogue" sites are posted to express someone's hostility to a particular organization, company, or its products. Deliberately deceptive URLs might be used by political sites that want to attract the attention of opponents: e.g., a Right to Life advocate using a site name that appears to belong to Planned Parenthood. Although First Amendment rights can be exercised on the Internet, just as in print, deliberate deception is not permitted.

1. Registering a Domain Name

Although it is not determinative, an easy first step in ascertaining the availability of a domain name you would like to use is a "whois" search at <http://www.internic.net>, to see if the name you want is already in use; there are also commercial search companies that ascertain availability for a fee.

The current practice is that Network Solutions, Inc. issues the domain names. In general, a domain name will be issued to the first party that requests it. However, the application requires a statement that using the name does not infringe on anyone else's rights (e.g., trademarks); that the statements on the application are true; and that the registrant legitimately intends to use the domain name in commerce, not hoard it or operate as a cybersquatter. The NSI doesn't do its own investigation, so getting the domain name you want doesn't mean that you won't be pursued by someone else who objects to your use of the name.

At the end of 1998, NSI changed its domain name policy, and said that it would only be proper to register an entire domain name (for instance, "Yourcompany.com") as a trademark if the domain name is a separate brand by itself, or has achieved recognition. Otherwise, just the underlying name (in this example, "Yourcompany") should be registered. NSI also suggests registering your domain name in several TLDs (.com, .gov, and .org) to prevent others from taking that route to

obtaining a similar name, although it seems inappropriate to encourage non-governmental, non-profit, non-educational entities from registering such TLDs.

The Patent and Trademark Office's February, 1996 guidelines for domain name registration say that domain names should only be registered if they are actually used in business as trademarks or servicemarks, not just as Internet addresses. The PTO prefers registration of addresses as servicemarks rather than trademarks. The mere fact that a mark is used on the Web doesn't make it "telecommunications service" (Class 38); the actual class of the underlying service or product should be registered.

On a related issue, the Eastern District of Virginia refused to issue a preliminary injunction forbidding AT&T to use the phrase "you have mail" in connection with its own e-mail service. America Online Inc. sought the injunction, claiming that it familiarized the phrase "You've Got Mail" in the e-mail context. The question to be decided at the full trial will be the extent to which secondary meaning can be asserted in common English phrases.

2. NSI Dispute Resolution

Most domain disputes do not involve greed or intentional deception, but a good-faith dispute between two companies already using or intending to use similar names in business. Under the current system, a private company called Network Solutions, Inc. (NSI) controls the assignment of URLs and arbitrates disputes under its Domain Name Dispute Policy, which is fairly cumbersome and lengthy. For the latest version of NSI's domain name policy, see <http://rs.internic.net/domain-info/nicrev03.html>. (There is no "www" in this URL.)

The first step is for the owner of a registered trademark that believes a domain name violates its rights in trademark is to notify the domain name owner that the trademark owner believes its legal rights have been violated. The two companies may be able to resolve the problem-perhaps the domain name owner will stop using the name, or will pay the trademark owner for the privilege. But if informal negotiations don't work, the trademark owner can seek relief from the NSI, supplying a copy of the trademark registration and the notification to the domain name owner.

The domain name owner is then given 30 days to submit a trademark registration certificate registered after it was notified of the challenge, or after the NSI's request for proof of ownership. If this cannot be done, the NSI puts the domain name on hold, and NEITHER claimant can use it until the dispute has been resolved in the courts. NSI determines whether the domain name is "identical" to the trademark; mere confusing similarity, even if it would be enough to win a court case for trademark infringement, isn't enough.

However, this procedure doesn't work when neither party has a registered trademark-or if the desired domain name is purely descriptive and is not entitled to trademark protection except to the extent of its secondary meaning. By the way, don't bother to sue NSI if you think that it injured you by issuing a domain name that infringes your trademark-the federal courts in California have already ruled that NSI is not liable in this situation

A federal court in New Jersey decided, in September, 1998, that the financial services company Citigroup (formed by merging Citibank and Travelers' Group) could not use the domain name "citigroup.com" because it was confusingly similar to "citgroup.com", the domain name already used by CIT Group, a rival financial-services company. (It's very possible that the outcome would have been different if CIT had been a gasoline company, a clothing manufacturer, or any other company that was not a direct competitor for the same customers in the same financial-services marketplace.) However, the court agreed with Citigroup that it had not violated CIT's trademark..

Note that, in the real world, CIT Group looks different from Citigroup, but URLs are usually written out in all lower-case letters, because not all of the hardware and software used on the Internet is "case-sensitive" (able to recognize the difference between capital and lower-case letters). Furthermore, URLs can't have spaces; either each element must be written out as a single word, or underscores or hyphens must be used.

An interesting 1997 case from Oregon involves a company whose trademark, Epix ® was used in connection with its video imaging hardware/software business. A theater group used the name epix.com (short for "electronic pictures") to publicize its Rocky Horror Show production. The video imaging company claimed trademark infringement and unfair competition, but lost because the court did not believe that consumer confusion was possible, given the great differences between a theatrical production and a video card.

In contrast, the Northern District of Iowa did issue an injunction forbidding a company to use its registered domain name, greenproducts.com; one of its competitors held the registered trademark Green Products. The defendant said that its greenproducts.com Website would avoid confusion by providing "comparative advertising" about the merits of each company's products. The court found this extremely unpersuasive: "In essence, Independence is capitalizing on the strong similarity between Green Products' trademark and its domain name to lure customers onto its web page. This Court finds that such a deceptive use of a competitor's trademark as a way to lure customers away from the competitor is a kind of consumer confusion." The defendant not only had to stop using greenproducts.com as a domain name, it had to transfer the domain name to the plaintiff.

C. Linking, Framing, and Caching

One of the most basic characteristics of the Internet is that it permits hyperlinking: i.e., it is possible to click on an active area, and have material identified by that "link" displayed on the user's computer screen. In addition to simple movement to the link, "framing" and "caching" are also technically possible. Framing is somewhat similar to linking, but in framing, material from another site is displayed as part of the "framer's" site. (When linking occurs, it is clear that the user has moved to another site, sponsored by someone else.) Caching lets Web Site A display the entire contents of Web Site B as of a particular moment in time.

The federal Copyright Act and its regulations do not provide specific guidance for what is permissible in terms of linking, framing, or caching. Some cases have been brought, but there is no firm guidance, because most of the cases were settled before trial.

The consensus that seems to be emerging is that it is permissible to link to another site, even without explicit permission-as long as linking has not been explicitly forbidden. (If you want to limit or restrict linking of your site, you can use technical means, such as imposing a registration or password requirement, or setting up your site so that the URL changes frequently to frustrate linkers. Of course, you may also be frustrating legitimate users whose attention is valuable to you.) The American Bar Association has drafted a detailed agreement for linking, with guidance for its use; you can purchase this "Web Linking Agreement: Contracting Strategies and Model Provisions" from <http://www.abanet.org>. (No, it's not free, but what do you expect from a bunch of lawyers?)

It's good policy to place a notice on your site indicating that, for instance, you provide links to sites maintained by other companies and organizations, but that you are not responsible for the content of these other sites and are not promising that content of the linked sites is accurate, or

making any warranties as to the quality of products or services featured on the sites to which you link. Furthermore, it's better practice to use plain text links to other sites; using an icon or logo could constitute misuse of the trademark represented by that logo.

However, framing has different legal consequences from mere linking. Framing can constitute unfair competition or trademark infringement, because you are "passing off" material from another site as your own, implying an association between companies that does not actually exist, and gaining additional traffic for your site (from people who want to see the "framed" content) and maybe even increasing your site's revenues, for instance if you have advertisers who pay on the basis of the number of times their advertisement is viewed. If your site refers to "our" products, you may be guilty of unfair business practices if, in fact, some of the products appear on a framed site rather than your own.

Caching is even more likely to create liability, because the owner of the site may be able to claim copyright infringement as well as trademark and unfair competition liability.

IV. Patent Issues

The Internet has shaken up the once-placid world of patents, just as it has affected copyright and trademark law. Patents are usually granted for tangible inventions or processes. However, several computerized business methods have been patented, including Cash Management Accounts, computerized auctions, small payments made as an incentive for Web users to read advertisements, and the "shopping carts" used to manage orders from transactional Websites. (The involvement of a computer actually promotes patentability, because it turns what might otherwise have been an unpatentable algorithm into a process that does justify patent protection.)

This is a two-edged sword. First, if you have an innovative e-commerce method, you may qualify for a patent, and can charge licensing fees to others who use your patented method. But the downside is that you may be infringing on other companies' patents. You'll have to tread carefully and get expert advice. The Patent and Trademark Office's Examination Guidelines for Computer Related Inventions (or the Computer Guidelines, for short, published in 61 Federal Register 7478 (2/28/96) give the requirements that the PTO uses in examining a patent application to see if there is a valid, patentable invention.

V. Liability Issues For On-Line Publishers And Distributors

A. Content Regulation

In 1996, as part of the Telecommunications Act, Congress passed the Communications Decency Act (CDA). The CDA made it a federal crime to grant minors access over the Internet to "indecent" transmissions of "patently offensive" displays. In 1997, the Supreme Court found the CDA unconstitutional, in the case of *Reno v. American Civil Liberties Union*, 117 S.Ct. 2329 (1997), on the grounds that it was vague, overbroad, and impermissibly restricted adults' access to controversial content.

Since then, Congress has attempted to draft bills (e.g., Senate 1482, Communications Decency Act II, and H.R. 3783, Child Online Protection Act) that are narrow enough to pass muster on the Constitutional level. The Child Online Protection Act (COPA), enacted at 47 USC §101, is a narrower law that imposes criminal penalties for permitting minors to access obscene material that is harmful to them. It is a defense that the site accused of a COPA violation that it used technologically feasible measures, such as requiring a credit card or an adult access code, to keep minors away from the harmful material. Enforcement of COPA has been enjoined by the Eastern District of Pennsylvania (*ACLU v. Reno*, No. 98-5591 (E.D. Pa. 11/20/98), because the court found that COPA violates adults' First Amendment Rights and the defensive mechanisms would

not be economically or technologically feasible.

In addition to obscene material to which children may be exposed on-line, service providers and site owners should be sure that their sites are free of child pornography-sexually explicit material that exploits children, in violation of 18 USC §§2251 and 2256(8), as well as various state laws. Child pornography created, for example, by manipulating non-obscene photographs of children to create obscenity is illegal (18 USC §2252A), and using computer networks to transmit child pornography definitely violates the anti-child-pornography statutes.

Some federal statutes banning pornography that does not involve children apply to Internet distribution of pornography (such as 18 USC §§1462 and 1465), but §1466, engaging in the business or selling or transferring obscene matter-does not, because the statutory language fails to refer to computers and computer networks.

Although it is a complicated issue that falls outside the scope of this paper, the basic definition of pornography is sexually explicit material that violates community standards. When the Internet is involved, the question of which community becomes very relevant. According to the Sixth Circuit's 1996 Thomas decision, the relevant community is the one where the pornographic materials were downloaded, not the place where they were created or placed on the network server. (This seems kind of unfair, since the person who downloaded the files presumably wasn't offended, but that's the rule.)

While these problems are being worked out, you may wish to protect yourself by adding a voluntary rating system, indicating whether materials on your site include nudity, four-letter words, sexually explicit materials, political speech, and other material which, even if lawful to transmit, may be offensive to some users or unsuitable for young users.

Although pornography is the major issue usually thought of in terms of content regulation, it is not the only one. Contests and sweepstakes must avoid deception as to what the prizes are, who is eligible to play, who is eligible to win, and what the odds of winning are. Even if all these hurdles are met, a contest or sweepstakes that involves luck rather than skill (or a predominance of luck over skill) may be deemed illegal gambling in many states; Internet gambling is not favored by U.S. law.

The Northern District of Georgia struck down a Georgia statute that made it a crime knowingly to transmit data over a computer network using a false ID, or knowingly to use a trade name, trademark, or logo to create a false impression of permission to use the corporate identity material. The court found (*ACLU v Miller*, 977 Fed.Supp. 1228 (N.D.Ga. 1997)) that the law was an overly broad, content-based restriction on free speech, and was vague enough to be unconstitutional.

B. Defamation

In addition to its concerns with protecting children from obscene matter, the CDA contained some interesting indemnification provisions to protect on-line service providers from liability based on information that they distributed but did not publish (i.e., whose content they did not furnish, supervise, or control). This indemnification clarified some earlier case law, which implied that on-line services could become liable for defamatory statements appearing on the service, if the on-line service moderated or exercised some degree of editorial or other control over message boards.

Defamation consists of damaging someone's good name or reputation by making untrue factual

statements. (Pure statements of opinion cannot be defamatory; true statements are never defamatory; and some leeway is permitted for political commentary.) One-to-one oral defamation is slander; written or published defamation is libel. It is clear that material on the Internet, or e-mail, can constitute libel.

On December 28, 1998, a New York appellate court ruled that Prodigy Communications Corporation was not liable for threatening prank communications falsely issued in the name of one of its subscribers. Prodigy's lack of editorial function or supervision in transmission of the message insulated it from liability.

VI. Important Recent Legislation

The summer and fall of 1998 were important in the history of intellectual property law; several important pieces of legislation were passed, and other important bills were in the pipeline (including a revised version of the Communications Decency Act).

A. Digital Millennium Copyright Act

In the real world, it's impractical for Internet Service Providers (ISPs) to monitor not only the ever-changing content of the sites that use their service, but the traffic on message boards and in chat rooms. Unfortunately, however, many kinds of illegal activity could be occurring: manipulation of stock prices and securities fraud; pornography; libel; passing around copyrighted software and music files, for instance. The DMCA creates a procedure that ISPs and related service providers (such as those that provide network access or router service) can use to protect themselves from liability. Protection is available in connection with system caching; transitory digital network communications; information placed on the system by a customer; and hyperlinks and other navigational tools. A "service provider," under 17 USC §512(k)(1), provides on-line services or network access, or operates facilities for on-line services or network access. The service provider just stores, forwards, or routes information supplied by others, and does not select or edit the material or determine who receives it. The DMCA specifically permits "system caching" i.e., retaining a copy of a site so that other users can access it faster.

The Digital Millennium Copyright Act protection depends on the service provider's maintaining a policy of kicking out customers that they know engage in repeated copyright infringement. The policy must be communicated to customers (so they know what not to do) and must actually be enforced, not just stated. Service providers who benefit financially from the infringement are not entitled to protection.

What happens if one of the service provider's customers does, in fact, commit copyright infringement (for instance, by maintaining a "warez board" containing pirated software)? To earn protection under the Digital Millennium Copyright Act, as soon as the service provider receives notice of infringing material, it must move as soon as possible to remove the material from the on-line service, or to prevent access to it. Not doing this means that the service provider can still be sued by the copyright proprietor of the infringed material. Copyright owners also have the right to demand information about the infringer.

The service provider must designate an agent for notification of claimed infringement: i.e., someone to whom copyright proprietors can complain. See <http://lcweb.loc.gov/copyright/onlinesp/> for the procedure for designating an agent. The Copyright Office maintains a publicly-available list of designated agents, so it's always easy to find out where complaints of infringement should be addressed.

The DMCA requires the integrity of Copyright Management Information (CMI) to be preserved.

CMI constitutes data about the work, its author, who owns the copyright, and, if applicable, who the performer or director is. It's illegal to falsify this information, or to remove it or alter it without permission. (Digital "watermarks" can be applied to text or images to identify their origin, facilitate "pay-per-view" access, or prevent unauthorized copying or alteration.)

B. Y2K Information and Readiness Disclosure Act (Y2K Act)

Congress' response to the looming Y2K problem is a law, P.L. 105-271 (enacted 10/19/98) that encourages companies to prepare for Y2K by immunizing them from liability in certain circumstances and encouraging them to exchange information freely with other companies and disclose their own Y2K preparedness status without fear of lawsuit (as long as they do not make deliberately false statements about this issue). Furthermore, companies—even direct competitors—can get together to implement uniform Y2K policies without worrying about antitrust liability.

However, the Y2K Act does not apply to actions brought by consumers based on advertisements and other solicitations to buy consumer products, and does not prevent claims that are not based exclusively on Y2K claims. Nor does it reduce the duty of care owed by any fiduciary (party responsible for someone else's money or finances). Intellectual property rights are unaffected, and plaintiffs can still seek injunctions based on Y2K statements.

Even for sales of Y2K remediation products and services by one business to another, the maker of the statement provides the required notice. The notice says "Statements made to you in the course of this sale are subject to the Year 2000 Information and Readiness Disclosure Act [with the P.L. number]. In the case of a dispute this Act may reduce your legal rights regarding the use of any such statements, unless otherwise specified by your contract or tariff."

The law doesn't apply to any lawsuit that was already pending by July 14, 1998, but does apply to Y2K statements made between July 14, 1998 and July 14, 2001, with special rules for statements made between January 1, 1996 and July 14, 1998.

C. The Internet Tax Freedom Act and Sales Taxes on Internet Transactions

The Internet Tax Freedom Act, passed July 29, 1998 (it doesn't have a P.L. number yet), finally carries out President Bush's campaign pledge, "Read my lips—no new taxes." In the Internet Tax Freedom Act, Congress has created a two-year moratorium, beginning July 29, 1998 during which states will not be allowed to impose any NEW taxes that are specific to e-commerce or Internet access. ITFA §201 says that "it is the sense of Congress that no new Federal taxes similar to" the state taxes covered by the moratorium "should be enacted with respect to the Internet and Internet access during the moratorium"—but this stops far short of either a ban on new federal taxes or a promise by Congress that it will hold off on imposing new taxes.

This law has been widely misunderstood. It doesn't mean that states are not allowed to impose sales tax on on-line purchases. After all, bricks-and-mortar stores are already worried about competition from on-line merchants; it would be politically unsound to give extra help to e-commerce sites.

While the moratorium lasts, states are allowed to enforce tax laws that were already on their books (such as sales taxes generally applicable to all transactions, or even special taxes imposed only on Internet access or other forms of telecommunications). They are even allowed to adopt new tax laws of general application, or to increase sales taxes, but not to add new taxes that cover electronic communications, or on-line sales, but nothing else. However, the moratorium does NOT apply to providing Internet access as part of a package including other services (e.g., bundled with phone service), unless the service provider breaks out the part of the bill that is

traceable to Internet services. For ITFA purposes, "online services" means "the offering or provision of information, information processing, and products or services to a user as part of a package of services that are combined with Internet access service and offered to the user for a single price." "Internet access service" is defined as service (other than telecommunications services already regulated under other federal laws) "that enables users to access content, information, electronic mail, or other services offered over the Internet., and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers."

ITFA §203 expresses Congress' belief that international e-commerce should be free of tariffs and similar barriers, and discriminatory regulations or taxation, and directs the President to try to negotiate treaties and other international agreements to preserve on-line freedom of trade.

Therefore, after ITFA, on-line e-commerce is treated exactly the same way for sales tax purposes as telephone or mail orders. That is, a seller must collect sales tax on all sales made in its state of incorporation (unless, of course, the state doesn't have a sales tax). It must also collect sales tax on sales made in any states in which the seller has "physical presence". Obvious examples of physical presence are branch offices, stores, and warehouses. Less obvious examples are salespeople sent into other states on a regular basis to solicit orders; repeated presentations at trade shows in the same state; and even locating a router in the state. Since coast-to-coast Internet transmission often requires 15-20 router locations, this last point can create a lot of sales tax liability!

1. Basic Sales Tax Principles

Sales to consumers are subject to sales tax. (Although hardly anyone does it, consumers are legally obligated to calculate and pay use tax on items that they purchased out of state and on which no sales tax was collected.) Sales to businesses are subject to sales tax if the items are for use by the business itself (e.g., office supplies) but are not subject to sales tax if the items will be re-sold by the purchaser, or will be used in manufacturing. You should get re-sale certificates from all customers who claim exemption from sales tax, and should keep these on file in case you become subject to a sales tax audit.

As if things weren't confusing enough already, not all states impose sales tax on the same basis. Some of them impose tax only on the merchandise itself; some on merchandise plus shipping and handling; some on shipping but not handling, or vice versa. The only answer is to get advice from an attorney and/or accountant specializing in sales tax matters. For practicality, your shopping carts and other software used in e-commerce should be programmed to calculate sales tax (and EU value-added tax) and add it to the total; it's much easier to "gray out" lines of a form that are not needed in a particular state, than to re-program later to add a new capacity.

VII: Protection of Consumers

Perhaps there is nothing new under the sun; and many of the problems of e-commerce and on-line securities trading are simply old-fashioned larceny and fraud, adopting new media. However, in addition to problems that are or should be obvious to consumers, there are hidden dangers, including misuse of information supplied by consumers (for instance, when they register at a site or place an order for merchandise) or gathered automatically from the consumers' computers (in the form of "cookies"). A cookie is a file that appears on the browser's hard drive and contains information about that computer—information that can be tracked by the operators of sites to which the computer connects.

Many ISPs and other service providers draft their contracts with persons, companies, and

organizations whose sites they host to provide that the service provider will not be responsible for "consequential damages"—i.e., lost business or suits by ultimate consumers if, for instance, there is a service outage or transmissions are garbled.

Don't forget that any site can be accessed outside the United States. Some countries (generally French-speaking) require at least some content in their own native language in commercial materials used in the country. If sales are made outside the United States, there is an excellent chance that the law of the purchaser's country, not U.S. law, will apply. Under German law, German law applies to ALL Websites that can be accessed in Germany, and the European Union's rule is that the law of the consumer's home country applies, even if the purchase was made under a contract specifying adherence to laws of another country (e.g., the United States).

A. Privacy Protection

Once the owner of a site collects information about site usage, it can do many things with the information—some negative, some positive. The owner can use the information to contact the site user, perhaps supplying valued information or giving the user the ability to purchase something that the user wants. A user who has already ordered merchandise can be urged to purchase additional merchandise, perhaps based on the orders already placed or based on orders placed by other customers who have similar tastes. The site owner can also sell information about a particular customer and that customer's preferences, or can aggregate information about all its customers and sell the aggregated database or interpretations of it. In many cases, customers give information—or it is possible to deduce information—that the customer does not want generally known: e.g., sexual preference, controversial religious or social beliefs, participation in a 12-Step Program.

1. FTC Measures

The Federal Trade Commission has issued a report on on-line privacy in 1998, to determine if self-regulation by business will adequately protect consumer privacy. The conclusion is skeptical, and the agency recommends legislation and other measures for change. The FTC has also published an administrative notice, soliciting industry and consumer comments, in 63 Federal Register 24996 (May 6, 1998), to clarify the application of FTC requirements (e.g., for disclaimers in advertisements) to electronic communications.

The FTC report says that notice, choice, access, and security are the four most important principles for making sure that "collection, use, and dissemination of personal information are conducted fairly and in a manner consistent with consumer privacy interests." The FTC conceded that business self-regulatory guidelines usually provide notice of information practices and a degree of choice, but are deficient with respect to access (consumers' ability to view their data and confirm its accuracy) and security (protection against unauthorized use and disclosure of information about the consumers). The FTC found that consumers are usually worried about misuse of personal information—especially personal information about child users of the Internet, so the FTC recommends that Congress adopt laws giving parents greater control over information collected about their children.

GeoCities, the on-line "community builder," has been charged by the FTC with improper collection of information on its Website, misrepresentation of the purpose behind its collection of personal identifying information, deceptive practices in collecting information from children, and improper use of the information. GeoCities has entered into a settlement agreement with the FTC forbidding misrepresentation of the reason for collecting consumer information; requiring the site to display a clear, prominent privacy notice disclosing information that is being collected, why, who has access to the information, and how consumers can correct or remove information about

themselves. Parental consent is required before GeoCities can collect information about children under twelve.

GeoCities was able to settle the FTC case without monetary liability, but companies that fail to heed its example may be fined by the FTC or sued by angry customers. The antidote is to maintain an appropriate privacy policy, disclose it to consumers, make sure that customer data is secure and protected from hackers, and do not depart from your own guidelines about re-use or sale of information.

2. EU Directive

The European Union has far less faith in the power of the market to regulate itself. It has issued a directive on protection of privacy of personal data, which took effect in October, 1998. Any site within the European Union that gathers electronic data must post privacy policies; disclose the use of the data; and grant access so individuals can monitor and alter data about them, or object to use of the data. Sites are not permitted to collect irrelevant data, or an amount of data that is excessive in light of the purpose of the sight. Furthermore, identifying characteristics of identifying site users may not be retained longer than purpose for which the data was collected remains in force. All EU member states are required to create an enforcement authority for the policy and to impose penalties on businesses that violate the rules.

The EU directive also forbids transfer of personal data to non-EU countries that fail to ensure an adequate level of protection—and, pending the outcome of negotiations, the United States is regarded as such a country.

B. False Advertising

The same principles of truth in advertising apply, regardless of whether the statement is made in print, on a broadcast, or electronically. However, certain adjustments were already made prior to widespread Internet use: e.g., more "fine print" disclosure information is required in print ads than in television commercials.

As of the end of 1998, the FTC had already brought about three dozen enforcement actions to halt or penalize on-line scams, but most of these cases simply used electronic means to carry out "traditional" frauds such as pyramid schemes.

The agency published a set of guidelines for on-line commerce and electronic publishing (including CD-ROMs and e-mail, not just the Web) early in 1998. There's nothing really revolutionary about the guidelines, because they simply carry ordinary standards of honesty and openness to the electronic marketplace:

Endorsements: The advertiser should disclose real performance buyers can expect (unless the endorsement reasonably represents real-world performance)

Warranties: If a product warranty is mentioned, the viewer should be given information about where the full warranty can be examined

Specific products: The FTC has rules about products such as jewelry, tires, furs, and leather, requiring disclosure of the actual composition of the product.

Required disclosures: Display on the Internet should make the disclosures "unavoidable"; it's not enough to bury them somewhere on the site, several clicks deep. The FTC suggests (but doesn't require) the mandatory disclosures should be on the same Web page as the offer to sell the merchandise; this can be done by keeping the disclosures in a frame that remains on-screen as the

viewer scrolls through information about the various products on offer. The FTC doesn't require an "I accept" or "I understand the terms" button as part of the ordering process, but it makes sense for on-line merchants to protect themselves by getting consumers to indicate that they did read the on-line equivalent of the "fine print."

C. Credit Card Fraud

Many consumers are apprehensive about inputting their credit card information into on-line order forms, although it has often been pointed out that the danger is no greater than in letting a store clerk or waiter see a physical charge plate, or giving a card number over the telephone. Furthermore, although there have been instances of hackers maliciously intercepting credit card numbers, and even posting this information to hacker bulletin boards, there has been little or no actual credit card fraud occurring through this medium.

The consumer's vulnerability to on-line credit card fraud is quite low, because of the federal law protective mandate that applies to all uses of credit cards. Under 15 USC §1643, a cardholder's liability for unauthorized use of the card is limited to \$50, as long as the card issuer maintains a commercially reasonable policy for reporting lost and stolen cards and card misuse, and as long as the cardholder follows the policy. In fact, many card issuers will even waive the \$50 as a courtesy to their cardholders (or the owner of the site will agree to indemnify their customers against credit card fraud).

The benefit to merchants of accepting credit cards (less risk of check fraud; less need to keep large sums of money on the premises; encouragement of mail and Internet orders; freer spending by customers who don't have to pay right away) are so great that they, and the banks that issue the cards, are willing to accept some risk of fraud, and to insulate consumers from significant financial risk even if their cards or card information are stolen, misused, or misappropriated.

Incidentally, we will soon be seeing a large-scale early test of Y2K readiness, as consumers begin to use credit cards with post-1/1/2000 expiration dates.

D. Securities Fraud

In this arena, the Securities and Exchange Commission (SEC), not the FTC, is the lead agency. Although in effect the Internet merely facilitates the basic techniques of fraud and securities manipulation, it has already become a problem area. For instance, many people buy and sell securities on the basis of tips given on bulletin boards and in chat rooms; some of this information is well-intended, but some of it is deliberately deceptive or involves illegal insider trading. The SEC maintains a special Website specifically for complaints of on-line securities fraud: the "Internet Enforcement Complaint Center," <http://www.sec.gov/enforce/comctr.htm>.

E. Spam

Spam is unsolicited consumer e-mail, but the recipient's perception of what constitutes spam can be very different from the sender's perception. An ISP or other service provider has the right to draft its contracts to forbid spamming by service users, and to enforce such contract provisions by kicking violators off the service. A legal theory that has worked in some cases is "trespass to chattel": i.e., abuse and misuse of the service provider's business property by the spammer (the CyberPromotions case noted above took this position). Sometimes abusive spam operations use counterfeit e-mail addresses (to prevent recognition of the messages as spam, and consequent deletion by recipients unread); this can constitute infringement or dilution of any trademark that is used in the counterfeit address (as in the Hotmail case noted above).

There are anti-spam laws in some states (and such legislation is pending in several other state

legislatures). Similar bills have been introduced in Congress, but none has yet become law.

F. Click-Wrap Agreements

Traditional contract law assumes that contracts are made between parties of relatively equal power, after they've had a chance for face-to-face negotiations. This assumption is very unrealistic in the Web context, for two reasons. First of all, most contracts are offered by a comparatively sophisticated corporation to a consumer who doesn't know much about contract law (and usually cares less). Second, the speed of on-line commerce is such that there's no opportunity for back-and-forth discussions. The buyer of software, or the user of an on-line service, is usually placed in a "take it or leave it" position: either accept the seller's/service provider's terms, or do without the desired electronic product or service.

A shrink-wrap license is the set of detailed terms, usually in small print, that appears on the box software is packaged in. It's called a shrink-wrap license because (if you're patient and have a magnifying glass) you can read the terms before you unwrap the software; but once you tear open the wrapping, you are deemed to have agreed to the terms. For a while, courts were dubious about the validity of these non-negotiated arguments, but since 1996, their validity has been upheld both for computer software and computer hardware.

A "click-wrap" agreement is the Internet equivalent of a shrink-wrap agreement. Typically, a click-wrap agreement appears on the computer screen as part of the Terms of Service for an on-line service, or in connection with downloading software. The potential user has to indicate agreement with the terms of the agreement (usually by clicking on an "I Agree" check-box) in order to use the service or obtain the software.

The Northern District of California has ruled that click-wrap agreements can be enforced by the courts, even though the user has no real chance to negotiate. Probably, in the future, shrink-wrap and click-wrap agreements will gain even greater legal status. That's because the legal scholars who are revising the Uniform Commercial Code (UCC) to cope with e-commerce have suggested new UCC provisions that make shrink-wrap and click-wrap agreements enforceable if computer users indicate explicit agreement with the terms—or if their conduct (such as use of the service, software, or hardware) indicates agreement.

VIII: Jurisdiction: Where You Can Be Sued Based On On-Line Activities

The Web is short for World Wide Web, and except in unusual cases (such as a password-protected site where passwords are issued in only one state), its reach is indeed multi-national. Yet the average business that has a Website, or the average service provider, has offices in only one state or a few states, and probably won't have any offices outside the United States at all. Does that mean that people outside that state or those states will not be able to sue the service provider or the business that operates the Website? Or will they have to go to the courts of the state where the business is located, even if this is not convenient for them?

A court can hear a case only if it has both "subject matter jurisdiction" over the case itself, and "personal jurisdiction" over the parties. There are some issues that can only be heard in federal courts, because they involve questions of federal law and are areas in which the states are supposed to stay out of the picture. (This is called "federal question jurisdiction.")

Federal courts can also hear certain cases where the plaintiff and defendant come from different states; this provision was added to the Constitution because of a fear that courts in one state would always be prejudiced in favor of local people and against "outsiders" from other states. But a plaintiff who wants a federal court to exercise this "diversity jurisdiction" has to be able to claim damages of at least \$75,000; smaller cases can only be heard in state court.

Therefore, the vast majority of cases end up in state court—either because they involve only state issues, or because they're too small for federal court, or because the plaintiff prefers state court (where the case can generally be heard a lot faster, and where remedies unavailable in federal court might be available). So then the question becomes WHICH state the case will be brought in.

State courts always have jurisdiction over the citizens of their own state, so it's always appropriate to go to the state where the defendant lives and sue there. To look at it from the other viewpoint, any person or business is vulnerable to suit in the state where the person lives, or a corporation is incorporated—and may also be vulnerable to suit in many other states, because of so-called "long-arm jurisdiction." Long-arm jurisdiction permits a defendant to be sued in any state in which he, she, or it has at least "minimum contacts"—but not in any state where minimum contacts are lacking.

Doing business in a state definitely provides those minimum contacts, so a company that has a transactional Website, or provides Internet service in any state, can certainly be sued there. The problem is more difficult for a Website that is not transactional, and where the user does not pay to access it, because it could be argued that there are no minimum contacts between the "publisher" of the site and that state, and that it would be unfair to make the defendant appear in an inconvenient state to defend itself. (Maybe in the future, there'll be an on-line cyberspace court just to deal with these issues, and nobody will have to "appear" in a physical courtroom at all.)

So far, there have been a number of court cases about jurisdiction over Websites. Most of the cases say that a company that has a Website can be sued in the home state of anyone who accesses the Website and claims some form of injury as a result, although some of the cases draw a distinction between an "active" Website (which gives rise to jurisdiction) and a "passive" Website which does not. However, New York courts have been much less willing to accept jurisdiction based on electronic contacts with the state.

In short, you may have to defend yourself in courts of states other than the one(s) in which you have an office, or even any physical presence (such as network hardware). One way in which you may be able to protect yourself is drafting your contracts to include a provision that the contract should be interpreted according to the law of a state (such as New York) that has a narrow interpretation of when Internet activities confer jurisdiction. However, there is always a risk that the contract will be interpreted under the "choice of law" rules of a state that will not adopt the jurisdictional rules that are favorable to your position. ("Choice of law" is an area of law that determines which state's law should apply, if there are two or more possibilities.)