



Web Wise

A guide to the issues and exposures of E-Commerce

Prepared by:

Peggy Patterson CPCU
AON GROWTHWORKS
303-639-4154

This article is a publication of Aon Corporation and should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general information purposes only, and you are urged to consult your own lawyer concerning your own situation and any specific legal questions you may have

<i>Categories of e-business</i>	<i>1</i>
Types of websites	1
E-Commerce Business Models	1
<i>Infringement</i>	<i>2</i>
Copyright Infringement	2
Insurance Available	4
Patent Infringement	4
Insurance Available	4
Trademark Infringement/Cybersquatting	5
Insurance Available	6
Inevitable Misappropriation Doctrine	7
Other Infringements & Violations	7
Insurance Available	7
<i>Defamation</i>	<i>8</i>
Insurance Available	8
<i>Privacy</i>	<i>8</i>
Insurance Available	9
<i>Legal & Regulatory Issues</i>	<i>9</i>
Taxation	9
Regulated Products	10
Freedom of Speech	11
SEC Regulations	11
Illegal Activities	12
Spam & Netiquette	13
Digital Signatures & Certificates	14
Privacy Legislation & Regulations	14
Jurisdiction	16
Insurance Issues	16
<i>Contractual Liabilities</i>	<i>17</i>
Breach of contract	17
Online Contracts	17
Conflicts with other Channels of Distribution	18
Denial of Service/Repudiation of Access	18
Unauthorized Access	18
<i>Extortion</i>	<i>18</i>
<i>Damage to Property</i>	<i>19</i>

First Party	19
Intellectual Property	19
Property of Others	20
Business Income	21
<i>Disaster Recovery</i>	<i>22</i>
<i>Consumer Fraud</i>	<i>23</i>
<i>Antitrust/Unfair Competition</i>	<i>23</i>
<i>False Advertising</i>	<i>23</i>
<i>Tortious Interference</i>	<i>24</i>

The Internet poses unique problems because of its global reach and digital format. Its phenomenal growth contributes to the confusion by posing as yet unanswered legal and regulatory questions. The entrants into electronic commerce are often unaware of some of the more troublesome aspects of their industry. As insurance and risk management professionals, we also struggle to stay abreast of these issues and advise our clients. The purpose of this paper is to highlight some of the unique exposures faced by the burgeoning e-commerce industry and to identify some of the shortcomings of traditional insurance offerings as they relate to these exposures.

Categories of e-business

Types of websites

In general, there are three types of e-business websites:

Passive – these websites only offer information about the company – similar to a print advertisement. A company operating a Passive website faces few new exposures. These would be limited to:

- Infringement of copyright, trademark, patent, etc. in the design or content of the website
- Defamation of persons or products based on the content of the website
- Jurisdictional issues due to its presence on the web
- False advertising or Unfair competition resulting from the content of the website

Interactive – these websites allow the customer to interact with the website by requesting or providing information. These sites may contain chat rooms or other interactive forums. In addition to the exposures faced by a Passive website owner, the Interactive site operator faces:

- Privacy violation from information gathered or displayed on the site
- Unauthorized access of information gathered or displayed on the site
- Extortion based on unauthorized access
- Theft of intellectual property

Active – these websites allow the customer to actually make purchases from the website. In addition to the exposures identified above, the Active website owner faces:

- Tax issues from sales via the web
- Compliance with varying regulations regarding the sale of regulated products
- SEC regulations if involved in these types of transactions
- Digital certificate failure
- Consumer fraud
- Repudiation of Access
- Increased contractual liability exposures
- Loss of business income if the website is shut down

E-Commerce Business Models

There are four business models for e-commerce:

- Business to Business (Cisco)
- Business to Consumer (Amazon.com)
- Consumer to Consumer (eBay)
- Consumer to Business (Priceline.com)

Infringement

Traditional 'Bricks & Mortar' businesses can face claims alleging many different kinds of infringement. An e-business faces these same exposures but on a magnified scale because of the ease and anonymity the Internet provides.

Copyright Infringement

The most common type of infringement claim is Copyright Infringement. In the United States, federal copyright law protects original works of authorship fixed in a tangible medium of expression. Copyright law imposes absolute liability (injunctive or monetary relief whether violation is intentional or accidental) for violations of the five types of copyrights: Reproduction, Distribution, Modification, Public Performance and Public Display.

The ease of access to information on the Internet creates broad potential liability under copyright law. A person need not know that he is infringing on a copyright to be liable. This broad liability extends not only for a company's own acts but also for acts of third parties. The liability that comes from third parties can be Vicarious or Contributory:

Vicarious Infringement is assessed when the defendant has a relationship with the third party infringer that makes it unfair not to impose liability. Usually, the defendant has supervisory control over the infringer.

Contributory Infringement is assessed when the defendant knowingly induces or contributes to the infringement.

Unlike the source code of most other computer programs, the source code of Web pages is not secret and can be accessed with the help of any Web browser. Source code and object code are 'literal elements' of a program which are protected by copyright law as 'literary works'. In addition, not only the code itself, but also the computer screen displays, as non-literal elements generated by the underlying code, may be independently protected by copyright. Since Web pages are stored permanently on a server, they are also fixed in a tangible medium of expression, as required by 17 U.S.C. § 102(a).

Web pages may contain text, images, audio and video clips. These elements may independently qualify for copyright protection as literary or audiovisual works or sound recordings. Even though Web pages are computer programs and are protected as such, they are mostly used as "carriers" for copyrighted works which happen to be stored in digital format.

Browsing the Internet and viewing its contents does not implicate the copyright laws, as long as the Web pages loaded into the user's computer RAM are neither printed nor saved to a permanent storage device. Similarly, linking to other Web pages using the plain URL only does not involve any exclusive copyrights. However, embedding links and framing could infringe the copyright owner's adaptation right, and the Web page creators should seek permission from the respective copyright owner prior to framing or embedding copyrighted material. Caching and mirroring also fall within the scope of certain exclusive copyrights and Internet Service Providers should be aware of the potential liability that proxy caching implies.¹

¹ "Internet Basics and Copyright Law", Jon D. Grossman and Cyril P. Rigamonti, *Journal of Internet Law*.

A recent Federal Appeals Court decision in RIAA vs. Diamond Multimedia declared that computer users have the right to "space-shift" (lawfully make copies of Copyrighted digital files they obtain lawfully). Although hotly contested by the music industry, saying it encourages piracy, the court held that computer hard drives are not subject to the Audio Home Recording Act. (The AHR Act applies to "digital audio recording devices" and requires that manufacturers of the devices must pay a royalty to artist organizations and that the devices must contain a system to prevent the making of serial copies.²)

The Digital Millennium Copyright Act (DMCA), which was signed into law on October 28, 1998, modified Copyright Law to take into consideration some of the peculiarities of doing business over the Internet. The major provision of the Act, pertaining to the Internet, provides safe harbors for some Internet activities and grants performance rights and statutory licenses for certain webcasting transmissions of sound recordings. If a service provider's (SP) activity qualifies for protection under the DMCA, it is not liable for monetary relief for claims of direct, vicarious or contributory copyright infringement based on that activity. The DMCA does permit limited injunctions against such activities in lieu of monetary damages.

Safe Harbors established by the DCMA³:

1. Conduit Functions: Applies to an SP providing transmitting, routing, or connection through a network (and intermediate and transient storage) of materials provided that the transmission was initiated by a third party, the functions were carried out automatically, a copy is maintained only so long as is reasonably necessary to perform these functions and the material is unchanged.
2. System Caching: Applies to an SP that provides temporary or intermediate storage of materials on a network provided that the material is posted by a third party, the process of storage and providing access to the material be automatic, the material must be unchanged, the material must be updated if required by the originating site, limited access to the material, and the caching must not interfere with providing information to the originating site.
3. User Storage: Applies to an SP who provides storage on its system for material at the request of a user provided that the SP must not have actual knowledge or reason to know that the material is infringing, does not receive a direct financial benefit from the material residing on its system and promptly removes or disables access to the infringing material after proper notice of potential infringement.
4. Information Locator: Applies to an SP who links or refers a user to a site with infringing material or infringing activity provided that the SP must not have actual knowledge or reason to know that the linked site is infringing and does not receive a direct financial benefit from the infringing activity and promptly removes or disables access to the infringing material after proper notice of potential infringement.

To be eligible for the safe harbors, the SP must inform its subscribers of its termination policy for repeat infringers.

The laws protecting databases have been unclear since the Supreme Court rejected copyright protection for 'fact compilations' in 1991. Two bills are in the U.S. House of Representatives that may resolve the issues arising from the subsequent use of databases by unauthorized users.

At issue in both bills are the organized collections of all sorts of information, ranging from facts as transient as stock quotes to compositions as potentially eternal as judicial decisions. Once created, others can easily duplicate and then resell the information, often

² "In Court's View, MP3 Player is Just a 'Space Shifter'", Carl S. Kaplan, *Cyber Law Journal*, *New York Times*.

³ "Digital Millennium Copyright Act: Forging the Copyright Framework for the Internet: First Steps", Mark Radcliffe, *Journal of Internet Law*.

at lower cost. The task now facing Congress is how to restrict unauthorized use without limiting the ability of others to transform or add value to the information in the database. Both bills seek to prevent unfair competition in the form of unauthorized copying, while thwarting the ability to lock up swaths of data and then charge exorbitant prices for access.

4

Insurance Available

General Liability: The standard CGL policy provides limited coverage for Copyright Infringement, and excludes coverage for insureds whose business is advertising, broadcasting, publishing or telecasting. It is limited to that provided in the Advertising Injury coverage. For instance, if the infringement involves the copying of code in the development of a product, this copyright infringement would not be covered because it did not have its nexus in advertising. The most widely used form (11/01/88) limits coverage to "an offense committed in the course of advertising your goods, products or services". Coverage only applies to suits seeking "damages" and therefore would not respond to requests for non-monetary (injunctive) relief. An insured's Vicarious or Contributory Infringement may be covered if the offense was "committed in the course of advertising your goods, products or services."

Multi-Media Policies: These policies eliminate the advertising nexus requirement of a GL policy.

E-Commerce Policies: The various supplemental E-Commerce policies provide defense of claims arising from Copyright Infringement, but specific policy forms must be addressed to determine the scope of coverage. Most will provide coverage Copyright infringement without the nexus of Advertising Injury. Few provide defense from suits seeking non-monetary relief.

Patent Infringement

Patent Law in the U.S. is based on a federal statute, the Patent Act. States are prohibited from granting protection similar to that provided by the Patent Act. Patent law protects inventions involving processes, machines, manufactures and compositions of matter ("utility" patents) and ornamental designs ("design" patents).

Inventions protected by utility patents can be electrical, mechanical, chemical, or biological in nature. There are strict requirements for the grant of utility patents and design patents

Numerous patents have been given for Internet technology, processes, designs and even computerized methods of doing business. With the proliferation of this medium, it is easy to independently develop a technology or process that is very similar to one protected by patent.

Insurance Available

General Liability: Patent infringement cannot occur in the course of Advertising activities since a patent is infringed by making, using or selling a patented item. Since the only infringement coverage provided is in relationship to Advertising Injury, no coverage for Patent Infringement is provided.

Media Professional Liability: This specialty coverage often includes Defensive Patent Infringement coverage for specified patents.

Intellectual Property Coverage: A limited amount of Defensive and Offensive (Enforcement) coverage is available from specialty markets for specified patents.

⁴ "Congress Tackles Database Law ", Harvey Berkman, *The National Law Journal*

Trademark Infringement/Cybersquatting

Trademarks and service marks are words, names, symbols or devices used by the manufacturers of goods and providers of services to identify their goods and services and to distinguish their goods and services from goods manufactured and sold by others. For trademarks used in commerce, federal trademark protection is available under a federal trademark statute, the Lanham Act.

Trademark protection is available for words, names, symbols, or devices that are capable of distinguishing the owner's goods or services from the goods or services of others. A trademark that merely describes a class of goods rather than distinguishing the trademark owner's goods from goods provided by others is not protectable.

Domain Names

Domain names and trademark rights can overlap. Even where a name associated with a company has not been registered by that company, it may qualify as a trademark if it is associated with that company. As a result, disputes have been proliferating over the ownership and use of domain names. The Federal Trademark Dilution Act creates a federal cause of action for trademark dilution (an unauthorized use of a mark that tends to weaken, blur, or tarnish the mark) in the United States for famous marks. This law is being used by trademark owners to attempt to prohibit third parties from using their marks as domain names on the Internet.

A practice known as "cybersquatting" has developed, where particularly attractive domain addresses have been registered with no intent to use the addresses, but merely to re-sell them at a profit. A number of situations have arisen where a common name has been registered by an individual (e.g., *www.macdonalds.com*) and the individual has attempted to sell the name to the organization with the brand name. Companies have fought back on this practice claiming trademark protection of the domain address. In 1998, the 9th Circuit Court of Appeals ruled that the Trademark Dilution Act is violated by cybersquatting.⁵

The Senate adopted S. 1255, The Anti-Cybersquatting Consumer Protection Act, August 5, 1999 aimed at limiting cybersquatting. The bill allows trademark owners to recover statutory damages in cases where it is proven that a trademarked name was registered in bad faith by a person who intended to unfairly profit from its sale. The measure also allows trademark owners to assert claims *in rem* seeking the forfeiture, cancellation or transfer of an infringing domain name after satisfying the court that it has tried but was unable to locate the person who registered

The U.S. Patent and Trademark Office has reported a significant increase in the number of applications to register domain names as trademarks. Such registration provides an effective basis to a) prevent others from obtaining identical domain name in the U.S. and b) preclude the use of registration of a confusingly similar trademark.

In addition to the traditional trademark issues, the Internet presents some unique trademark Infringement opportunities.

⁵ Legal Issues Associated with the Creation and Operation of Web Sites, *Richard D. Harroch, Orrick, Harrington & Sutcliffe LLP*

Metatags: Because terms contained in Web sites will be detected by search engines and used as identifiers for that Web site, designers of Web sites try to maximize the use of trademarks to gain the attention of search engines. Metatags are words contained in code that are not visible on the web site but that can be detected by search engines. Placing trademarks owned by others in this code *can* constitute Trademark Infringement and/or Unfair Competition. However, the courts have recognized some uses of Metatags as legitimate. Courts have found no Trademark Infringement where the trademark is used in good faith to index the content of the Web site.

Links: The ability to use trademarks in hyperlinks can create confusion on the part of consumers. In Playboy Enterprises, Inc. vs. Universal Tel-A-Talk, Inc., the defendant was held liable for using the Playboy trademark both in a hyperlink and in the navigational bar of its home page. These links promoted products competitive with Playboy's. Thus, the links may have been misconstrued as branding the plaintiff's products. The use of links or framed links can result in the substitution of the advertising of a defendant's products in place of those of the plaintiff, resulting in lost advertising and income. Although certain aspects of linking have been challenged, in some contexts there may be a right to use trademarks of others in connection with linking.⁶

File and Directory Names: Several suits have been filed over the use of trademarks in file or directory names.

Territorial Boundaries: Traditionally, trademark law gives the holder of a trademark the exclusive right to use the mark in a geographically defined area. Because the publication of a web page amounts to publication nationwide, and indeed worldwide, the use of a trademark to which the publisher has rights in one jurisdiction may amount to the infringement of another's rights in a different jurisdiction. Indeed, courts have found infringement in some cases based on the use of a mark on a web site. Since it is a new area of the law, it is not yet completely resolved how courts will ultimately treat this inherent conflict.⁷

Insurance Available

General Liability: The typical General Liability policy will not respond to Trademark or Servicemark Infringement claims. The 1998 ISO form will respond to infringement of Trade Dress in advertising. The 1993 & 1988 forms will respond to infringement of title and style of doing business *in advertising* which may afford some coverage. (However, in Lebas Fashion Imports of USA v. ITT Hartford Insurance Group, a California court held that the advertising injury clause in the policy was ambiguous and therefore non-advertising trademark infringement was covered)

Multi-Media Policies: These policies eliminate the advertising nexus requirement of a GL policy and often include trademark infringement, plagiarism or unauthorized use of titles, formats, ideas, characters, plots, performance of arts, or other program material, invasion of privacy, libel, slander and other forms of defamation.

E-Commerce Policies: The various supplemental E-Commerce policies provide defense of claims arising from Trademark/Servicemark Infringement but specific policy forms must be addressed to determine the scope of coverage. Few provide defense from suits seeking non-monetary (injunctive) relief.

⁶ "A Guide to Internet-Based Trademark and Unfair Competition Decisions", Mark D. Robins, *Journal of Internet Law*

⁷ "E-Commerce and the Law; Regulatory and Legal Implications of Electronic Commerce on the Insurance Industry", *Future One*, a cooperative partnership of the Independent Insurance Agents of America (IIAA)

Inevitable Misappropriation Doctrine

The inevitable misappropriation doctrine dates back over thirty years. Ex-employers seeking injunctive relief from employees who start a new job with a competitor are now using it to protect their Trade Secrets. The standards for obtaining injunctive relief under an inevitable misappropriation theory can be condensed into a three-part test, in which the ex-employer must prove:

- (1) the former employee has knowledge of the first employer's trade secrets [knowledge test];
- (2) the employee's new job duties (and the products or technology she is working on) are so similar or related to those in the former position that it would be extremely difficult for her not to rely on or use the first employer's trade secrets [similarity of jobs test]; and
- (3) the former employee and the new employer cannot be depended upon - for any number of reasons ranging from ignorance or carelessness to bad faith - to avoid using the trade secret information [dependability test].⁸

Other Infringements & Violations

Businesses on the Internet also face Infringement accusations from other causes including Infringement or Violation of:

- Trade Secrets
- Trade Dress
- Title
- Mask Works
- Confidential Information
- Non Disclosure Agreements
- Licenses
- Franchises

Insurance Available

General Liability: The General Liability policy will respond to the "oral or written publication of material that violates a person's right of privacy". The 1998 ISO form will respond to infringement of Trade Dress in the course of advertising your goods, services or products. Theft of trade secrets is not covered because the offense occurs as a result of the theft, not in the advertising. An exception has been made by the courts when the theft includes customer lists and marketing techniques used to solicit those customers to buy competing products or services.

Multi-Media Policies: These policies eliminate the advertising nexus requirement of a GL policy and often include trademark infringement, plagiarism or unauthorized use of titles, formats, ideas, characters, plots, performance of arts, or other program material, invasion of privacy, libel, slander and other forms of defamation..

E-Commerce Policies: The various supplemental E-Commerce policies provide defense of claims arising from some forms of Infringement but specific policy forms must be addressed to determine the scope of coverage. Few provide defense from suits seeking non-monetary (injunctive) relief.

⁸ TRADE SECRET MISAPPROPRIATION:ACCEPTING THE INEVITABLE?, Terrence P. McMahon, Gary E. Weiss, Sean A. Lincoln, Erin M. Farrell, Orrick, Harrington & Sutcliffe LLP

Defamation

Defamation is used to describe libel (written falsehoods) and slander (oral falsehoods). What defamation is to individual reputation loss, *trade libel* or *product disparagement* is to product or business (economic) loss.

Most courts have long held that vendors and distributors of defamatory publications are not liable *if they neither know nor have reason to know of the defamation*. The requirement that a distributor have knowledge of the defamation is rooted in the guarantees of freedom of speech and press contained in the First Amendment.

The Communications Decency Act of 1996 protects ISPs from defamation liability if they take reasonable measures to screen for offensive materials. This shield does *not* extend to most employers whose employees use e-mail and the Internet.

Sponsorship or operation of a chat service or bulletin board service raises significant (and as yet unresolved) issues of liability under defamation law. Since the very purpose of chat and bulletin board services is to permit customers to "post" messages and engage in dialogue, customers might commit acts of defamation or copyright infringement in posting messages, or in uploading material online. Decisions that have addressed whether the operator of a bulletin board or chat service is a "distributor" as opposed to a "publisher" suggest that the degree of editorial control exercised by the operator will be determinative of the question.⁹ In Cubby Inc. vs. CompuServe, the court held that:

A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor ... than that which is applied to a public library, book store or news stand would impose an undue burden on the free flow of information.

In addition, determination of whether defamation in a chat room is considered libel or slander (spoken or written) may be significant, as some jurisdictions require proof of actual loss to prove slander, but not to prove libel.

Insurance Available

General Liability: The typical Personal Injury section of the GL policy will respond to allegation of defamation of persons, goods or services from oral or written publication of material arising out of your business.

Multi-Media Policies: These policies eliminate the advertising nexus requirement of a GL policy and often includes invasion of privacy, libel, slander and other forms of defamation..

Privacy

Traditional issues of protection of privacy apply to Internet commerce, but are intensified by the easy to which e-commerce can collect and retain personal and confidential information.

⁹ "Liability Online", Richard Kurnit, *Journal of Internet Law* .

Concern over the privacy of their personal information is the reason most often cited by consumers for not making purchases over the Internet. This fear is buoyed by the practice of some Internet sites of selling customer information.

Examples of personal information that is often gathered from consumers and/or maintained in databases that are accessible over the internet are:

- Credit information
- Financial Records
- Personal History / Preferences
- Passwords
- Criminal records
- Medical Information

In early 1998 the FTC conducted a survey of over 1400 industry sites to determine the extent to which customer privacy was being protected. The survey found that while 85 percent of the sampled sites collected personal information from consumers, only 14 percent of them referenced their information collection practices and only two percent made their privacy policies available for review. The FTC concluded that the industry's efforts to encourage voluntary adoption of the most basic fair information practices have fallen short of what is needed to protect consumers. In the wake of the FTC's report to Congress, and the threat that the federal government might impose its own system of regulation, industry groups have stepped up efforts to encourage self-regulation.

Inter-personal e-mails are afforded the same protection as first class mail by the Electronic Communications Privacy Act of 1986. The ECPA does not protect employees from having their e-mails monitored by an employer. However, a recent Minnesota case did recognize the privacy tort of invasion in a case involving the monitoring of employee e-mail.

Insurance Available

General Liability: A GL policy will only respond to allegations of invasion of privacy arising out of the oral or written publication of material. Therefore, allegations of a breach of security which results in an invasion of privacy would not be covered.

Multi-Media Policies: These policies eliminate the advertising nexus requirement of a GL policy and often include invasion of privacy, libel, slander and other forms of defamation.
E&O: Many E&O forms exclude breach of security which may eliminate important coverage for privacy violations.

Legal & Regulatory Issues

Taxation

Although Internet retailers take the position that state and local sales taxes do not apply if the company has no presence in the state where sales are made through their Web site, the nation's 30,000 local, state and federal taxing authorities are quite aware of the revenue potential of the Internet. Each one of these jurisdictions potentially could levy taxes on monthly Internet access fees, the sale of goods and services over the Internet, "bits" of digital information and information "packets" sent over the Internet. Eight states so far have enacted laws imposing taxes on Internet access or Internet commerce. The potential for multiple and differential taxation of Internet transactions is obvious.

With this potential taxation quagmire in mind, Congress late last year approved the Internet Tax Freedom Act (ITFA) as part of the 1998 Omnibus Consolidated

Appropriations bill. President Clinton signed the Appropriations bill, including the ITFA, on October 21, 1998. The Act has four main provisions, but the most important is that beginning October 1, 1998, the Act imposes a three-year moratorium on "taxes on Internet access" and "multiple or discriminatory taxes on electronic commerce."¹⁰

An Internet Tax Panel headed by David Pottruck of Charles Schwab has been established by Congress to recommend tax policy for the Internet. As a subcommittee of the Advisory Committee on Electronic Commerce, this panel has established an agenda which includes the possibility of: allowing local governments to tax goods sold over the Internet or by catalogue; taxing Internet access.

The National Governors' Association has publicly opposed the White House's no-tax policy, although some governors support a tax-exempt Internet market.

Regulated Products

It is unclear how advertising and sales criteria for regulated products such as drugs, liquor and guns will be enforced. On July 10, 1999, President Clinton issued an executive order requiring Attorney General Janet Reno to head up a group which is charged with preparing a report on whether existing laws are sufficient to investigate and prosecute Internet crimes such as the sale of guns, explosives, controlled substances and prescription drugs as well as fraud and child pornography.

The issues faced by e-commerce companies can reach beyond the obvious. Both Amazon.com and Barnesandnoble.com have been notified by the German government that their sales of Anti-Semitic books such as Mein Kampf to German citizens is in violation of German law. Any web based business must exercise caution to make certain that they are in compliance with regulations in any country to which it ships its products.

Drugs: With traditional media, the FDA also must approve all advertisements and labels. The FDA has not indicated whether it intends to be as rigorous in requiring Web sites to post disclaimers on every single page or otherwise provide all site content for approval. Given that Web pages are sometimes altered daily, it is unclear how FDA requirements could be wholly incorporated onto the Internet. As of yet, the FDA has done little to clarify its position, although it has committed itself to developing a consistent enforcement policy regarding links.¹¹

Liquor: On July 20, 1999, the House Judiciary Committee approved a bill that would give states the authority to prosecute companies that violate the state's liquor sales laws. The states could take out-of-state companies to federal court. The proposal would also give the states more power to collect taxes on liquor shipped to their state. This supposedly would not violate the moratorium on new internet taxes as it focuses on collection of existing taxes. However, if upheld, this would raise the question of collection of sales tax on other internet sales.

Guns: A proposal to include internet gun sales in the Liquor bill described above was ruled "out of order" so no action was taken.

¹⁰ "Sweet Land of E-Liberty: The Internet Tax Freedom Act", Eric J. Sinrod and Jeffrey W. Reyna, *Journal of Internet Law*.

¹¹ Legal Issues Associated with the Creation and Operation of Web Sites, *Richard D. Harroch*, Orrick, Harrington & Sutcliffe LLP

Freedom of Speech

In Reno v. the ACLU, the Supreme Court ruled that the First Amendment applied over the Internet and struck down some of the provisions of the Communications Decency Act. The Ninth Circuit court ruled in Bernstein v. U.S. Department of Justice that computer source code (but not object code) merits full protection under the First Amendment. [Source code is written in languages such as BASIC and can be read by people rather than just by other computers.] This decision is being appealed by the DOJ and may end up in the Supreme Court due to national security issues regarding distribution of encryption technology.

SEC Regulations¹²

The Securities Act of 1933, as amended, requires that the offer and sale of securities be made pursuant to a registration statement filed with the Securities and Exchange Commission ("SEC"), unless otherwise exempted. State securities or blue sky laws similarly require qualification or registration with a state securities administrator prior to the offer and sale of securities, unless otherwise exempted. Furthermore, even if the securities are validly registered with the SEC, Section 10 of the Securities Act of 1933 mandates that any written materials concerning an offering may only be made by means of the filed prospectus.

The SEC has brought suits against promoters and companies for illegal offers and sales over the Internet. On the other hand, some companies have successfully employed a limited offering under Rule 504 of Regulation D, governing offerings of less than \$1 million, and/or Regulation A, governing offerings with an aggregate offering price of less than \$5 million.

Much has been written about raising capital over the Internet. A New York-based microbrewery called Spring Street Brewing became the first company to publicly sell securities over the Internet under Regulation A, when it raised \$1.6 million by making a direct offering by using an online prospectus to solicit investors. Since then, a number of public offerings have been effected through use of the Internet.

Companies who want to use the Internet for "offshore" offerings of securities can do so, if the offerings are made in compliance with SEC Regulation S. The SEC has provided guidance and set forth special requirements for such offerings. See SEC Release No. 33-7516 (March 23, 1998).

If the company is attempting to employ a private placement exemption to avoid federal and state registration for a stock offering, it must remember that any reference to the offering on the company's Web site may be deemed a prohibited advertisement or general solicitation. The Regulation D exemption under the Securities Act of 1933 generally prohibits advertising and general solicitation as a condition to the availability of the exemption. Therefore the company must generally not make any references to a *prospective* private stock offering on its site.

In the event of a conventional stock offering, the information on the company's web site must also be reviewed to avoid any inconsistencies in disclosures contained in a prospectus or private placement memorandum. Web sites tend to be very marketing oriented, in stark contrast to the typical cautionary statements included in securities disclosure documents. Counsel also will be concerned that information in the site may be deemed a prohibited hype of the offering, which could require cancellation or delay of the offering.

¹² Legal Issues Associated with the Creation and Operation of Web Sites, *Richard D. Harroch*, Orrick, Harrington & Sutcliffe LLP

At present, the SEC and most of its state-level counterparts seem willing to allow companies to use the Internet for "testing the waters" as to whether a market for the offering of a security exists (pursuant to SEC Rule 254). Issuers may not, however, make any sales before they file an issuing statement with the SEC.

In March 1997, the SEC staff also allowed MSNBC Interactive LLC's Private Financial Network ("PFN") to conduct a "road show" to prospective underwriters, investors, and others using Web site-based video transmissions where each PFN subscriber received "a filed prospectus from the issuer or the underwriter . . ." prior to the transmissions. The SEC staff further approved transmission of a company's road show presentation over the Internet (SEC no-action letter, Net Roadshow, Inc., January 30, 1998 and September 8, 1997.)

For public companies, the Web site information also should be reviewed to ensure consistency with the company's filings with the SEC (such as Forms 10-K, 10-Q, and 8-K) and regulatory filings (such as with bank or insurance company regulators).

A move by the SEC may signal further change in policy regarding electronic trading. In May 1997, the SEC issued a 230-page "Concept Release" (No. 34-38672) with 143 questions focusing on the creation of a new regulatory framework for securities trading that takes technological advances into account. The SEC is seeking input particularly regarding oversight of alternative trading systems, national securities exchanges, and foreign market activities in the United States. Given that the number of broker-dealers integrating the Internet and Web sites into their services doubled in 1996 alone, the SEC may be planning further regulation of alternative trading systems. Thus, companies interested in electronic trading should pay close attention to future actions by the SEC. Issuers that are in the midst of contemplating going public or are in the midst of preparing for a registered securities offering must be particularly cautious. There is a risk that under the Securities Act of 1933, information made publicly available about the company on its Web site may be deemed to constitute offering material distributed in violation of Section 5 of the Securities Act of 1933. The argument that the SEC or disgruntled investors could make is that various marketing materials on the site were (i) misleading, (ii) directed towards potential investors, or (iii) designed to condition the market for a prospective securities offering (thus potentially violating the "gun jumping" rules of the SEC). The SEC has addressed this issue and has stated that the federal securities laws apply equally to electronic and paper-based mediums. SEC Release 33-7223 (October 6, 1995).

With respect to links from a public company's Web site, it would appear to be prudent practice not to link to any analyst's report on the company. Such a link runs the risk that the company may be deemed to be endorsing or validating the analyst's report.

A public company posting information on its Web site also may need to be concerned about an obligation to update stale information. A company will often post large amounts of information on the Web about its products or services, market initiatives, programs, and other information. That information can become quickly outdated, perhaps misleading prospective investors.

Illegal Activities

Operators of web sites must be careful not to violate existing laws. Since an activity may be legal in one jurisdiction but illegal in another, extreme caution must be exercised. Some examples:

- on-line gambling is legal in some jurisdictions, but specifically prohibited in others (Illinois, Louisiana, Nevada & Texas). An on-line gambling site may attempt to check the state of residence of its gamblers, but if the gambler accesses the site from within a state where on-line gambling is prohibited, they could be breaking the law. The DOJ has brought charges against 22 Internet gambling sites under the Wire Communications Act. The Wire Communications Act -- currently prohibits someone in the

business of betting and wagering from using a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers on any sporting event or contest. This law was originally enacted to assist the states and territories in enforcing their laws and to suppress organized crime involvement with gambling. To the extent that Internet casinos are likely to be located abroad and beyond the easy reach of state authorities, the states are likely to seek federal assistance more frequently when foreign casinos offer gaming to local citizens in violation of local law.

¹³ The U.S. Senate is considering the Internet Gambling Prohibition Act of 1999 which would bar the use of the Internet for gambling or for the transmission of information which assists in a gambling enterprise.

- In a recent case filed in Alabama and Wisconsin, *credit card companies* are being sued for violating state and federal laws by collecting debts incurred as a result of illegal internet gambling. The action alleges violations of RICO and seeks reimbursement of six years of gambling debts.
- On-line auction houses often post pictures of the art being offered for sale. While this is considered 'fair use' of the copyrighted painting in the US, it is illegal in France.
- Vitamin and food labels that meet US standards may not conform to statutes in other countries. This is particularly sticky when it comes to food stuffs which contain genetically modified elements – common in the US but prohibited in most of Europe.
- English libel laws are more stringent than US laws and do not allow many of the defamation defenses recognized in the US.

Spam & Netiquette

E-mail has made it possible to contact millions of consumers with the mere press of a button — at almost no cost to the marketer. As might be expected, however, this practice has aggravated and annoyed most of the recipients of such junk e-mail. As a result of the Internet community's strong dislike of this kind of unsolicited mail, an array of legislation regulating such mail has either been proposed, is pending, or has been passed at both the state and federal level. Some state laws prohibit unsolicited e-mail messages unless they are readily identifiable as advertisement and contain the sender's name, address and e-mail address. Others expand the scope of existing state "junk fax" laws to include unsolicited e-mail while others require that e-mail solicitors establish a toll-free telephone number enabling the recipient to call and "opt-out" of any future mailings.¹⁴

In 1267623 Ontario Inc v. Nexx Online Inc., the Ontario Superior Court of Justice found on June 14, 1999: "I conclude after reviewing the principles that emerge in the American caselaw, the excerpts from the literature provided, and the reaction of individual internet users that unless a service provider specifically allows in the contract for unsolicited commercial bul e-mail to be distributed, it appears clear that sending out unsolicited bulk e-mail for commercial advertising purposes is contrary to the emerging principles of "Netiquette"."

Netiquette, although mostly unwritten, is fast becoming the common law governing internet transactions.

¹³ Statement of Kevin V. Di Gregory, Deputy Assistant Attorney, General Criminal Division before the Subcommittee of Crime Committee of the Judiciary U.S. House of Representatives concerning gambling on the Internet, June 24, 1998

¹⁴ "E-Commerce and the Law; Regulatory and Legal Implications of Electronic Commerce on the Insurance Industry", *Future One*, a cooperative partnership of the Independent Insurance Agents of America (IIAA).

Digital Signatures & Certificates

A digital signature in its most basic form is a means of signing an electronic document and ensuring its ultimate integrity. The use of digital certificates & signatures is necessary in order to secure transactions over the internet.

To assist in verifying the authenticity of a digital signature, the signature often includes a digital certificate issued by a "certification authority (CA)." A CA is analogous to an electronic notary that verifies the identity of the person seeking certification.

Of the states permitting use of digital signatures, jurisdictions are split between those that authorize digital signatures for both public and private communications and those that authorize such signatures for public use only (i.e., filing documents with state agencies). Arizona, California, Idaho, Indiana, Maryland, Mississippi, New Mexico, North Carolina, North Dakota, Rhode Island and Texas authorize the use of electronic signatures for electronic communications with state departments and public agencies.

Alaska, Florida, Georgia, Illinois, Kansas, Kentucky, Minnesota, Mississippi, Nebraska, New Hampshire, Oklahoma, Oregon, South Carolina, Utah, Virginia, Washington, West Virginia and Wisconsin authorize the use of digital signatures for both public and private communications. In these states, a digital signature is generally acceptable where a statute or rule of law requires a signature if: a) the signature is authorized by the person or governmental entity receiving it; b) the original signer intended to be bound; and c) the recipient has no knowledge that the signer has breached a duty or does not rightfully hold access to use the digital signature.

In most states, the Secretary of State is authorized to act as the certification authority regulating transactions, verification procedures, and licensing. In West Virginia, the Secretary of State is authorized to issue certificates as well as contracts with third parties to serve as private certification authorities. In comparison, the North Carolina Secretary of State issues one-year licenses to certification authorities who meet certain requirements.¹⁵

Internationally, the regulations regarding licensing of a CA is quite varied and often unclear. Most significantly, the EU draft Directive on Electronic Signatures prohibits member states from requiring licensing of CAs but allows voluntary licensing.

There are many legislative initiatives worldwide regarding digital signatures. If these result in too many discrepancies, they may inhibit the use of electronic signatures in international commerce.

The liability of the CA to the recipient of the message for any inaccuracies or misrepresentations contained in the certificate is at this time unclear.

Privacy Legislation & Regulations

Although the U.S. Federal government protects access to its own databases, there is virtually no regulation of private databases containing personal data because the law has not kept up with the technology of the Internet. More than 40 countries have enacted or intend to enact privacy laws protecting the use of personal consumer data. The European Parliament promulgated a directive in 1995 that took effect on October 26, 1998. Article 26 of the Directive prohibits any company doing business in the European Union from

¹⁵ *ibid.*

transmitting personal data to a country that does not guarantee comparable privacy protection. The Commerce Department issued its own report in response to the E.U. Directive. It stated that the role of government is to advise, pressure, and advocate, but not legislate, except in such areas as medical records and child privacy.

For the most part, the FTC and the Clinton Administration have supported the concept of self-regulation. FTC Chairman Robert Pitofsky has said that self-regulation, if done right, could have a flexibility that legislation and bureaucratic rule-making will never have. Pitofsky has also issued a warning to the private sector stating that if we don't have a level of self-regulation that gives us a sense that there's real progress being made, Congress will step in. The FTC also continues to assess the effectiveness of self-regulation, and the results of second survey are expected in the Summer of 1999. If the results are as damaging as those released in June 1998, the call for active federal regulation will be greater than ever.

The Clinton Administration's focus on privacy issues was further highlighted with the March 1999 appointment of Ohio State University law professor Peter Swire as the country's first Chief Counselor for Privacy. At least initially, Mr. Swire is likely to be focused on quelling the dispute between the U.S. and the European Union over the E.U.'s strict privacy directive that went into effect in October 1998. That declaration gives the citizens of the E.U. access and control over their personal information and prevents the sharing of such information with countries that do not provide adequate level of privacy. The directive could prevent American companies from using information about European consumers.

To prevent U.S. companies from having international data transfers cut off by the E.U., the Clinton Administration has proposed creating safe harbors that would allow firms to continue exchanging data if companies voluntarily comply with a set of basic privacy standards. As recently as November 9, 1998, the Clinton administration released a proposed voluntary approach for U.S. companies to meet the requirements of the European Directive. In this proposal, companies abiding by the seven principles would be considered in compliance with the European requirements. These principles reflect the Administration's previous discussions with U.S. companies but have not been approved by the E.U.

The E.U. nations generally believe, however, that the federal government is inadequately enforcing privacy protections. They want the U.S. to offer individuals greater access to their personal data while also developing a compliance and enforcement mechanism. The two sides hope to have an online data privacy agreement in place when their June 1999 summit convenes.¹⁶

The U.S. Electronic Communications Privacy Act (ECPA) governs unauthorized access to and disclosure of electronic mail messages. Title 18 of the United States Code (USC) covers federal government activities and grants federal entities the authority to promulgate rules and regulations addressing electronic records access, thereby establishing new federal offenses. For example, it is now a federal offense to access a computer system without authorization or to exceed a designated level of authorized access on any computer system. The ECPA does not provide protection in the workplace, primarily because the ECPA applies to *interception* of electronic messages and not the review of stored messages. While employers are prohibited from monitoring an employee's telephone calls or e-mail transmissions where the employee has a reasonable expectation of privacy, the ECPA acknowledges that employers may monitor electronic transmissions if employees are notified in advance or if the employer has reason to believe the company's interests are being compromised. Interception of electronic messages is also

¹⁶ *ibid.*

permissible under certain circumstances. It is also important to point out that although Title II covers federal crimes it also provides for private civil actions.

S. 2236 - The Children's Online Privacy Protection Act of 1998:

This bill was introduced by Sen. Bryan (D-Nevada) on July 17, 1998. It was enacted into law as part of the omnibus appropriations bill Congress adopted in its closing hours. In short, the bill requires the Federal Trade Commission to issue regulations to protect the privacy of personal information about children on the Internet. Specifically, it directs the FTC to issue regulations requiring commercial web site operators to obtain the verifiable consent of parents for collecting and using personal information about children under the age of 13. The new law authorizes States to enforce such regulations by bringing actions on behalf of residents.¹⁷

Jurisdiction

Internet use may subject businesses to multiple jurisdictions, theoretically requiring them to comply with the most of the restrictive laws created by a single state or nation. In this multi-jurisdictional scenario, which entails the prospect for conflicting regulation, the potential for civil litigation may require electronic commerce participants to be concerned with which foreign courts they may be subject to suit in and the legal standards under which their conduct will be assessed.¹⁸

States, through their "long arm" statutes, may also exercise personal jurisdiction over a foreign entity if that entity has systematic contacts in the state or commits some injury in the state. Courts will often review the scope of the web site's operations when considering whether a foreign defendant's Internet web site has the requisite contact to become subject to a state's long arm statutes. While the majority of the courts seem reluctant to find jurisdiction based solely on the maintenance of a passive web site, some courts have found jurisdiction on this basis alone. In cases involving personal jurisdiction arising from an interactive website, jurisdiction is generally determined by examining the level of interactivity and the commercial nature of the information being exchanged online.¹⁹

Since consumers will be able to access company web sites in all U.S. jurisdictions, the establishment of an online web site could potentially involve issues of multi-jurisdictional licensing for professionals (Physicians, Accountants, Lawyers, Insurance Agents, etc.) and issues relating to unlawful solicitation/advertising.

As of the writing of this paper, jurisdictional issues continue to be hotly debated in the courts. In Fix My PC, L.L.C., et al. vs. N.F.N. Associates Inc. et al, the court determined that the existence of a 'passive' web site was not sufficient to create personal jurisdiction. In PurCo Fleet Services In. vs. Michael Towers, et al, the existence of a web site that allows users to make contact via e-mail was ruled to constitute transaction of business within Utah.

Insurance Issues

Any policy written with a territory less encompassing than "Anywhere" could provide gaps in coverage.

¹⁷ *ibid.*

¹⁸ "The Confluence of International, Federal, and State Jurisdiction over E-Commerce (Part II)", Thomas P. Vartanian, *Journal of Internet Law*.

¹⁹ "E-Commerce and the Law; Regulatory and Legal Implications of Electronic Commerce on the Insurance Industry", *Future One*, a cooperative partnership of the Independent Insurance Agents of America (IIAA).

Contractual Liabilities

Breach of contract

If goods or services provided on the site do not live up to the expectations of the customer or user, the owner may be exposed to a breach of contract claim.

Online Contracts

Online contract transactions are often formed by the use of web-wrap agreements. A web-wrap agreement constitutes an offer transmitted over the Internet and acceptance of the offer transmitted back by the consumer who clicks an "I agree" or "I accept" button at the computer. While web wrap agreements are increasingly prevalent, it is not yet known whether the courts will enforce such agreements.²⁰

Because of the dearth of authority on the topic of webwrap agreements, some commentators have sought guidance from legal decisions involving similar "shrinkwrap" or "clickwrap" license agreements in the area of computer software. Currently there have been some cases upholding the enforceability of such agreements and the analogy probably makes sense when applied to the sale of goods over the Internet.²¹

Since current case law and legislation has not kept pace with issues relating to contract formation in an electronic context, the most current draft of Article 2B of the Uniform Commercial Code (UCC) could serve as an important model for future state regulations and future case law. The American Law Institute (ALI) has prepared a draft of uniform commercial laws that would apply to software and electronic transactions.

The underlying philosophy of Article 2B is that contracts created by computers should be valid, binding, and enforceable. The absence of a writing presents one obstacle to having a binding electronic contract. UCC 2B addresses this issue by replacing the word "writing" with "record." The change in terminology is not merely semantic, but important in that it divorces the traditional concepts associated with writings and makes electronic records the functional equivalent of a writing on a piece of paper. Article 2B also discards the term "signature" and replaces it with "authenticate." The new term is of special relevance to those situations where two computers form a contract in the absence of human review.

UCC 2B also introduces the new concept of an "electronic agent." The introduction of an "electronic agent" is quite new to contract law. Essentially, it acknowledges that electronic contracts can be formed without human intervention. Consequently, a computer without regard to human decisions on either side of the transaction can now perform the formalities of offer and acceptance, which have traditionally required some form of human input.

Efforts to agree upon a final version of Article 2B have recently in the wake of opposition from several entertainment and communication industry groups. Several associations, including the Motion Picture Association of America, National Association of Broadcasters, National Cable Television Association, Recording Industry Association of America,

²⁰ *ibid.*

²¹ *ibid.*

Newspaper Association of America and Magazine Publishers of America have urged that UCC 2B be confined to software and not applicable to electronic transactions. Nevertheless, it appears likely that some version of Article 2B will ultimately be agreed upon and serve as the basis for electronic transactions, including insurance transactions conducted via the Internet.²²

Conflicts with other Channels of Distribution

Many companies now sell their products not only through traditional distribution systems but also via the Internet. This dual methodology can create unexpected conflicts. Traditional distribution contracts will grant a licensee the right to market a product or service in a given geographic area. Because web sites are not directed to a geographic territory, their use can conflict with the exclusive arrangements in other contracts.

Denial of Service/Repudiation of Access

Denial of Service attacks against computers connected to the Internet cause those computers to disconnect or crash. Denial of Service attacks are a federal crime under the National Information Infrastructure Protection Act of 1996. Penalties include substantial fines and imprisonment.

Operating System attacks target holes in the system's security and can be patched to prevent repeat attacks. The latest versions of many popular operating systems are already safe against these attacks, including Windows 98, MacOS 8, and Linux.

Networking attacks often cannot be patched or defended against. These attacks can overwhelm your bandwidth, crippling your network.

Although most Internet web site owners feel that they are not responsible for economic loss resulting suffered by a customer who is unable to access their site (or slowdowns due to high use), there are several cases currently pending which challenge that assumption by asserting that the web site operator was contractually obligated to provide access. The direct loss to the web site owner, in addition to the defense of such allegations, is the loss of customers, and negative publicity which may keep new customers from their site.

Unauthorized Access

Unauthorized access to confidential information – whether or not it results in a financial loss to the owner of the information – is a critical issue for companies doing business over the Internet. Many companies now specify the type of routers, firewalls, and security procedures that each of its internet partners must employ to protect their data. Cisco Systems is even sending its own engineers to examine a partner's security measures and holds them liable for any security breach. As this practice becomes more common place, failed security measures will result in contractual liabilities.

Extortion

While all businesses can face extortion demands tied to threats of damage to persons or property, electronic commerce adds a new dimension to the threat potential. Extortionists can threaten to:

- shut down a network through a Denial of Service attack,

²² E-Commerce and the Law; Regulatory and Legal Implications of Electronic Commerce on the Insurance Industry; by *Future One*, a cooperative partnership of the Independent Insurance Agents of America (IIAA)

- take over critical operations remotely via a 'Trojan Horse',
- expose confidential or embarrassing information
- damage or destroy data

Damage to Property

First Party

Electronically based businesses are particularly vulnerable to loss of income from damage to property – their own or property upon which they depend. These businesses are at the mercy of nature, employees, contractors and outside parties. Whether the damage is caused accidentally or maliciously, the economic impact is the same. The business can be shut down or seriously injured if any of the following are damaged, destroyed or tampered with:

- Computer systems including web sites, networks, servers, intranets, extranets, e-mail, etc. & related equipment
- Computer programs, software, firmware, etc.
- Electronic databases, off line libraries etc.
- Electronic media
- Telecommunications equipment
- Utility services
- Satellites
- Service Providers & other contractors

INSURANCE AVAILABLE

Property Insurance: Property and EDP forms often contain limited coverage for damage done by Virus. These policies often limit coverage for damage to data to the cost to reproduce *or the cost of the media if the information cannot be reproduced*. Most exclude Employee Dishonesty, unless it is an act of vandalism. Questions remain as to whether hacking and spread of virus is vandalism.

Business Income: Most business income forms will only respond if there is a corresponding covered property loss. Therefore, lost income from damage to or theft of intellectual property would likely not be covered.

Intellectual Property

Employees or outsiders can steal or copy Intellectual Property that is critical for the operation of electronic businesses. The definition of Intellectual Property as it relates to e-commerce goes far beyond the traditional concept of Patents, Copyrights, Trade rights and R&D. Intellectual Property can include sound bytes, program code, a style of doing business, colors, processes, knowledge or technological methods. Value often comes from the information obtained by processing of data rather than from the data itself. Measuring the value of this information is often difficult. The value needs to include the uses of the information as well as the actions of competitors if the information is revealed.

Theft or copying of Intellectual Property can result in significant loss of revenue, Goodwill, market share (or market potential), damage to reputation, re-creation costs, enforcement

expenses, and lost opportunities. The loss of key employees to competitors is a critical concern when those employees have access to Intellectual Property. Employees who have developed or contributed to the development of Intellectual Property assets have 'knowledge' that can be very detrimental if divulged to competitors.

Access to Intellectual Property can be denied—referred to as Breach of Utility. This occurs when employees or others encrypt valuable documents, thereby denying access to the document to anyone who does not have the decryption key. This can be intentional (ie when a disgruntled employee leaves the company) or unintentional (an employee simply forgets the decryption code.).

Property Insurance: These policies often limit coverage for damaged or stolen data to the cost to reproduce *or the cost of the media if the information cannot be reproduced*. They will not respond to the lost market potential from the theft of Intellectual Property.

Business Income: Most business income forms will only respond if there is a corresponding covered property loss. Therefore, lost income from damage to or theft of intellectual property would likely not be covered.

Intellectual Property Coverage: These forms are usually limited to Patent Infringement and can be either defensive or offensive.

Property of Others

The electronic business, through the dissemination of material, goods or services, may cause damage to Property of Others. This property may be physical property (computer systems, media, equipment) or intangible property (data, software, business processes).

Insurance Available

General Liability: The General Liability policy covers Property Damage which results in Physical injury to *tangible property or a loss of use of tangible property which has not been physically injured or destroyed*. Courts are split on the determination of the status of 'data'—some consider data to be physical property, others do not. If data is not tangible property, the associated economic loss from the failure of hardware or software to perform as intended is also not covered. The GL policy will not respond to claims of property damage to the insured's product or work. Therefore it will not cover the cost to repair, recall or replace software or other goods or services manufactured, sold or distributed by the insured. It also will not respond to the claimant's economic loss from this circumstance. In Seagate Technology, Inc. v St. Paul Fire & Marine, the court held that malfunction of equipment or handling of data which causes loss of data fails to qualify as property damage under a GL policy.

Electronic Errors & Omissions: These policies will respond to allegations of economic damage or intangible losses other than property damage arising out of specified professional services which may include the insured's product. Properly worded, this coverage may fill some of the gaps in a traditional E&O policy.

E-Commerce Policies:

Damage to Your Electronic Products: These policies cover any claim arising out of damage to your electronic products arising out of the sudden and accident physical injury to such products.

Business Income

In addition to traditional exposures to their income, firms engaged in e-commerce face significant potential for loss of income from:

- Attacks - Denial of Service, Trojan Horse, Virus, Worms, etc.
- System down time
- Theft of Information
- Fraudulent credit card use
- Inability to take, process or ship orders
- Inability to verify or collect payments

Crime Exposures

Over the past 10 years or so, most businesses have become highly computer reliant even if they are not doing business over the Internet. Retail stores can't ring up a sale when the computers are down; manufacturers can't track merchandise when the system is off line; etc. Amassing critical information and/or processes into a single system is akin to single-sourcing a critical supply item – if the system goes down, you don't have alternatives.

By placing this information in an application accessible via the Internet, the exposures are not necessarily increased, but the ease of access is certainly enhanced. Some of the exposures faced by e-commerce include:

- Loss of funds during electronic transfer – either by fraud or error
- Computer Fraud
- Theft, destruction or modification of data or intellectual property
- Fraudulent credit card use
- Inability to verify or collect payments/receivables

Insurance Available:

Computer Fraud Coverage: Available either as enhancements to Fidelity coverage or stand alone.

Funds Transfer Fraud Coverage:

Computer Virus Coverage:

Property Coverage:

Fidelity Coverage:

Financial Institutions Bonds:

Disaster Recovery

For an electronic business, being shut down can be disastrous - regardless of the reason or length of time.

On the retail side, you may only get one chance to attract a prospective customer to your site – if it is down, the customer may never return. Regular customers may be somewhat more forgiving, but repeated or lengthy down time will send the internet shopper quickly to a competitor's site.

On the business-to-business side of e-commerce, down time for business linked for logistical reasons can be damaging to the relationship and cause unacceptable delays in the processing of orders.

With e-commerce being such new industry, there are few case studies and no 'off the shelf' disaster recovery plans. Traditional disaster planning focuses on natural disasters, fires and other damage to tangible property. These plans attempt to get the business back into operation within weeks or months – a time period that bodes disaster for e-commerce. For many e-commerce businesses (i.e. electronic trading & electronic banking) an outage of even a few hours is unacceptable.

In addition to traditional exposures, a disaster plan for e-commerce needs to include at least:

Prevention

- Regular security assessments and 'ethical hacking'
- Real time monitoring of potential attacks & intrusions
- Physical site security
- Extortion guidelines
- Enforcement of Intellectual Property rights guidelines
- E-mail usage guidelines
- Internet usage guidelines
- Anti-piracy guidelines
- Documentation of Intellectual Property & valuations
- Education of employees in disaster prevention & recovery

Planning

- Periodic review of Data Center Disaster Recovery Plan
- Contingent power & utility supply
- Duplication of business processes & data
- Customer notification and communication procedures
- What to do in case of attack to minimize damage & downtime
- Forensic processes

- Hot-site, warm-site, or cold-site switch over plans
- Alternative space & equipment for staff
- Alternative internet access
- Methods to provide 'Traditional' customer support during crisis
- Security of Intellectual Property & confidential data during crisis
- Crisis management of brand image
- Control of news media

Consumer Fraud

The news is filled with stories about consumers being ripped off over the internet – goods that are never delivered, fraudulent auctions, credit card fraud etc. Technology such as on-line escrow services and 'safe wallets' are being used in conjunction with digital certificates to make transactions safer.

Companies providing goods and services via the internet are also being defrauded by consumers. Losses due to fraudulent sales now equal about 1% of online revenues. The Federal Trade Commission, the SEC and several state attorney generals are looking into the specifics of internet fraud.

Antitrust/Unfair Competition

Violation of advertising laws; deceptive practices; and unfair competition. These somewhat broad categories encapsulate various improper business conduct, including "unlawful, unfair or fraudulent business act[s] or practice[s] and unfair, deceptive, untrue, or misleading advertising." See, e.g., Cal. Bus. & Prof. Code § 17200. Companies open themselves to these claims when they publish false, misleading or material unverified information relevant to their commercial activities on the Web. Common deceptive practices include false designations of origin and/or sponsorship on or about a Web site and false advertising on or about the Web site.²³

One type of misleading practice widely used on the web is to take advantage of a consumer's typographical mistake. For instance, until July 23, 1999, a consumer who misspelled www.geico.com as www.geigo.com would end up at a site called AllStates Car Insurance. Although a disclaimer stated that it was not related to Allstate Insurance Co., users who clicked on a state in order to obtain a quote were sent to a Web site for Progressive Insurance Company. This site was shut down after complaints by Geico.

False Advertising

False-advertising claims are often brought under section 43(a) of the federal Lanham Act which provides that "Any person who, on or in connection with any goods or services ... uses in commerce any ... false or misleading description of fact, or false or misleading representation of fact, which ... in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's

²³ Legal Issues Associated with the Creation and Operation of Web Sites, *Richard D. Harroch*, Orrick, Harrington & Sutcliffe LLP

goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act."

To bring a claim of False advertising, a company must prove five things:

1. a false statement of fact by the defendant in a commercial advertisement about its own or another's product;
 2. the statement actually deceived or has the tendency to deceive a substantial segment of its audience;
 3. the deception is material, in that it is likely to influence the purchasing decision;
 4. the defendant caused its false statement to enter interstate commerce; and
 5. the plaintiff has been or is likely to be injured as a result of the false statement, either by direct diversion of sales from itself to defendant or by a lessening of the goodwill associated with its products.
- Consumers cannot bring suit for false advertising under the federal Lanham Act. The purpose of the Act is to "protect persons engaged in ... commerce against unfair competition," 15 U.S.C. § 1127, as opposed to protecting consumers. State laws do provide consumers with remedies for misrepresentation.

The financial penalties for false advertising under the Lanham Act can be stiff. In some circumstances, a monetary award might include, for example:

- perhaps the profits made by the defendant as a result of the false advertisement;
- perhaps the profits lost by the plaintiff;
- perhaps the cost of advertising by the plaintiff to correct the misleading impression left by the false advertisement;
- perhaps the plaintiff's attorneys fees and expenses.²⁴

The greatest stumbling block in the battle against false advertising on the Internet is establishing personal jurisdiction over non-resident originators of tortious material. Without jurisdiction, no court has the power to adjudicate claims brought before it. Thus the question of whether the mere transmission of false advertisements from a non-resident originator's homepage to the user's computer screen can serve is sufficient to warrant personal jurisdiction.

Traditionally, personal jurisdiction over non-resident defendants requires a two-part analysis. The exercise of jurisdiction must first satisfy the applicable state long-arm statute. If the long-arm statute is satisfied, the court must then determine whether sufficient minimum contacts exist to satisfy the Due Process Clause of the Fourteenth Amendment so that "maintenance of the suit does not offend traditional notions of fair play and substantial justice". If both prongs are satisfied, a federal or state court may properly exercise personal jurisdiction over a non-resident defendant.²⁵

Tortious Interference

A company might sue a Web site owner if the owner has wrongfully interfered with the company's business relationships and thereby caused it damage. A plaintiff may claim wrongful injury where no contractual relationship exists, as well as of where the interference is unintentional. An owner might be open to such a claim simply by being

²⁴

²⁵ Transmission jurisdiction: the power to adjudicate false advertising on the internet; *Jon Cooper*

negligent, i.e., by not exercising the proper amount of care established by the laws of a particular jurisdiction.²⁶

²⁶ Legal Issues Associated with the Creation and Operation of Web Sites, *Richard D. Harroch*, Orrick, Harrington & Sutcliffe LLP

A
Antitrust 2
Audio Home Recording Act..... 3

B
Business Income.....2, 19, 20, 21

C
Caching 2, 3
Contracts 1
Copyright 1, 2, 3, 4
Cybersquatting..... 1, 5

D
Defamation 1, 8
Denial of Service 1, 18, 21
Disaster Recovery 2, 22

E
Extortion 1, 22

F
False Advertising..... 2
Fraud 2
Freedom of Speech..... 8, 11

I
Intellectual Property 2, 4, 19, 20, 22, 23

J
Jurisdiction 1, 16

L
Lanham Act..... 2, 5, 23, 24

M
Metatag..... 6

P
Patent 1, 4, 20
Privacy..... 1, 9, 14, 15, 16

R
Repudiation of Access..... 1, 18

S
Safe Harbors..... 3
SEC..... 1, 11, 12, 23
Source code 2, 11
Spam..... 1, 13

T
Tortious Interference 2
Trademark 1, 5, 6