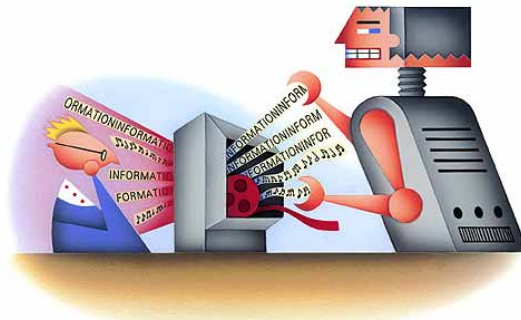


What Every Business Needs to Know

about the Legal Issues Surrounding
Information Use in the Workplace



By Jon M. Garon



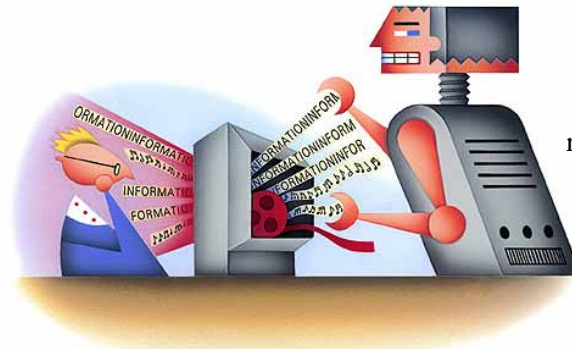
What Every Business Needs to Know

about the Legal Issues Surrounding
Information Use in the Workplace

By Jon M. Garon¹

The growth of the Internet continues to expand at a pace unimagined by science fiction writers, economists, and hobbyists. The changes have reached less than a small percentage of the economy, yet the effect has been to challenge fundamental notions regarding old and new economies. For some companies, the Internet has become the sole means of delivering their products,² while for others the Internet provides an added feature — an extension beyond the retail shop.³ Nonetheless, the technology continues to evolve, metamorphosing first from a military communications network to an entertainment novelty, it has now transformed into an indispensable corporate tool.⁴

Internet activity and e-commerce solutions are an inevitable component of every facet of the modern business. Internal operations can no longer operate without e-mail, the Internet is supplanting the Yellow Pages as the access point for new businesses, and a broad array of state and federal law are



requiring accommodations to the digital economy for banking, health care, securities, and other industries.

“As business-to-business and business-to-consumer practices explode on the Internet, U.S. government agencies and a host of attorneys are casting a pensive gaze on what they consider to be e-commerce’s many legal gray areas. Exchanges, marketplaces, portals, and other Internet initiatives add a new dimension and complexity to current laws that for decades have dictated the way commerce is conducted. ... [G]overnment officials and lawyers look increasingly at questions of antitrust, anti-competition, digital signatures, and validating and upholding online contracts...”⁵

This paper provides an overview of the legal issues that a business must address regarding a strategic implementation of Internet and e-commerce technologies.

Developing an E-Commerce Strategy

E-commerce “involves the use of the Internet and proprietary networks to facilitate business-to-business, consumer, and auction sales of everything imaginable—from computers and electronics to books, recordings, automobiles, and real estate.”⁶ This definition highlights the role of computer technology as a tool in business transactions. More precisely, e-commerce covers a broad set of tools that can be used by companies to assist in communications, warehousing, distribution, payment systems,

“Since e-mail is used for communications between members of a business organization both internally and with the public, a number of legal issues must be addressed through a comprehensive policy”.

and the subject matter of the transactions. “E-commerce has the potential to broaden store brand, give the ability to sell products in markets and countries not served by stores, and increase the total market share of a product category, according to a Merrill Lynch research study called e-Commerce: Virtually Here. The downside is that it might also reduce store traffic, put a downward pressure on prices and bring in more competition.”⁷

For business today, the pressures created by the Internet demand an e-commerce strategy. Even the choice to reject the Internet must be made in the context of the competitive forces reshaping commerce and communications.

This paper provides a brief introduction to the legal issues and fundamental legal framework for each issue. Both the law and the business practices are in great flux, so the statements included herein are only accurate as of its date of initial publication.

This outline should provide only an introduction to the legal topics included, and any individual using these materials and information presented must always research original sources of authority and update information to ensure accuracy when dealing with specific issues.

E-Mail

E-Mail Communications. E-mail allows a person to send a message to one or more recipients. It can also be used to attach other documents or software files. Once sent, an e-mail will travel an unpredictable path to its destination. E-mail is the basic tool for the Internet, yet despite the simplicity, a number of legal issues may arise from its use. Since e-mail is used for communications between members of a business organization both internally and with the public, a number of legal issues must be addressed through a comprehensive policy. Most of those issues involve the varying rules of privacy that surround e-mail. Because the rules of privacy vary with use, this remains an area of law that is subject to ongoing change.

Attorney Client Privilege. E-mail provides a very useful tool for communicating between a lawyer and client. “Unlike postal mail, simple e-mail generally is not ‘sealed’ or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted).”⁸ Because it is not secure, questions have continued regarding its use for privileged communications. In ethics opinions from 1994 to 1998, a number of bar associations warned attorneys to avoid use of e-mail or at least use caution because it is unsecure.⁹

The fear of unsecure transmission has given way, however, to the ubiquity of e-mail and a greater expectation of privacy by the users. The unpredictable path of an e-mail means that one cannot casually find an opportunity to see open e-mails. Courts have treated the contents of e-mail between attorneys

Jon M. Garon, Of Counsel Gallagher, Callahan & Gartrell, is a Professor of Intellectual Property Law at the Franklin Pierce Law Center, Concord, New Hampshire. He may be reached at 603.228.1181, or garon@gcglaw.com.

© 2000 Jon M. Garon.

and their clients as protected under attorney-client privilege or work product without comment on its unsecured status.¹⁰ Finally, as described in the paragraph below, courts have applied the Electronic Communications Privacy Act (“ECPA”) to criminalize the intentional interception of an e-mail transmission.¹¹ As a result, e-mail is sufficiently secure for many attorney/client communications.

Despite the ability to use e-mail for confidential communications, caution must still be used. Accidental transmission to third parties will waive an attorney’s privilege to the communication. In addition, the relative ease of interception may also create problems for some clients or transactions, notwithstanding the illegality of the interception.

Criminal Liability for Interception. In 1986, Congress amended the original Federal Wiretap Act with the ECPA to cover wired and wireless electronic communications, although as an example of the limits on this focus, Congress excluded wireless telephones because they were so easily intercepted.¹² In 1994, Congress plugged this hole and demonstrated that anti-interception laws were designed to stop interception of private communications regardless of the simplicity with which the interception can be made.¹³ Along with a series of other criminal statutes, courts are no longer having difficulty finding criminal and civil liability for interception of e-mails.¹⁴ The interception of the e-mail must come during transmission, however, rather than through the unauthorized reading of e-mail off another’s computer screen or unauthorized access to the computer files.¹⁵

Monitoring and Expectation of Privacy. Given the criminal protection from the intentional interception of e-mail, courts are validating the public’s growing expectation of privacy in e-mail transmissions.¹⁶ Despite this, numerous exceptions exist to the ECPA. The first is a legal interpretation that retrieving a message from storage does not constitute interception and therefore does not trigger the statute.¹⁷ Second is the exception that a communication may be intercepted if done with the consent of a party.¹⁸ This permission may be granted as part of the contractual conditions of employment. As a result, there should not be any reasonable reliance on

the privacy of e-mail transmissions by corporate employees, except to the extent created or eliminated by the employment policy.

Employment policies on e-mail must also comport to the same requirements of other employee communications. For example, if employers are required to provide employees access to company mail systems or telephone systems for the purpose of

“...there should not be any reasonable reliance on the privacy of e-mail transmissions by corporate employees, except to the extent created or eliminated by the employment policy.”

union activities, then that same type of access must be allowed for e-mail. This will include providing privacy for those communications.

Misuse by Employees. One of the primary reasons companies need policies to monitor e-mail is the potential liability that can occur from misuse. E-mail can be used to disseminate trade secrets and proprietary information very easily. It can also be used to share jokes and personal information. This interaction, which leaves a permanent record in the corporation’s data files, may empower employees who are acting improperly. “For example, Chevron Corp. was recently forced to pay four female employees over \$2.2 million as a settlement for sexual harassment, including an image of one employee doctored to look obscene and offensive sexual e-mail messages circulated over the company networks.”¹⁹ Even if the defense of the lawsuit is successful, the costs may be formidable.²⁰ The same policy that allows the employer to monitor the e-mails, however, may also increase the obligation to monitor and intervene.

E-Mail Storage. Any message sent by a company, no matter how off-the-cuff, becomes a permanent document that may be shared with far more people

than the intended recipient. Under most corporate data policies, e-mail becomes permanently stored in back-up recordings. Those e-mail records are subject to discovery and available against the organization in the event of litigation. Because the e-mail (and all computer back-up files) are corporate records subject to discovery, a company should incorporate any strategic document storage plan to include the e-mail tapes. Further, a business pattern of regularly deleting e-mails may not eliminate the legacy of the e-mail content if the residual information remains stored on the computer hard drives or back-up systems.²¹

Spam. In addition, a business can purchase millions of e-mail addresses and send a mass-distribution of its literature to that list. This technique — known as ‘spam’ — is strongly disfavored on the Internet by most users, but select ‘calls-to-action’ might not be received too negatively. Currently there is no federal legislation banning spam, despite numerous attempts.²² Proposed legislation is again being considered by the House of Representatives, but even that legislation reduces rather than eliminates the practice.²³ Industry leaders have promised to set voluntary industry guidelines to curb the worst practices, but to date, no voluntary efforts have had any substantial effect on the practice.²⁴

Websites

Websites embody an important marketing tool for modern business, and may serve as the focus of the core of the company’s business activities. Websites can range from simple, static descriptions of the company — electronic Yellow Page advertisements — to complex, dynamic, interactive product or service delivery. Online retailers like Amazon.com, auction houses including e-bay.com, and online banks such as Compubank.com, move every customer transaction to the Internet. Whether a company has developed a business model delivering all services on the Internet or simply uses the Internet as an introduction to its customers, certain common issues surround the website.

Content Requirements. Any pictures, text, photographs, and music used on a website are subject to copyright protection. Original work created by the company is protected under copyright law, whether or not a copyright application has been filed by the company. A business concerned about protecting the value of the copyrights in its website should register the work with the Copyright Office and create dated archival copies of the site for evidentiary purposes.

Original Content. Websites often contain work not created by the website owner.²⁶ These other works may be created for the website by independent contractors, licensed from other content providers, or ‘borrowed’ from the Internet. An independent contractor can create the content of a website to be owned either by the company or the creator of the content, depending on the agreement. Congress treats the owner of a copyright as the initial author. In a work made for hire, the hiring party may be treated as owner if “a work specially ordered or commissioned for use as a contribution to ... [an] audiovisual work ... if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire.” Absent the written agreement, the ownership in the content of the website will remain owned by the independent contractor, who may be free to sell it to other business or use it in competing manners.

Licensing. Licensing content owned by other parties provides another effective strategy for dealing with copyright issues. Many commercial publishers make news feeds, customized content, financial data, and other changing, topical information made available for website publishers. This transfers the obligation on content creation to a third party, may substantially reduce the cost of creating the content, and may result in very dynamic, timely content.²⁸

Fair Use. Borrowing materials for a website, although not uncommon, creates strong potential for copyright violations by the website publisher. The posting of copyrighted material on a website is copyright infringement unless there is an exception to the exclusive rights of the copyright holder. The fair use doctrine provides the greatest flexibility for the owner of a website hoping to use the work of

another. The fair use doctrine provides that “the fair use of a copyrighted work... for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright.”³⁰ Fair use is an equitable balancing test that accommodates the public’s need to comment on a work, to quote portions in other critical works, and to build upon the works that have gone before.

The use of a copyrighted work for profit is one factor the courts use to determine whether a use infringes the copyright holder’s interest.³¹ While the balancing test also includes the nature and extent of the use, the nature of the work, and the market for the work, use by a for-profit business without permission suggests that the use is not a fair one.³² For example, unless the material is in the public domain, use of clip art must be licensed.³³

Most importantly, companies must be educated to understand that the placement of copyrighted works on the Internet does not make that work part of the public domain. Copyrights now extend for seventy years from the life of the author, or 95 years in the case of a corporate entity.³⁴ This is true for both new works and those published prior to 1978, if those works had not already fallen into the public domain.³⁵ By extending valid copyrights for an additional twenty years, Congress protected the financial interests of the copyright holders, but increased both the distribution costs and the opportunity for business organizations to transform works from the 1920s and 1930s.³⁶ As a result, Internet publishers must be particularly careful to confirm that a work is in the public domain before electing to use ‘free’ content.

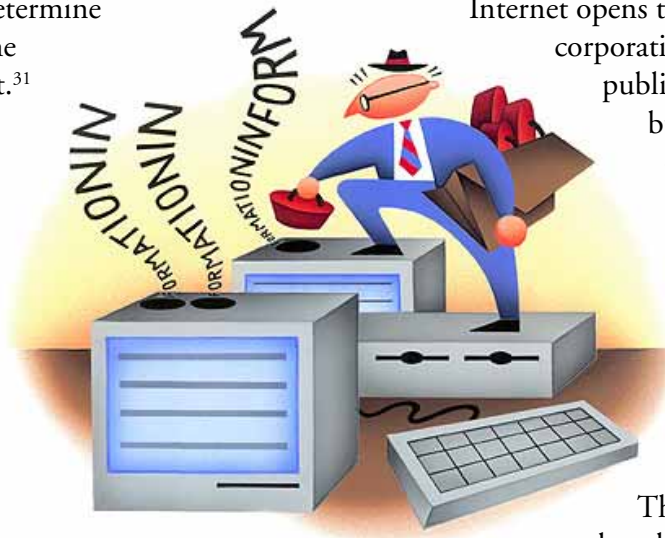
The fact that a work is free to the public on one website does not mean that the work can be re-posted to a second website without permission.

While fair use provides for some flexibility in the posting of otherwise unauthorized, copyrighted material, the doctrine is generally far narrower than non-lawyers tend to think. Fair use can only be determined by a court as an affirmative defense to illegal copyright infringement. Therefore, it should be relied upon in only rare situations, after careful analysis.

Common Law Privacy and Defamation Rights. The Internet opens the ability for any person or corporation to become a commercial publisher with the push of a button. For most companies, common law publication obligations remain in full force on the Internet. The law of defamation and common law privacy remain a significant restriction to unbridled use of the Internet for publication.

The issues involving common law defamation and privacy rights are not unique to business organizations on the Internet. The potentially volatile nature of instantaneous publications should make organizations aware that dangers may exist. Policies that require editorial control, content review, and regular policing should be adopted and enforced so the organization does not find itself embarrassed or liable for the words published on its behalf.

Defamation. A statement is defamatory if “it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him.”³⁷ The traditional, common law definition called a statement defamatory if it held one out for hatred, ridicule, or contempt. Any publication to a third person, such as through publication on a website or through sending an e-mail, will give rise to liability. Even if the statement is not made directly by or on behalf of the organization, the organization is liable if it republishes the statement by posting another’s materials to the website or if it fails to take



reasonable steps once it is made aware that defamatory material has been posted on one of its facilities. As a result, a business is responsible for defamatory material in work it creates, licenses, or borrows. It will also be liable for the defamatory work posted to its site by third parties if it fails to remove that defamatory material once it is on notice of the content.

One particularly insidious form of libel is to falsely attribute quotes to a person. The Supreme Court has held that otherwise unobjectionable statements could be deemed libelous when they were transformed into quotes.³⁸ The practice of forwarding e-mail could give rise to such liability, if harsh statements are mis-attributed in forwarding the e-mails to a listserv or newsgroup.

False Light Privacy Invasion. The common law doctrine of False Light has evolved into a close approximation of defamation for those statements that are injurious but not so contemptuous as to be defamatory, as such privacy invasions are intentional torts requiring intent or reckless disregard of the truth rather than the negligence standard available for libelous statements made regarding private persons.³⁹

c. Intrusion into Seclusion. Statements do not have to be false to be actionable. Unwanted, highly offensive, broadly disseminated publication of one's personal private information remains a common law tort susceptible to Internet abuse.⁴⁰ Broad publication of physical or mental health issues, which identify individuals, may result in liability. A well-meaning public service notice, intended to promote social responsibility, that identifies a family in dire financial need might also be actionable if published to the public on the Internet.

Publicity Rights. Another aspect of privacy is the publicity rights of those whose name, likeness or other identifying information is used on the website.⁴¹ States like New York, California and many others protect these publicity rights very broadly. The California statute is representative: "Any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes

of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent . . . shall be liable for any damages sustained by the person or persons injured as a result thereof."⁴²

While a website may be analogized to publishing, courts have recognized that a website that is used to promote the goods or services of an organization may be deemed to be a commercial use.⁴³ Further, most states do not require that the photographs be of famous people.⁴⁴ Showing recognizable individuals from corporate events, or panel discussions creates the impression of association with a company's products or services and requires the permission of each person who is identifiable in the photographs

Trademarks. Trademarks create a number of issues for corporations on the Internet. Management of trademark disputes have given rise to some of the most controversial aspects of the international Internet policies.⁴⁵ Trademarks, trade names, and service marks represent significant corporate assets for most businesses. They must be utilized effectively in the design of the corporate website, coordinated with the domain name of the company, and policed aggressively to prevent improper uses.

Trade Names as Domain Names. The U.S. Patent and Trademark Office has been reluctant to register domain names as trademarks.⁴⁶ "The mark as depicted on the specimens must be presented in a manner that will be perceived by potential purchasers as indicating source and not as merely an informational indication of the domain name address used to access a web site."⁴⁷ As a result, mere addresses will not serve as trademarks. Neither will a domain name if it merely serves to advertise the organization's own products or services.⁴⁸

The use of a company's existing trademark poses no additional problems to trademark protection. Instead the domain name, if it differs from the organization's name, must be distinctive and be used as an identifier of the company's goods or services rather than merely serve as an address for the website that promotes those goods or services. If the company wishes to create a trademark out of its domain

name, however, the Patent Office policy requires that the entire name, such as Amazon.com, be used in the marketing and advertising of the company. L.A. Times is a trademark but LATimes.com would not be because that is not the newspaper's identifying mark on its advertising. Sites such as "Shop.com" are not using the domain name as a trademark.⁴⁹

Additionally, market changes to the domain name industry and the growth of registered names has moved commercial traffic beyond the top level domain of ".com" into ".net" and to the county code top level domains such as ".tv." Absent trademark rights, there is no protectible interest in generic.net by generic.com. Since market power and consumer identification improve a company's revenue, a company should develop enforceable trademarks as part of its domain name strategy to limit public confusion and improve customer service.

Policing Trademarks on the Internet. Companies should be careful to protect both the trademark of the organization and the domain name.⁵⁰ On an ongoing basis, companies must research its name to be sure that other organizations are not using the name or a close facsimile as a domain name on the Internet.⁵¹ An example of the difficulties faced in policing trade names is shown with the 2000 presidential race. Political organizations for both the Bush and Gore presidential campaigns have been closely mirrored by parody sites.⁵² www.gwbush.com mocks www.georgebush.com site, while www.algore.org does the same to Gore's official site at http://www.gore2000.org/.⁵³ The parody websites may become an embarrassment, while more cleverly targeted sites could steal sales and income. To the extent that these websites are trading on the confusion caused by using the organization's name, the organization should aggressively seek court protection of its trademarks to prohibit confusion and commercialization.⁵⁴

Confusing use of a company's trademark by a third party in a domain name is now actionable under federal law. Under the anti-cyberpiracy provisions of the Lanham Trademark Act,⁵⁵ a party who registers a domain name using the trademark of another party with the intent to resell the mark or use the mark in a manner that would create public

confusion will be liable.⁵⁶

In addition to policing the various top level domains for uses of the company's trademark, a company must also police from similar uses of the mark. The practice of "typosquatting" is the practice of using domain names that include the common typographical errors to popular trademarks. For example, Foxmews.com is a site dedicated to promoting civil disobedience and anti-corporate activities.⁵⁷ This practice can be turned to a corporation's advantage. For example, Britannica Encyclopedias is available from both Britannica.com and Britanica.com to account for the alternate spellings.⁵⁸

Linking and Framing. Another common use of an organization's website is to link that site to others on the Internet by adding a hyperlink address to a web page owned by another party.⁵⁹ Although a common practice, linking may raise some legal issues that companies should recognize.

“Since market power and consumer identification improve revenue, a company should develop enforceable trademarks as part of its domain name strategy to limit public confusion and improve customer service.”

Linking. There seems no significant concern that linking violates the copyright of the site being linked. The address itself is a fact that cannot be protected by copyright.⁶⁰ The link does not violate any of the exclusive rights of the copyright holder to the work - it merely provides an efficient marker to find the work. Finally, at least one court has suggested linking as a way for a defendant in an infringement action to avoid liability.⁶¹

Deep Linking. The primary intellectual property concern for linking arises when the link bypasses

layers of information that the author of the linked site had intended the audience to see. This process, sometimes referred to as ‘deep linking’ may result in directing consumers past pages with a competitors advertising. Although doubtful, deep linking may still give rise to liability on contract grounds or trademark grounds. If the website usage policy prohibits any linking to the page for commercial use, then this contract may be enforceable.⁶² Enforcement is more likely if the prohibition is embodied in an agreement that requires the user to make an affirmative acknowledgement of the provision rather than a passive paragraph in a hard to find page of terms and conditions.⁶³

Careful web page design can eliminate the ability of a viewer to bypass pages, so in the absence of any legal precedent, a technological rather than legal solution should be sought to protect from unwanted linking. This approach may be beneficial and economically more efficient in many e-commerce situations.

A remaining concern with linking is the extent to which the design of a web page may create the false impression that the content is created by the linking company. Trademark infringement may arise from deep linking, if the referencing page and the selected deep link are such that users will likely be confused as to the source of the linked pages. Linking may, in some situations, create an endorsement of the linked content. If the linked pages are violating the privacy or publicity rights of a third party, the linking site should be under an obligation to remove the links once it is aware of the tortious conduct.

Framing. “Framing enables a Web page designer to split a page into independent scrollable regions, each capable of displaying a separate and distinct external Web page. Rather than having to leave the screen of one Web page to access another, the framing feature allows a user to “display” a portion of a separate Web site on the one originally accessed.”⁶⁴ This practice creates far more potential liability than the acts of linking.

The frames can create the mistaken impression that the computer user is receiving content or services from one website, when another source is



providing the data. For example, Total News created frames which it used to provide news stories of interest to its readers. The news content came from publishers such as the Washington Post. Total News never copied the stories, but by framing the news with its own advertising, it used the content of other publishers to help it sell advertising.⁶⁵ Because there is no direct copying, most analysts do not believe it is a copyright violation, although it could be argued that this creates a derivative work when used to create a likelihood of confusion or to hide the trademarks of the content provider; however, it is likely that it would violate the Lanham Act or state trademark laws. To date, no reported litigation has addressed the matter.

Wherever possible, cooperative licensing agreements should be utilized to eliminate any issues regarding permissible conduct. Such agreements should protect the trademarks of both parties to the agreement, outline the acceptable uses to which each party can put its website, and provide for mutual policing of the Internet from potentially misappropriating conduct. The license agreement may also serve as evidence regarding the value of the content and enforceability of the publisher’s rights in future litigation.

Metatags. Metatags are words embedded in a website that allow Internet search engines to locate a site. Some search engine prioritize a site by the number of times the term appears from that site.⁶⁶ The use of metatags is a common practice. The legal question is whether the use of trademarks from

competitors constitutes an infringement of that trademark. The use of a competitor's metatag allows a competitor to appear on a search engine list when a consumer types another company's name. For example, by embedding "Barbie" in an adult website, that site appeared on searches for Mattel's doll.⁶⁷ The potential for infringement may exist if the extensive use of the competitor's trademark and the design of the website will lead to the likelihood of consumer confusion. Assuming there is not trademark infringement from the domain name or other conduct, limited use of trademarks in the metatags should not be sufficient to create the likelihood of confusion or dilution of a famous trademark.⁶⁸

The issue of linking metatags to the advertising of third parties has also been tested once in court. Playboy sued the Internet portal Excite.com for selling banner advertisements that were triggered by a consumer's use of the trademarked Playboy® or Playmate® as a search term.⁶⁹ The court dismissed the trademark because to find the claim actionable would be to expand the role of trademarks in the English language. The claim that the banner advertisements created initial interest confusion was also found wanting because the advertisements themselves did not create any confusion. Nonetheless, Estee Lauder has brought a similar suit against Excite.⁷⁰ Since that is a proper name, and the issue may also include the use of a name for commercial purpose, the analysis may be somewhat different.⁷¹

Design Agreement Provisions. As is discussed above, it is important that copyrights and intellectual property interests not be violated with regard to use of the Internet. If the organization is relying upon third party developers to put together its web site, then before the website is designed, the parties should establish what materials and content will be incorporated into the site and which company owns those materials.

Unfortunately, the company purchasing the website design may not be able to insist that it be the copyright holder of the website for practical reasons. Many of the elements utilized on a complex web page may be built from software programs owned by the independent contractor creating the site and

used repeatedly by that vendor on site after site. In those situations, a more specific license agreement should be used itemizing what works are granted as a non-exclusive, perpetual license and what materials are assigned to the company. Be wary of short-term licenses because those licenses will result in renego-

“Another issue that may arise from the website design is which party is responsible for selecting, editing and posting the content on the website, as well as liability and indemnification issues for that content.”

tiation of the website contracts or redesign of the website.

The issue of website design is more critical if the site includes information from multiple parties or through affiliated organizations. When a third party web host is used, the contract should clearly provide who owns the data that is generated (names, addresses, etc.) and what usage rights the other party has to that data.

Another issue that may arise from the website design is which party is responsible for selecting, editing and posting the content on the website, as well as liability and indemnification issues for that content. Web page designers range from graphic artists who happen to use the computer to sophisticated software programs customized to the needs of an individualized client. The specifications of the website, its operations, suite of customer services, and general design should all be specified in advance through the design agreement. Finally, the agreement should provide for testing of the site and, to the extent it is an interactive site, maintenance and updating of the software embedded in the site.

Data Collection from Web Users

Introduction to Data Tracking. DoubleClick.Com is the industry leader in reviewing the demographic marketing of online businesses. As a result of its purchase of Abacus, it has created Abacus Direct, a direct market targeting tool that boasts 1500 participants, 2 billion transactions, a database of 90 million households, 10-20 million transactions weekly, and access to every mail order buyer.⁷²

Although DoubleClick's policy identifies only non-personal information,⁷³ its ownership of the compressive Abacus database creates the power for almost unlimited individual transaction tracking. As the company explains: "The non-personally identifiable information collected by DoubleClick is used for the purpose of targeting ads and measuring ad effectiveness ... [h]owever, as described in 'Abacus Alliance' and 'Information Collected by DoubleClick's Web Sites' below, non-personally identifiable information collected by DoubleClick in the course of ad delivery *can be associated with a user's personally identifiable information* if that user has agreed to receive personally-tailored ads."⁷⁴

As the policy explains, DoubleClick is committed to giving consumers notice of its activities and the choice to opt out of the system.⁷⁵ In respect to the areas that are most actively being regulated, the DoubleClick policy provides that "the Abacus Online database will not associate any personally-identifiable medical, financial, or sexual preference information with an individual. Neither will it associate information from children."⁷⁶

The tracking of data is often accomplished through the use of "cookies." These are small text files stored in the computer. They have no executable code and do not act to operate or interfere the computer. They can be used to store account information or passwords for the user. They also can provide data on which websites and web pages have been viewed. Other tracking devices allow for monitoring of the data packet information as it travels from the consumer to the ISP and into the Internet so that no software browser option in Netscape or Internet Explorer can block this passive tracking.

Privacy concerns also create perceived barriers to use and involvement by the public. The Federal Trade Commission ("FTC"), the federal regulatory body most actively involved with online privacy issues, identified privacy concerns as one of the inhibitors to Internet growth. The FTC explained that "consumers have less confidence in how online service providers and merchants handle personal information than they have in how traditionally offline institutions, such as hospitals and banks, handle such information. In fact, a substantial number of online consumers would rather forego information or products available through the Web than provide a Web site personal information without knowing what the site's information practices are."⁷⁷

Nonetheless, the policies of DoubleClick are representative of the industry and the law. The demographic information provides valuable information for retailers and allows marketing to be targeted selectively and efficiently. While the public is generally disdainful of the intrusion into private activities, there has been no effective effort to ban the practice or change public disclosure of private data. DoubleClick's choice not to track sexual preference may reflect sensitivity to invasion of privacy torts and other litigation stemming from improper disclosure of such information.⁷⁸ The other areas where it does not track data — children, medical or financial information — reflect where current legislation in the United States has limited free access to personal information.⁷⁹

Minors. Despite the concerns raised by the FTC, the only federal regulation for general online privacy covers children under thirteen years of age, which was adopted as part of the Children's Online Privacy Act ("COPPA").⁸⁰ The federal requirements apply "[i]f you operate a commercial Web site or an online service directed to children under 13 that collects personal information from children or if you operate a general audience Web site and have *actual knowledge* that it collects personal information from children, you must comply with the Children's Online Privacy Protection Act."⁸¹ Organizations that offer children chat rooms, e-mail or hobby informa-

tion that may result in collecting the child's personal data, such as name and address or e-mail must comply with the FTC regulations.⁸²

These regulations require that any party that collects personal information from children must first receive parental consent. The obligations for consent are more detailed if the data is shared with third parties. Although not stated, the implicit goal of the regulations is to eliminate the collection of data on children in all situations other than those in which the child has been enrolled in a program by the parent. From the planning perspective, nothing in the regulations suggest that the FTC will remain limited by Congress to enforcing regulations for only those under thirteen years of age. Business should not be surprised to see the FTC jurisdiction expand over time.

Financial Data. In a comprehensive update of federal banking and insurance law, Congress has begun the piecemeal regulation of online privacy. As it said in the preamble to the Gramm-Leach-Bliley Act “[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.”⁸³ Under this policy, a financial institution must allow a customer to opt out of having nonpublic personal information to non-affiliated third parties.⁸⁴ The financial institution must provide the disclosure at the time of the initial transaction and at least annually thereafter. In addition to permitting disclosure for a variety of service-related activities, disclosure may be allowed with the consent of the consumer.⁸⁵

Health Care Information. In 1996, Congress adopted the Health Insurance Portability and Accountability Act (“HIPAA”) to promote the ability of the public to transfer health care and insurance coverage from one provider to another and to simplify the transactions involved in the insurance industry.⁸⁶ Under HIPAA, private health care information also requires substantial privacy and security measures be taken to protect an individual from improper disclosure of health care information.



International Transactions. For organizations that operate beyond the borders of the United States, the obligations may be greater than they are domestically. For example, Canada has just enacted the Personal Information Protection and Electronic Documents Act, which requires that an organization obtain permission before collecting data, except in certain enumerated circumstances, such as for police purposes or journalistic, artistic, or literary uses.⁸⁷ Similar, significantly more restrictive privacy regulations exist in other jurisdictions such as the European Union. As a result, multinational corporations must choose to create very restrictive policies that meet the most stringent jurisdiction or impose geographical limitations on the Internet services so that each service is appropriate the nation which it serves.

The European Union's Directive on Data Protection (“Directive”) has created a much more protective policy for European Union companies and those foreign organizations that choose to do business in Europe.⁸⁸ “The Directive requires companies to ensure that data is: 1) collected only for specific purposes, 2) accurate and current, and 3) discarded once no longer needed. In addition, the Directive prohibits the flow of collected data to non-EU countries that do not provide “adequate” privacy protections.”⁸⁹

The European Commission threatened to prohibit U.S. companies that were not in compliance

with the directive. U.S. industry has resisted because the Directive gives customers “the right to: access collected data, correct the data, object to its use, oppose automated decisions, and seek judicial remedies.”⁹⁰ Under intense trade pressure, the European Commission and the U.S. Department of Commerce developed a “safe harbor” provision under which U.S. companies can self-certify that they satisfy the agreed-upon provisions.⁹¹ These provisions do not reflect the European content and use restrictions, however, but rather codify the FTC approach to a comprehensive, voluntary privacy policy that allows for consumer notice and consent. A privacy policy that meets the FTC approach outlined below should meet the safe harbor provision as well.

Privacy Policy for General Sites. For adults, the unregulated marketplace provides little relief. The problem of regulating privacy concerns grows larger when the business organization uses the website

“Any business website that gathers demographic information is well served to adopt a comprehensive privacy program. The FTC has identified five core components for a privacy policy deemed fair to the public.”

services of another, commercial entity. If the business has outsourced its website to a commercial service provider, then the information gathered may have been sold as part of the original contract. From the outset, it is critical that the business understand the privacy policy of the organization with which it is contracting for website services. If that company intends to aggregate the data from the business website, the contact information may be sold before the business has an opportunity to allow its members to object. In most cases, the contract should include significant restrictions on the use of the data.

Any business website that gathers demographic information is well served to adopt a comprehensive privacy program. The FTC has identified five core components for a privacy policy deemed fair to the public. They are: “(1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.”⁹² Under such a privacy program, every user of the website would have access to the terms of the policy. These five steps do not limit the ability of a company to collect demographic or market data. Instead, the policy serves to reflect the activities in an accurate manner.

(1) *Notice.* The notice should be written in plain English, for quick consumer understanding, designed to explain the types of data that are collected by the website and how the information might be used. This should include who is collecting the data, how the data will be used, and what choices the consumer has regarding this data.

(2) *Consent.* The policy should allow users to choose whether or not to provide the data. For most business organizations, the decision not to provide personal information should not eliminate the person from participation in at least some of the website’s services. For some activities, such as chatrooms and listservs, the ability to monitor and control the users require that personal contact information be collected by the organization.

(3) *Access.* Access refers to the user’s ability to review the information provided and insure that it is correct. The FTC states that “[t]o be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.

(4) *Integrity.* Business organizations generally recognize the value of the data they have collected in their membership lists. The value of this data is directly proportional to the security of that information and the accuracy of its content. Outdated, inaccurate information should be destroyed. Reasonable steps should be taken to protect the confidential-

ity of the data. And to the extent that data is used for demographic study, personal identification should be removed from the statistical profiles. In many instances, for example, use of zip codes provides all the geographic specificity necessary for a business's study of usage and trends. Using names and addresses to study the neighborhood living habits will slow the process while risking the confidentiality of individual privacy as the data is shared by multiple participants in the study.

(5) *Enforcement.* The FTC does not actively advocate that privacy policies be enforced through operation of law. Outside the arena of children, such enforcement has not been statutorily granted, although intentional violations of a posted policy may be deemed a deceptive trade practice. The preferable enforcement mechanism is through membership in a trade association that verifies the credibility of the privacy policy. Third party enforcement relationships can be established with organizations such as the Better Business Bureau Online,⁹³ Entertainment Software Rating Board,⁹⁴ TRUSTe,⁹⁵ and the DMA Privacy Promise.⁹⁶

A comprehensive privacy policy, once adopted, will have the force of contract against the company publishing the website, unless its terms limit the scope. As a contractual right for the user, the policy will have some legitimacy; as an altruistic statement ignored in operation, the policy could result in significant liability.⁹⁷ Like other voluntarily adopted policies, the adoption of a privacy policy will obligate the company to be bound by its terms even if those terms become inconvenient. To protect the organization, every agreement with third parties regarding the Internet should include a copy of the policy and an express provision obligating that party to enforce the policy as it now exists or is amended by its terms in the future.

Self-Enforcement of Privacy Policies. Following the guidelines of the FTC provides only the first step in creating a valid privacy policy. A policy, no matter how well intended, provides no protection to a company if it is not followed. To the contrary, failure to follow a policy once adopted and published to the public may result in liability for breach of contract or

“Following the guidelines of the FTC provides only the first step in creating a valid privacy policy. A policy, no matter how well intended, provides no protection to a company if it is not followed.”

for allegations of deceptive trade practices. GeoCities, a popular website for virtual communities, was accused of “unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act” after the FTC received complaints that GeoCities members were receiving solicitations from companies that they had not specifically authorized to contact them.⁹⁸ The GeoCities privacy policy included the statement that “[w]e will not share this information with anyone without your permission....”⁹⁹ The settlement with GeoCities created a FTC guideline of explicit disclosure of reuse practice for personal information.

In addition to FTC action, companies face tremendous public pressure to comply with their stated disclosure policies. Companies like Microsoft, Toysmart, and Amazon.com have come under intense media scrutiny for misuse – and sometime even authorized but aggressive use – of the detailed customer information.

The lesson of GeoCities and the increasing power of the FTC is that the policy must be drafted with enforcement in mind. An absolute guarantee is probably unwise. “Never” is a long time in the Internet age. “Never” may also imply a guarantee against inadvertent disclosure, hacker attacks, and future business transactions.

The privacy policy must be tailored to the particular company and industry. Information may be treated differently if required for particular uses rather than voluntarily given as part of customer surveys or transactions. For example, the Amazon.com practice of informing customers of

other purchasers' related purchases is seen as a significant customer service that can only be built by tracking transactional data. Customers are not given an automatic method of opting out of the system, however, the practice of Amazon.com is to exclude gift items. By purchasing all products as gifts, savvy customers can avoid some aspects of the profiling.

Form & Content. Many of the FTC guidelines for COPPA compliance apply equally well to other companies regarding the structure and drafting of privacy policies:

An operator must post a link to a notice of its information practices on the home page of its Web site or online service and at each area where it collects personal ... Operators may want to use a larger font size or a different color type on a contrasting background to make it stand out. A link in small print at the bottom of the page — or a link that is indistinguishable from other links on your site — is not considered clear and prominent. The notice must be clearly written and understandable; it should not include any unrelated or confusing materials. It must state the following information:

- The name and contact information (address, telephone number and email address) of all operators collecting or maintaining [personal information] ...
- The kinds of personal information collected from children (for example, name, address, email address, hobbies, etc.) and how the information is collected — directly from the child or passively, say, through cookies.
- How the operator uses the personal information. ...
- Whether the operator discloses information collected from children to third parties. If so, the operator also must disclose the kinds of businesses in which the third parties are engaged; the general purposes for which the information is used; and whether the third parties have agreed to maintain the confidentiality and security of the information.¹⁰⁰

Privacy policies should be drafted as if they are binding contracts. Reasonable efforts or best efforts clauses to protect the privacy are more accurate than blanket promises. A comprehensive policy should also include the right to modify the policy from time to time without notice.

Protection of Data from Bankruptcy, Assignments, Etc. Another threat to the protection of personal data comes from the myriad of business transactions that might befall a company after a stringent privacy policy has been adopted. Proposed mergers between companies with differing privacy policies may give rise to regulatory challenges. Similarly, bankruptcy courts are beginning to balance the creditors' interest in assets of the corporation with the stated privacy rights of the consumers in the database. In a bankruptcy proceeding involving Toysmart, the FTC, 40 states' attorneys general and counsel for TRUSTe wrangled over the rights involved in the data. Ultimately, the settlement required that the data only be sold as part of a going concern sale of the website rather than in gross.¹⁰¹ The legal problems associated with the bankruptcy action might lead companies to retreat on privacy protection rather than face unwanted legal obligations in the future.

The bankruptcy proceedings also emphasize the need for lenders to properly value the intellectual property assets of a creditor. Assets that may not be assigned should have significantly less value than those assets that are freely transferable. This distinction may only be discoverable after significant due diligence. It is not uncommon for intellectual property licensing agreements to restrict voluntary and involuntary transfers, further complicating corporate mergers and bankruptcy proceedings.

Additional Regulations and Issues

Digital Signature Law. With the adoption of the Electronic Signatures in Global and National Commerce Act, Congress has created the first step in bringing about the theoretical "paperless office" that was once highly touted at the dawn of the computer age.¹⁰² This relatively simple statute provides that "a signature, contract, or other record relating to such

transaction may not be denied legal effect, validity, or enforce-ability solely because it is in electronic form.”¹⁰³ Under the law, consumers must agree to use digital signatures, and certain types of documents — wills, court papers, and notices of termination of utility services or health care benefits — are excluded from the law. Nonetheless, many transactions that previously required paper documentation can now be done using digital signatures. Similar legislation has been developed for the states as a model statute — Uniform Electronic Transactions Act — which has seen substantial adoption. To the extent that the states adopt the model act in its standard form, the federal law complements it. Where the states try to limit the scope of digital signatures, however, the federal law preempts the state restrictions.

UCITA & Shrinkwrap License Agreements. More controversial than the digital signature laws is the Uniform Computer Information Transactions Act (“UCITA”).¹⁰⁴ UCITA provides for default contractual provisions that will govern transactions in computer information which attempts to create a commercial code similar to that of goods.¹⁰⁵ The goal behind UCITA is to promote uniformity among the states, to guarantee that consumer license agreements are enforceable, and to reduce uncertainty in the software marketplace.

At its core, UCITA provides a series of publisher friendly default contracting principles for the software industry. It specifically excludes financial services as well as most traditional film, television, and music agreements.¹⁰⁶ The proposed model is highly controversial, so uniform adoption is unlikely.¹⁰⁷ Instead, until questions of federal preemption are answered and widespread adoption occurs, UCITA may result in greater instability regarding software transactions. Because UCITA primarily serves as a set of default contract terms, however, it can be used to facilitate the drafting of express agreements governing software transactions. When adopting UCITA provisions into a contract, the actual text of the provisions should be used rather than reference to section numbers or other parts of the model that may continue to be modified over time.



Security Regulations. The goal of security regulations embodied in Gramm-Leach-Bliley, HIPAA and other federal law is to protect the confidentiality of private data from both “the risk of improper access to electronically stored information” and “the risk of interception during electronic transmission of the information.”¹⁰⁸ These security measures look both inward and outward. Companies must utilize the best practices to thwart hacker attacks and accidental disclosure. The data must also be protected from improper access by unauthorized employees as well as natural disaster and human error. The security standards provide a comprehensive, formal process for protection of information not unlike that necessary in most industries today.

As such, the steps necessary to comply require the use of good technical practices that are available today, along with rigorous documentation and ongoing supervision. Security regulations are being developed under the regulations being finalized pursuant to HIPAA as a comprehensive single regulation embodied in 45 C.F.R. 142.308. This regulation has been proposed as the most comprehensive Internet security regulation to date, and should be expected to serve as the basis for much of the future security regulations.

The proposed security regulations, however,

reflect a comprehensive series of steps designed to maximize the security of private health care information. In addition, during the current presidential campaign both presidential candidates Gore and Bush have promised greater federal protection for the personal financial and health care data of the public. This campaign emphasis suggests that federal action, through legislation or executive order, may expedite the implementation date of regulations substantially similar to those proposed by the Department of Health and Human Services.

Proposed section 142.308 attempts to combine administrative procedures, physical safeguards, technical security services, and technical mechanisms into a comprehensive security standards. At its core, the standards attempt to set a minimum standard to provide standards in each of the following areas:

- Identification and Authentication;
- Authorization and Access Control;
- Accountability, Integrity and Availability;
- Security of Communication; and
- Security Administration.

The proposed regulations emphasize the following components for the organizational practices that must be adopted within each organization having access to the private health care data:

- Develop and adopt security and confidentiality policies;
- Identify information security officers; and
- Provide education and training programs.

Similarly, the proposed regulations emphasize the following technical practices and procedures that must be adopted to safeguard the private health care data during storage, transmission and retrieval:

- Individual authentication of users;
- Access controls;
- Audit trails;
- Physical security and disaster recovery;
- Protection of remote access points;
- Protection of external electronic communications;
- Software discipline; and
- System assessment.

“Companies must utilize the best practices to thwart hacker attacks and accidental disclosure. Data must also be protected from improper access by unauthorized employees as well as natural disaster and human error.”

The need for access controls, audit trails, physical security, disaster recovery, software discipline, and system assessment is required for any company that provides services involving the data or computer equipment.

Chatroom as Boardroom. For formal meetings of the Board of Directors, chatrooms may provide a valid alternative to a physical meeting, provided that members can participate concurrently in all matters.¹⁰⁹ An organization may also be required to verify who attended the meeting.¹¹⁰ This can be done with simple passwords, mailed to each voting director prior to the meeting, or through the use of security software. A chatroom provides the users with real-time interaction that could be used by a charity in lieu of face-to-face meetings. The remaining obstacle for broad adoption of this technology is the difficulty in having some participants attend in person while others are typing. So long as all participants can see a computer screen, this poses only a practical, rather than legal difficulty. If voice and sound capability are added to the Internet tools, then the those uses should be treated as a telephone conference.

SEC Disclosures for Publicly Traded Companies.

Although most securities issues are beyond the scope of this introduction, the impact of the Internet on securities publications and public disclosure must not be segregated from other e-commerce and Internet-related issues. The Securities and Exchange Commission (“SEC”) has adopted the position that

“when an issuer embeds a hyperlink to a web site within a document that is required to be filed or delivered under the federal securities laws, the issuer should *always* be deemed to be adopting the hyperlinked information for purposes of the anti-fraud provisions of the federal securities laws.”¹¹¹

This means that statements made on a company’s website may be incorporated by reference into those documents filed with the SEC on an ongoing basis. Put another way, material misstatements on a corporate website could lead to federal securities fraud allegations.

Undoubtedly, most corporations do not review their websites with the same degree of due diligence as the documents annually filed with the SEC. Most likely, even press releases are given greater scrutiny. Nonetheless, the material misstatement of a material fact or failure to include a material fact in a manner that leads the statement to be misleading could result in securities liability. It is critical, therefore, that the

Internet be deemed part of the corporate publication and given appropriate due diligence within each company.

Conclusion

The issues raised in the use of e-mail and websites provide both a challenge and an opportunity for all business. Careful planning, respect for privacy and its broader implications, and understanding of the role as a corporate publisher are the common issues that all e-commerce companies face. Whether a company has embraced the new technology or merely provided e-mail as a courtesy for limited uses, the issues discussed above must be addressed. Despite the attention given to e-commerce, business remains at the threshold of this new business model. Careful planning today will allow business to make the transition to the truly new business world that is coming.

Notes

¹ Of Counsel, Gallagher, Callahan & Gartrell and Professor of Law, Franklin Pierce Law Center. Sections of these materials are adapted from Jon Garon & Lisa Runquist, *Business In Cyberspace - An Introduction To The Practical And Legal Hurdles Of The New Frontier*, Presented before the California State Bar, Business Law Section Annual Meeting June 2000 and the American Bar Association Annual Meeting, July 2000.

THESE MATERIALS ARE PRESENTED WITH THE UNDERSTANDING THAT, DUE TO THE RAPIDLY CHANGING NATURE OF THE LAW, INFORMATION CONTAINED IN THIS PUBLICATION AND THE PRESENTATION MAY BECOME OUTDATED. AS A RESULT, ANY INDIVIDUAL USING THESE MATERIALS AND INFORMATION PRESENTED MUST ALWAYS RESEARCH ORIGINAL SOURCES OF AUTHORITY AND UPDATE INFORMATION TO ENSURE ACCURACY WHEN DEALING WITH A SPECIFIC CLIENT OR FIRM MATTER. IN NO EVENT WILL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THESE MATERIALS.

THESE MATERIALS WERE FIRST PRESENTED OCTOBER 3, 2000.

² E.g., toys.com, Amazon.com.

³ E.g., Toys-R-Us, Barnes & Noble.

⁴ See, *ACLU v. Reno*, 521 U.S. 844, 849 (1997).

⁵ Jennifer Baljko Shah, *E-commerce faces slew of legal issues*, Electronic Buyers' News, May 15, 2000.

⁶ Encyclopedia Britannica, "Computer Science" <<http://www.britannica.com/bcom/eb/article/4/0,5716,117724+7+109626,00.html>>.

⁷ E-mail set to alter retail methods, SGB UK, May 20, 1999 at 11.

⁸ *ACLU v. Reno*, 929 F. Supp. 824 834 (E.D. Pa. 1996), aff'd 521 U.S. 844 (1997).

⁹ James Q. Walker, *Serving Clients Well: Avoiding Malpractice and Ethical Pitfalls in the Practice of Law*, 60 PLI/NY 297 (October 1999) (citing New York, (N.Y. City 94-11 (1994)); North Carolina RPC 215 (1995); Iowa Op. 96-01 (1996); Arizona Op. No. 97-14 (1997); and Tennessee Op. 98-A-650 (a) (November 19, 1998)).

¹⁰ E.g., *Playboy Enterprises, Inc. v. Terri Welles Inc.*, 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999).

¹¹ 18 U.S.C. §§ 2510, 2511 (1999). See, James Q. Walker, *Serving Clients Well: Avoiding Malpractice and Ethical Pitfalls in the Practice of Law*, 60 PLI/NY 297 n.4 (October, 1999).

Several state bar ethic opinions have cited the criminalization of the interception of e-mails as one reason for concluding that e-mail enjoys a reasonable expectation of privacy, or at least have concluded that the

risk of interception is no greater than with telephone calls and therefore communication by e-mail does not necessarily waive the attorney-client privilege or violate DR4-101 or its equivalent. See, e.g., D.C. Bar Op. 281 (1998) (transmission of confidential information by unencrypted e-mail not per se violation of confidentiality rules); Tennessee Op. 98-A-650(a) ("It is generally accepted that the security of e-mail is probably no more problematic than the security of a non-cordless telephone."); Pennsylvania Op. 97-130 (1997) ("the risk of intentional or inadvertent interception does not appear to be materially different for e-mail when compared to other forms of communication"); South Carolina Op. 97-08 (1997) (lawyer has reasonable expectation of privacy when sending confidential information through electronic mail) (overruling contrary prior ruling in S.C. 94-27); Vermont Op. 97-5 (1997) (since e-mail privacy is no less than that expected with telephone calls, and unauthorized interception is illegal, no violation of 4-101 in communicating by unencrypted e-mail); see also Illinois State Bar Op. 96-10 (1997) (observing that the distinction between Internet messages and telephone calls is that Internet messages may be temporarily stored at a router maintained by an ISP, and therefore a router employee could lawfully read all or part of the message in the course of monitoring transmissions, or may violate the law by impermissibly intercepting a message).

¹² Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

¹³ Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-1010 (1994)). See, Tatsuya Akamine, *Proposal For A Fair Statutory Interpretation: E-Mail Stored in a Service Provider Computer is Subject to an Interception under the Federal Wiretap Act*, 7 J.L. & Pol'y 519 (1999).

¹⁴ See, Tatsuya Akamine, *Proposal For A Fair Statutory Interpretation* n.5. Akamine identifies the following additional statutes: Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801-1811 (1994), 18 U.S.C. §§ 2511 (1994 & Supp. III 1997), and 18 U.S.C. §§ 2518-2519 (1994)); Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-1010 (1994) and in scattered sections of 18 U.S.C. and 47 U.S.C.) (CALEA requires telephone companies' cooperation with law enforcement and also extends the protections under the ECPA to a cordless telephone); Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. III 1997) (regulating government's handling of individual information); Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1994 & Supp. III 1997) (regulating credit reporting agencies to protect the confidentiality of credit reports); Video Privacy Protection Act of 1988, 18

U.S.C. §§ 2710-2711 (1994) (prohibiting video stores from disclosing customers' rental records); Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (codified in scattered sections of 47 U.S.C., 15 U.S.C., 46 U.S.C., 18 U.S.C., 50 U.S.C.) (prohibiting cable operators from disclosing customers' viewing records).

¹⁵ See, Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994); Bohach v. City of Reno, 932 F. Supp. 1232, 1236-37 (D. Nev. 1996) ("An 'electronic communication,' by definition, cannot be 'intercepted' when it is in 'electronic storage,' because only 'communications' can be 'intercepted,'"); United States v. Reyes, 922 F. Supp. 818, 836 (S.D.N.Y. 1996).

¹⁶ See, e.g., U.S. v. Charbonneau, 979 F. Supp. 1177, 1184-85 (S.D. Ohio 1997) (e-mail transmission enjoys a limited reasonable expectation of privacy); United States v. Maxwell, 45 M.J. 406, (U.S.A.F. Crim. App. 1996) (because of privacy policy and the private storage of e-mail by America Online, the military court found its users are afforded more privacy than other Internet messages).

¹⁷ Bohach v. City of Reno, 932 F. Supp. 1232, 1236-37 (D. Nev. 1996). See also, Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994).

¹⁸ 18 U.S.C. § 2511 (2)(d). State law and other statutory provision may require the permission of both parties to the transmission.

¹⁹ Stratton Oakmont Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. May 24, 1995), slip op.

²⁰ Curtis v. DiMaio, 46 F. Supp. 2d 206, 209-10 (E.D.N.Y. 1999) (dismissing claims of a hostile work environment. The lawsuit stemmed from racial jokes sent via e-mail and forwarded to ten additional readers.).

²¹ Playboy Enterprises, Inc. v. Terri Welles Inc., 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999) (allowing for discovery of hard drive because defendant regularly deleted e-mail from system). The court nonetheless recognized that e-mail to attorneys was protected by attorney-client privilege. Welles ultimately prevailed under the claims of fair use for the metatags in her "Playmate of the Year" description of her website.

²² See, Houston Chronicle March 30, 2000.

²³ Unsolicited Electronic Mail Act of 1999, 106 H.R. 3113, introduced October 20, 1999. The requirements also serve as a code of good practice until such time as the legislation becomes law (if ever). Most important, be courteous, brief, and provide both legitimate contact information and a method for recipients of the e-mail to request that no future e-mail be sent to that recipient.

²⁴ Kim S. Nash, *Amazon.com revises privacy policy on use of customer data*, Network World, September 11, 2000.

²⁵ See, 17 U.S.C.A. §106 (2000).

²⁶ An employee, creating the work within the scope of her employment will initially vest in the employer. 17 U.S.C. §101 (2000).

²⁷ 17 U.S.C. §101 (2000). "Audiovisual works are works that

consist of a series of related images which are intrinsically intended to be shown by the use of machines or devices such as projectors, viewers, or electronic equipment, together with accompanying sounds, if any, regardless of the nature of the material objects, such as films or tapes, in which the works are embodied." *Id.*

²⁸ This licensed content may still give rise to legal liability for defamation, privacy and publicity claims. See the discussion on defamation and privacy, *infra*.

²⁹ Posting a copyrighted work to a website would comprise a reproduction, distribution and display of the work. See, 17 U.S.C.A. §106 (2000).

³⁰ 17 U.S.C.A. §107 (1999). The full text is as follows:

Limitations on exclusive rights: Fair use

Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include—

- (1) the purpose and character of the use, including whether such use is of a commercial nature or is for business educational purposes;
- (2) the nature of the copyrighted work;
- (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- (4) the effect of the use upon the potential market for or value of the copyrighted work.

³¹ See, Harper & Row v. Nation Enterprises, 471 U.S. 539,562 (1985) ("The crux of the profit/ business distinction is not whether the sole motive of the use is monetary gain but whether the user stands to profit from exploitation of the copyrighted material without paying the customary price.").

³² *Id.*

³³ Marobie-FL, Inc. v. National Ass'n of Fire Equip. Distribs., 983 F. Supp. 1167, (N.D. Ill. 1997) (finding that the use of unlicensed clip art was not fair use. The court described the organization's website. "It is also undisputed that [the organization] uses its Web Page for the commercial purposes of promoting the association (whose members pay dues) and generating advertising revenue. The clip art files enhanced the Web Page and furthered these commercial purposes; they were clearly not placed on the Web Page for the purposes of criticism, comment, news reporting, teaching, scholarship, or research." *Id.* at 1175.

³⁴ 17 U.S.C.A. 302 (2000), Digital Millennium Copyright Act, Pub. L. 105-304, 112 Stat. 2860 (1998).

³⁵ 17 U.S.C.A. 303 (2000).

³⁶ See, Jon Garon, *Media and Monopoly in the Information Age: Slowing the Convergence at the Marketplace of Ideas*, 17

CARDOZO J. LAW & ART 491 (1999).

³⁷ Restatement (Second) Torts §559 (1977). Under California law, “libel is a false and unprivileged publication by writing . . . which exposes any person to hatred, contempt, ridicule, or obloquy, or which causes him to be shunned or avoided, or which has a tendency to injure him in his occupation.” Cal. Civ. Code § 45 (West 1999).

³⁸ Masson v. New Yorker Magazine, 501 U.S. 496, 522 (1991).

³⁹ Gertz v. Robert Welch, Inc., 418 U.S. 323, (1974).

⁴⁰ Restatement (Second) Torts § 625B (1977) (“One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”).

⁴¹ Cal. Civ. Code §3344 (Deering 1999).

⁴² Cal. Civ. Code §3344(a) (Deering 1999). The statute also provides for \$750.00 in statutory fees and injunctive relief.

⁴³ KNB Enters. v. Matthews, 78 Cal. App. 4th 362, 368, 92 Cal. Rptr. 2d 713, 718 (2d Dist. 2000) (holding use of models’ photographs on subscription website constituted actionable violation of Cal. Civ. Code §3344, not preempted by federal copyright laws).

⁴⁴ *Id.*

⁴⁵ See, The Internet Corporation for Assigned Names and Numbers (“ICANN”) <www.ICANN.org>. Debates over trademarks and domains names culminated in the adoption of the Uniform Domain Name Dispute Resolution Policy in 1999.

⁴⁶ United States Patent and Trademark Office, Trademark Examination of Domain Names, Examination Guide No. 2-99 (September 29, 1999) <<http://www.uspto.gov/web/offices/tac/notices/guide299.htm>>.

⁴⁷ *Id.*

⁴⁸ *Id.* citing In re Reichhold Chemicals, Inc., 167 USPQ 376 (TTAB 1970); TMEP §1301.01(a)(ii).

⁴⁹ Shop.com is an Idealab Company “pre-IPO” shopping portal. <<http://www.shop.com>>. Visited September 24, 2000.

⁵⁰ “A domain name is part of a Uniform Resource Locator (URL), which is the address of a site or document on the Internet.” United States Patent and Trademark Office, Trademark Examination of Domain Names, Examination Guide No. 2-99 (September 29, 1999) <<http://www.uspto.gov/web/offices/tac/notices/guide299.htm>>.

⁵¹ E.g., Brookfield Communications, Inc., v. West Coast Entertainment Corporation, 174 F.3d 1036 (9th Cir. 1999) (Moviebuff infringed by Moviebuff.com); Mattel, Inc. v. Internet Dimensions, Inc., 2000 U.S. Dist. LEXIS 9747 (S.D.N.Y. 2000) (Mattel’s Barbie infringed by pornographic Barbiesplaypen.com).

⁵² See, Massie Ritsch, *Parody Web Sites Skewer Campaigns*, L.A. Times, April 23, 2000 at A26.

⁵³ Meanwhile, www.algore.org is a commercial site used to divert traffic to a commercial credit service Creditcards.com. See also, <<http://www.algore.com/>> which sells political

trinkets and collectibles by PoliticalShop.com.

⁵⁴ E.g., New York State Soc’y of Certified Pub. Accountants v. Eric Louis Assocs., 79 F. Supp. 2d 331, (S.D.N.Y. 1999)

(Certified Public Accounts association won injunction and attorneys’ fees against commercial website using similar acronym); Online Partners.com, Inc. v. Atlanticnet Media Corp., 2000 U.S. Dist. LEXIS 783 (N.D. Cal. Jan. 18, 2000) (Gay.net successfully gained the website for Gaynet.com).

⁵⁵ 15 U.S.C. §1125(d) (1999).

⁵⁶ 15 U.S.C.A. §1125(d) Cyberpiracy prevention. The statute provides the following:

(1) (A) A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person-

(i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and

(ii) registers, traffics in, or uses a domain name that—

(I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;

(II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark

....

⁵⁷ <<http://www.foxmews.com/>>. Foxmews uses a logo graphically similar to Fox Television. The site also includes a very large disclaimer, and is designed to provide comment on sensational news techniques. The use as a non-commercial critique may allow Foxmews to avoid trademark infringement.

⁵⁸ <<http://www.britannica.com>; <http://www.britanica.com>>.

⁵⁹ “A core feature of the Web is “hypertext” links. A link, often represented by a colored textual icon or graphic image, allows a user to “click” on a designated area of the screen and transfer to the home page of another Web site, perhaps located on the other side of the world.” Frank C. Gomez, *Misappropriation: Washington Post v. Total News, Inc.*, 13 Berkeley Tech. L.J. 21, 22 1998.

⁶⁰ Ticketmaster Corp. v. Tickets.Com, Inc., 54 U.S.P.Q.2D (BNA) 1344, 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. 2000) (“Further, hyperlinking does not itself involve a violation of the Copyright Act (whatever it may do for other claims) since no copying is involved, the customer is automatically transferred to the particular genuine web page of the original author. There is no deception in what is happening. This is analogous to using a library’s card index to get reference to particular items, albeit faster and more efficiently.”); Shaw v. Lindheim, 919 F.2d 1353, 1356 (9th Cir. 1990) (“Copyright law protects an author’s expression; facts and ideas within a work are not protected.”).

⁶¹ Los Angeles Times v. Free Republic, 2000 U.S. Dist. LEXIS 5669 (defendant Free Republic was asked by L.A. Times and Washington Post to link to articles rather than reproduce the

articles in full as it had done for the Jewish World Review as a way to use plaintiff's content in a non-infringing manner).

⁶² *Ticketmaster Corp. v. Tickets.Com, Inc.*, 54 U.S.P.Q.2D (BNA) 1344, 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. 2000) ("the "terms and conditions" set forth on the home page of the Ticketmaster site. This provides that anyone going beyond the home page agrees to the terms and conditions set forth, which include that the information is for personal use only, may not be used for commercial purposes, and no deep linking to the site is permitted. In defending this claim, Ticketmaster makes reference to the "shrink-wrap license" cases, where the packing on the outside of the CD stated that opening the package constitutes adherence to the license agreement (restricting republication) contained therein. This has been held to be enforceable. That is not the same as this case because the "shrink-wrap license agreement" is open and obvious and in fact hard to miss. Many web sites make you click on "agree" to the terms and conditions before going on, but Ticketmaster does not. Further, the terms and conditions are set forth so that the customer needs to scroll down the home page to find and read them. Many customers instead are likely to proceed to the event page of interest rather than reading the "small print." It cannot be said that merely putting the terms and conditions in this fashion necessarily creates a contract with any one using the web site. The motion is granted with leave to amend in case there are facts showing Tickets' knowledge of them plus facts showing implied agreement to them.").

⁶³ *Id.* ("In defending this claim, Ticketmaster makes reference to the "shrink-wrap license" cases, where the packing on the outside of the CD stated that opening the package constitutes adherence to the license agreement (restricting republication) contained therein. This has been held to be enforceable. That is not the same as this case because the "shrink-wrap license agreement" is open and obvious and in fact hard to miss. Many web sites make you click on "agree" to the terms and conditions before going on, but Ticketmaster does not. Further, the terms and conditions are set forth so that the customer needs to scroll down the home page to find and read them. Many customers instead are likely to proceed to the event page of interest rather than reading the "small print." It cannot be said that merely putting the terms and conditions in this fashion necessarily creates a contract with any one using the web site. The motion is granted with leave to amend in case there are facts showing Tickets' knowledge of them plus facts showing implied agreement to them.").

⁶⁴ Frank C. Gomez, *Misappropriation: Washington Post v. Total News, Inc.*, 13 Berkeley Tech. L.J. 21, 22 1998.

⁶⁵ See *Washington Post Co. v. Total News, Inc.*, 97 Civ. 1190 (S.D.N.Y., complaint filed Feb. 20, 1997) (under a settlement agreement, Total News agreed to remove its frames, but retained the right to link to the plaintiff's news content). See, *Id.*

⁶⁶ "Search engines look for keywords in places such as domain names, actual text on the web page, and metatags. Metatags are HTML code intended to describe the contents of the web site.

There are different types of metatags, but those of principal concern to us are the "description" and "keyword" metatags. The description metatags are intended to describe the web site; the keyword metatags, at least in theory, contain keywords relating to the contents of the web site. The more often a term appears in the metatags and in the text of the web page, the more likely it is that the web page will be "hit" in a search for that keyword and the higher on the list of "hits" the web page will appear." *Brookfield Communications, Inc. v. West Coast Entertainment Corp.*, 174 F.3d 1036, 1045 (9th Cir. 1999).

⁶⁷ *Mattel, Inc. v. Internet Dimensions, Inc.*, 2000 U.S. Dist. LEXIS 9747; 55 U.S.P.Q.2D (BNA) 1620 (S.D.N.Y. 2000).

⁶⁸ See, 15 U.S.C.A. §1125(a), (d) (2000).

⁶⁹ *Playboy Enterprises Inc. v. Excite Inc.* SA CV 99-320, June 24, 1999 (C.D. Cal. 1999).

⁷⁰ See, G. Peter Albert, Jr., *It Started With Domain Names*, BNA (September 25, 2000).

⁷¹ *Id.*

⁷² <<http://b2b.abacus-direct.com/>> (visited September 25, 2000).

⁷³ <http://www.doubleclick.net/us/corporate/privacy/non-identify.asp?asp_object_1=&> visited (September 25, 2000).

DoubleClick collects the following types of non-personally-identifiable information about users who are served ads via DoubleClick technology:

Your IP address (a unique number assigned to every computer on the Internet). Information which DoubleClick can infer from the IP address includes the user's geographic location, company, and type and size of organization. Your domain type (i.e., .com, .net, or .edu.). Standard information included with every communication sent on the Internet. Information which DoubleClick can infer from this standard information includes your browser version and type (i.e., Netscape or Internet Explorer), operating system (i.e., windows or DOS), browser language (i.e., Java or Unix), service provider (i.e., MindSpring or AOL), your local time, etc. How you utilize the pages you visit within a DoubleClick client's site (e.g. which pages you view). On occasion, affiliated advertisers or Web publishers may provide DoubleClick with non-personally-identifiable demographic information so that you may receive ads that more closely match your interests. This information is afforded the same stringent privacy protections as the DoubleClick-collected non-personally-identifiable data.

⁷⁴ <http://www.doubleclick.net/us/corporate/privacy/default.asp?asp_object_1=&> (visited September 25, 2000, italics in the original).

⁷⁵ *Id.*

⁷⁶ *Id.*

⁷⁷ Federal Trade Commission, *Privacy Online: A Report to Congress* <[http://www.ftc.gov/reports/privacy3/history.htm#The Federal Trade Commission's Approach to Online Privacy](http://www.ftc.gov/reports/privacy3/history.htm#The%20Federal%20Trade%20Commission's%20Approach%20to%20Online%20Privacy)> (internal footnotes omitted) (visited April 30,

2000).

⁷⁸ E.g., *McVeigh v. Cohen*, 983 F. Supp. 215 (D.D.C. 1998) (AOL improperly disclosed personal information regarding Mr. McVeigh to the Navy which it then used in a discharge hearing resulting from his sexual orientation).

⁷⁹ Other state and federal laws may also limit disclosure of personal data. See, e.g., Family Educational Rights and Privacy Act of 1974 20 U.S.C.S. § 1232g (2000).

⁸⁰ Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, §1302(6), 1999 U.S.C.C.A.N. (112 Stat. 2681-728), 833, 15 U.S.C.A. § 6501 (1999).

⁸¹ < <http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm>>. See, *Id.*

⁸² "The Children's Online Privacy Protection Act and Rule apply to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The Act and Rule also cover other types of information - for example, hobbies, interests and information collected through cookies or other types of tracking mechanisms - when they are tied to individually identifiable information." *Id.*

⁸³ Gramm-Leach-Bliley Act, 106 P.L. 102; 113 Stat. 1338 (1999), codified at 15 U.S.C.S. §6801 (2000).

⁸⁴ 15 U.S.C.S. §6802(b) (2000). To opt out, the statute requires the following:

- (A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 504, that such information may be disclosed to such third party;
- (B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and
- (C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.

⁸⁵ 15 U.S.C.S. §6803 (2000).

⁸⁶ Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191).

⁸⁷ The Personal Information Protection and Electronic Documents Act (received Royal Assent April 13, 2000) < http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/90052b-1E.html>.

⁸⁸ <<http://www.ita.doc.gov/KPIFrameset.html>>.

⁸⁹ Christopher Paul Boam, *When Cyberspace Meets Main Street: A Primer for Internet Business Modeling in an Evolving Legal Environment*, 22 *Hastings Comm. & Ent. L.J.* 97, 121 (1999).

⁹⁰ *Id.*

⁹¹ < http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/90052b-1E.html>.

⁹² <<http://www.ita.doc.gov/KPIFrameset.html>>.

⁹³ <<http://www.ftc.gov/reports/privacy3/fairinfo.htm#Fair>

Information Practice Principles>.

⁹⁴ <<http://www.bbbonline.org>>.

⁹⁵ <<http://www.esrb.org/privacy/>>.

⁹⁶ <<http://www.truste.org>>.

⁹⁷ <<http://www.the-dma.org/topframe/index7.html>>.

⁹⁸ See generally, The Privacy Alliance <<http://www.privacyalliance.org/>>.

⁹⁹ In Re GeoCities, No. C-3850, <<http://www.ftc.gov/os/1999/9902/9823015cmp.htm>>.

¹⁰⁰ *Id.*

¹⁰¹ How to Comply With The Children's Online Privacy Protection Rule, November 1999, <<http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm>>.

¹⁰² FTC announces settlement against Internet toy retailer in privacy case, Fox Marketwire, July 21, 2000. See also, *Toysmart Bankruptcy Raises Novel Privacy Enforcement Issues*, Privacy In Focus/August 2000 published by Wiley, Rein & Fielding, legal counsel to TRUSTe.

¹⁰³ Electronic Signature in Global and National Commerce Act (Pub. L. No. 106-229) (2000).

¹⁰⁴ *Id.* at §101.

¹⁰⁵ National Conference of Commissioners on Uniform State Laws, Uniform Computer Information Transactions Act, Approved Draft July 1999 ("UCITA").

¹⁰⁶ *Id.* at §103.

¹⁰⁷ *Id.* at §103(d).

¹⁰⁸ See generally, <<http://badsoftware.com>>.

¹⁰⁹ Proposed 45 C.F.R. Part 142, Fed. Reg. 63-155 (August 12, 1998).

¹¹⁰ The exact method of holding meetings on line may vary by state. For example, see Cal. Corp. Code §5211 (Deerings 2000) (effective until January 1, 2003). The full text provides, in relevant part:

- (A) Each member participating in the meeting can communicate with all of the other members concurrently.
- (B) Each member is provided the means of participating in all matters before the board, including, without limitation, the capacity to propose, or to interpose an objection to, a specific action to be taken by the corporation.
- (C) The corporation adopts and implements some means of verifying both of the following:
 - (i) A person participating in the meeting is a director or other person entitled to participate in the board meeting.
 - (ii) All actions of, or votes by, the board are taken or cast only by the directors and not by persons who are not directors.

¹¹¹ *Id.*

¹¹² Securities Act Release No. 7856 (April 28, 2000) [65 FR 25843 (May 4, 2000)], at 25847 (the "2000 Release"); Securities Act Release No. 7233 (Oct. 6, 1995) [60 FR 53458 (Oct. 13, 1995)], at 53463 and 53465, Ex. 14, Ex. 15, Ex. 34, and Ex. 35.



GALLAGHER, CALLAHAN & GARTRELL
PROFESSIONAL ASSOCIATION
214 NORTH MAIN STREET
P. O. Box 1415
CONCORD, NEW HAMPSHIRE 03302-1415
www.gcglaw.com