



Online Business

©2010 eNotes.com, Inc. or its Licensors. Please see [copyright information](#) at the end of this document.

- [Background](#)
- [General Legal Issues Confronting Those Starting and Maintaining an Online Business](#)
- [Special State Law Considerations](#)
- [Additional Resources](#)
- [Websites](#)

Background

At the beginning of the Internet revolution, many proclaimed the World Wide Web would "change everything." Although it was impossible for the Internet to live up to the dizzying expectations and frenzied hype it garnered at its inception, its contribution to the business world cannot be understated. The exponential explosion of the Internet in the mid-1990s spawned an entirely new creature: the online business. Whether one calls the wired business world the dot-coms, the new economy, or e-biz, the Internet has definitely made it easier and relatively inexpensive for these businesses—big or small, new or old, local or international—to reach out to a larger population and customer base.

Because of the ease and economics of the Internet, thousands of brand-new ventures have been created exclusively online and "old economy" businesses have branched out to form online extensions of their "brick-and-mortar" bases. The following projections and facts illustrate this trend.

- Forrester Research projects that by 2003, business-to-consumer e-commerce revenues will total \$108 billion in the United States while business-to-business revenues will total \$1.3 trillion in the United States
- International Data Corp. (IDC) projects that business-to-business purchases through e-commerce will total \$4.3 trillion by 2005
- Jupiter Media projects that there will be 120 million online buyers in the United States by 2005, an increase from 65 million buyers in 2001
- Donaldson, Lufkin & Jenrette projects that by 2003, there will be 183 million worldwide online purchasers
- Keenan Vision projects that total online purchase revenues will equal \$1.4 trillion by 2004
- According to IDC, nearly 75% (5 million) of small businesses with PCs are on the Internet; while 2 million small firms maintain their own homepage and Website
- IDC found that 725,000 small companies were actively selling online by 2001

With the influx of thousands of online businesses, legal issues that entrepreneurs and seasoned business executives never had to consider, or could have even imagined, just a few years ago are now crucial to starting and maintaining an online business. Obscure or even nonexistent to the traditional business, issues such as domain names, customer privacy, links, metatags, and digital signatures have become an everyday concern. Further, entirely new rules, statutes, laws, and the fresh application of old laws have been created or modified to fit the landscape of the emerging online business world. At the local, state, federal, and international levels, laws are being debated and passed every day, and these new enactments are being tested regularly in courts of law. The online business must know these latest legal rules and the ramifications of starting and doing

business on the Net in order to survive and thrive.

General Legal Issues Confronting Those Starting and Maintaining an Online Business

Domain Names and Trademarks

One of the first tasks in starting an online business is to purchase a domain name, such as aol.com, amazon.com, and ebay.com. The top-level domain is the .com, .gov, .cc., .net, etc., of a web address. The second-level domain can be a company name, trademark, or industry buzzword. Obviously, no two domain names are the same. Over 33,000,000 domain names have already been registered, so finding a unique and unused name may be more difficult than appears at first glance.

The legal problems surrounding the registration of domain names most often involve trademark and service mark violations. TRADEMARKS and service marks are words, names, symbols, or devices used by businesses to identify their products and services. Even if one finds a domain name that has not yet been registered, that does not mean that it will not run afoul of trademark law. Typically, the first to register a domain name is entitled to keep it. However, if one registers a domain name that has been previously registered as a trademark, he or she may be in violation of the Anticybersquatting CONSUMER PROTECTION Act (ACPA), which created a new cause of action under Section 43(d) of the LANHAM ACT, 15 U.S.C. 1125(d). The ACPA contains penalties for bad-faith use of another's trademark of up to \$100,000 per domain-name violation. This law applies even if the trademark owner has not registered it as a domain name.

Similarly, if someone has used another person's trademark for a domain name, legal action may be necessary. All domain names registered after January 1, 2000 contain ICANN's (International Corporation for Assigned Names and Numbers) Uniform Domain Name Dispute Resolution Policy (UDNDRP), which requires all such disputes to be determined by an administrative panel. The only remedy under the UDNDRP for the [BAD FAITH](#) use of another's trademark is transfer of the domain name to the trademark owner. Even after such a determination, though, one may still seek [REDRESS](#) in a court of law.

Sound legal advice is for a new online business to protect its domain name by registering it as a trademark first. A trademark may be obtained electronically at the PATENT and Trademark Office web site using the Trademark Electronic Application System. Once individuals obtain trademarks, they may also then want to monitor the Internet for cybersquatters improperly using their trademarks. There are fee-based firms that will monitor usage of your trademark in the United States. Trademark owners may also avoid costs associated with hiring such a firm by doing manual searches for trademarks using search engines. [Whois.net](#) will find all domain names that contain the string of words a person's wishes to check and may also provide the registrar's name, address, email address, and other useful information that can be used to begin an investigation as to whether such entity is cybersquatting.

However, the holder of a trademark right is not automatically entitled to the same domain name that uses the trademark. In *Strick Corp. v. Strickland* (E.D.Pa. Aug. 27, 2001), 162 F.Supp.2d 372, Strick Corp., a provider of transportation equipment and trademark holder of the name, sued a provider of computer consulting services that had registered the domain name [Strick.com](#). Strick Corp. claimed there was blurring and dilution of trademark occurring when Internet searches using "Strick" as a search term encountered the alleged diluter's web page and concluded that the trademark holder had no Internet presence. The federal court found that the use of [Strick.com](#) by the computer consulting company did not dilute the trademark and did not violate the Lanham Act or state law. The court determined that any initial confusion that arose from the

defendant's use of the domain name was not substantial enough to be legally sufficient. The judge also found that there was not "dilution by blurring" because a reasonable consumer would not associate the two uses of the trademark in his or her own mind. The sensible practice to avoid an inevitable lawsuit for using another's trademark in a domain name is first either to hire an attorney to run a trademark search or check with the U. S. Patent and Trademark Office database at www.uspto.gov before registering the domain name.

Privacy Issues

Through their own analyses or the help of online advertising agencies, online businesses can track users' buying, what they look at, how long they look at it, what the referring site was, what other sites were visited, the time of day they browse, and where they live, not to mention the detailed information the browser supplies voluntarily through registration and purchases. Indeed, the browsing public knows the threat of websites gathering their personal information. PriceWaterhouseCoopers found that nearly 77% of those surveyed said that the disclosure of personal details was a barrier to purchasing online. Another 48% stated they do not shop online because they do not trust web retailers. Twenty-seven percent of Internet users surveyed by CyberDialogue said they had abandoned an online purchase because of privacy concerns regarding the abuse of personal data. This apprehension and mistrust have not gone unnoticed by lawmakers. As a result, online businesses must now pay careful attention to an array of privacy laws.

Several federal laws affect privacy issues for online businesses. The Federal Trade Commission (FTC) Act, 15 U.S.C. 41 et seq., has only limited effect on online businesses. The FTC's power under the FTC Act is generally to ensure that a website follows its own stated privacy policy. The FTC Act gives no power to the FTC to demand any specific privacy policy be followed or that any policy even be posted. The FTC does, however, use its wide-ranging power under Section 5 of the FTC Act to take action against "deceptive acts or practices." It should be noted, though, that the FTC Act provides no right of legal action for individual consumers wishing to obtain damages for privacy policy violations by a website.

The Children's Online Privacy Protection Act (COPPA), 15 U.S.C. 6501 et seq., enacted in 1998, applies only to web sites that target children under 12 years old as users or have actual knowledge that information is being collected from a child. COPPA requires that such a web site post privacy policies describing what personal information it collects and what it may do with such information. The law further requires that the online operator get prior "verifiable parental consent" before collecting, maintaining, or disclosing information about the child. The law also provides a "safe harbor" for those web sites that act in compliance with a self-regulatory program approved by the FTC. Any online business that may be marketing toward children must be aware of COPPA and its requirements.

The Electronic Communications Privacy Act of 1986 (ECPA), 18 USC 2510 et seq. and 2701 et seq., also has application to certain web site practices. The ECPA prohibits the interception or disclosure of electronic communications. Although the ECPA provides an exemption for those who are parties to a communication, a web site that considers collecting or distributing information obtained via emails to its site or through monitoring forum or chat-room services it provides should be wary of the prohibitions of the ECPA. Merely posting a privacy policy that explains that users of the service implicitly consent to collection and disclosure of their communications may not be enough. To be certain, web sites should obtain specific consent from those parties involved directly with the communications.

The Uniform Commercial Code and Online Business

Article Two of the **UNIFORM COMMERCIAL CODE** ([UCC](#)) applies to all contracts, both business-to-business and business-to-consumer, for the sale of goods, unless the parties agree to vary the terms of their agreement. Louisiana is the only state that has not adopted Article Two, and versions of Article Two vary from state to state. Further, unless otherwise agreed upon, if two parties are from countries that have

joined the United Nations Convention on the International Sale of Goods (UNCISG), the UNCISG may have control over the UCC with regard to their transaction. Four general provisions are particularly important to online businesses: the writing requirement, contract formation, warranties, and remedies.

The writing requirement of Article Two requires that for the sale of goods over \$500, there must be some writing sufficient to indicate a contract. For online businesses, it is likely sufficient for there to be an electronic record of the acceptance of the terms by the buyer or an indication of acceptance via email. A typed name on the email or the filling-in of the name on the online order is also likely to constitute sufficient signatures. (See UCC Section 1-201(39): "signed" includes any symbol that demonstrates the intention of a party. See also "Electronic and Digital Signatures" below.)

The requirement of contract formation requires that an offer can be accepted in any reasonable manner. An acceptance by e-mail is acceptable if the offer was by e-mail. If the offer was made by another medium, it is suggested that one first inquire if acceptance by e-mail is acceptable.

The [WARRANTY](#) requirements of Article Two provide that there is an express warranty, [IMPLIED WARRANTY](#) of merchantability, implied warranty of fitness for particular purpose, and implied warranty of title and noninfringement. Many online businesses limit these warranties through "clickwraps," which are a set of contract terms that an online customer accepts by clicking on an "accept" or similar button, usually on a separate screen. Online businesses should allow the consumer to agree to the limitations before completing the transaction. Under the remedies requirement of Article Two, buyers may obtain from sellers after a breach of contract certain remedies, including actual damages, incidental damages, and consequential damages. Many online sellers limit the buyer's remedy in the clickwraps to the damages of repair, refund, or replacement of the purchased goods. Consequential damages, however, may not be limited or excluded if "unconscionable."

Electronic and Digital Signatures

An electronic signature is generally any electronic data used to validate and authenticate the parties to a transaction. A digital signature, which is a form of an electronic signature, is a unique, encrypted code affixed to an electronic document or contract that authenticates the signor. The use of such electronic signatures allows parties to use the Internet to conduct transactions quickly and securely while reducing paperwork.

The most important federal legislation on electronic signatures is the Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 U.S.C. sec. 7001 et seq., which became effective on October 1, 2000. E-SIGN provides that a signature or contract may not be denied legal effect "solely because it is in electronic form," except as provided in the Act itself. See section 101(a)(1) and (2). An electronic signature is defined as any "electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or accepted by a person with the intent to sign the record." Although E-SIGN does not apply to all transactions and writings, it applies to "any transaction in or affecting interstate or foreign commerce." Because a "transaction" is defined as "an action or set of actions relating to the conduct of business, consumer, or commercial affairs site, and place it on the page." For example, an online businesses may use an HREF link to link to a manufacturer's web site or use an IMG link to insert images of a product from the manufacturer's web site onto its own web site. Generally, there are no laws against HREF linking to another web page because the HREF link merely contains the coded information of the target's address. Because the code is pure information, no [COPYRIGHT](#) or any other intellectual property laws provide protection. However, online businesses should keep in mind several issues related to the practice of HREF and IMG linking.

When one incorporates content from another's page via an unauthorized IMG link, there is no direct copyright [INFRINGEMENT](#) by the creator of the link because the image is not copied. As explained above, the visiting browser has provided the user's browser with instructions to retrieve the image. It is actually only the web viewer who has copied the image. However, the creator of the link may still be liable under copyright law for

contributory infringement, which occurs when one knowingly makes an infringement possible. Further, it is possible that a web site could be liable for copyright infringement if IMG links use several copyrighted images to form an entirely new "derivative work" on its web site. Generally, it is considered proper protocol for a web site to get permission from a copyright owner before placing an IMG link on its own web site. Web site operators should also be certain to properly attribute works or images that may be reached or created with links and not misrepresent the ownership of the work. Online businesses must also be careful not to infringe on the trademarks of others. If a web site falsely leads the user to believe that the web site is affiliated, approved, or sponsored by the trademark owner, it could be liable for trademark infringement.

A link to another's page or image may also be potentially defamatory if it communicates a false and damaging statement about a person or entity. Further, even if a statement alone is not defamatory, it could become defamatory by providing a link within, before, or after the statement that directs the viewer to further information or identification.

Framing is a technique that puts a frame, or several frames, on a webpage that stays in place even when the viewer links to another site. The practical purpose of a frame is to be able to see information from several different sources on one display. However, because the original web site's logo, color scheme, design, or other characteristics may still be on the frame(s), viewers may be led to believe that they are still on the original web site and seeing content created by the original web site. This situation creates a problem for some situations, such as when a web site that is being framed by another web site does not want to be associated with the framing web site but appears to be so because of the frame. Thus, framing can raise the same issues as HREF and IMG linking. Although the legality of framing is not certain, web site operators should appreciate the potential legal liability of linking other's pages into frames without permission.

It should also be noted that some consider "deeplinking" to be web [PIRACY](#) if it is done on a large scale. Deep-linking is when a link is provided to a specific web page within another's web site and not merely to the homepage. Some web operators are angered by this practice because the link takes the viewer directly to the page and bypasses its homepage, eliminating the ability of the homepage to build brand recognition, to supply important information, and to serve advertising functions. However, there is no law against deep-linking, and it is an extremely common practice that most see as not problematic, as long as it is not deceptive. Deep-linking has also been found legal by at least one federal court. See *Ticketmaster Corp. V. [Tickets.Com](#), Inc.* (C.D.Cal. Mar. 27, 2000), No. CV-99-7654 (use of deep links to [Ticketmaster.com](#) did not violate copyright law because there is no copying involved, and the online ticket consumer is openly and obviously transferred to Ticketmaster's website; deep-linking also did not constitute [UNFAIR COMPETITION](#) because a disclaimer negated any confusion as to the true source of the ticket purchase).

E-mailing and "Spamming"

Many online businesses use e-mail as an advertising and marketing tool because of the potentially vast reach it has and the very inexpensive cost of sending e-mail. Some e-mail used for these purposes is targeted to a specific group of consumers who have requested such useful information. However, an ever-growing amount of commercial e-mail is unsolicited, bulk e-mail sent en masse. This latter type is often referred to as "spam." One commentator from [Spam.abuse.net](#) cites several reasons for the maligning of spam: the receiver pays more in aggravation than the sender does in time and money; as spam grows, it will crowd out mailboxes and render them unusable; many spammers send their junk e-mail via innocent intermediate systems to avoid filters; spam clogs providers' systems; spam messages are nearly exclusively worthless, deceptive, and partially or totally [FRAUDULENT](#); and some spam may be illegal.

While the annoyance of having an e-mail inbox filled to the virtual brim with these clogging and often useless solicitations has raised the ire of millions of e-mail users, it apparently has not touched the federal legislators enough for them to enact federal laws directly pertaining to it. Several Federal laws were pending at the time

of this writing in the 107th Congress, including the Anti-Spamming Act of 2001 (H.R. 718), Anti-Spamming Act of 2001 (H.R. 1017), Controlling the ASSAULT of Non-Solicited PORNOGRAPHY and Marketing (CAN SPAM) Act of 2001 (S. 630), Netizens Protection Act of 2001 (H.R. 3146), Unsolicited Commercial Electronic Mail Act of 2001 (H.R. 95), and Wireless Telephone Spam Protection Act (H.R. 113). However, as discussed below, many states have enacted legislation regulating unsolicited e-mails.

Therefore, although spamming is generally not in violation of any federal laws at this time, it may soon be and is considered an extremely poor, if not unethical and despicable, business practice. Any business that wishes to use targeted, solicited e-mail as an advertising tool should be careful to steer clear of sending bulk, unsolicited advertising to unwitting recipients because doing so may tarnish its reputation and run afoul of the many state laws on the subject, as discussed below.

Metatags

Metatags are invisible HTML programming codes that contain commands to search engine programs that index web pages. In normal practice they provide keywords relating to the content of the page so a search engine will display the page in its results when a user inserts them as search terms. Thus, by successfully using metatags, a web operator can increase the frequency a search engine will index a site.

However, website operators quickly figured out that by using metatags unrelated to their own content or metatags that contained a competitor's company or product name, they could increase their own traffic. Even though metatags are not visible on the page (they may be viewed by clicking "View" and then "Source"), this deceptive practice has been the basis for numerous lawsuits brought by individuals, companies, and web sites asserting that unrelated websites are illegally using metatags.

In general, courts have enjoined the use of trademarks in a non-owner's metatag when the parties were competitors or when the use of the trademark in a metatag was used to divert business to the site for profit. The key factor courts consider in determining whether a website has infringed on another's trademark through its use in a metatag seems to be whether there could be consumer confusion. See, e.g., *Playboy Enterprises, Inc. v. Calvin Designer Label* (N.D. Cal. 1997), 985 F.Supp. 1220 (web site may not use "Playboy" and "Playmate" in metatags on web site because web site was attempting to profit by confusing consumers and diverting business to the site).

The improper use of metatags by online businesses can also raise issues of unfair competition or trademark dilution. Unfair competition prohibits a company from deceptively claiming a connection with or endorsement from another. Trademark dilution occurs when one uses the trademark of another in such a manner that it blurs the significance of the mark or when using a similar mark in an objectionable manner tarnishes the meaning of the mark. For an example, see *Ken Roberts Co. v. Go-To.com* (N.D. Cal. May 10, 2000), No. C99-4775-THE (competitor's use of plaintiff's name in metatags interfered with plaintiff's prospective economic advantage by knowingly diverting plaintiff's current or potential customers from plaintiff's website to competitor's, constituting unfair competition and trademark dilution).

However, businesses may use another company's trademark under certain circumstances. An online business may generally use another company's trademark as a metatag on a webpage with a comparison advertisement. Of course, an online business would also be permitted to use another's trademark as a metatag if it was a distributor of the trademark owner's product and had a license from the manufacturer to use the trademark. Courts have also refused to find trademark infringement when the metatag is used to indicate content that provides a description of goods or services of the mark owner or their geographic origin. Such are permitted as a "fair use" of a trademark. See, e.g., *Playboy Enterprises v. Welles* (S.D. Cal. 1998), 7 F.Supp.2d 1098, *aff'd* without opinion, (9th Cir. 1998), 162 F.3d 1169 (it was "fair use" for former Playboy Playmate of the Year to use "playboy" and "playmate" in metatags of her website because they were key words that identified

her source of recognition to the public). However, outside these limited circumstances, online businesses should not use a trademark as a metatag without permission, particularly if the trademark belongs to a competitor. Many companies and trademark owners regularly search the Internet for metatag trademark violations, and such searches are simple to conduct.

Internet Sales Tax

On November 28, 2001, President George W. Bush signed H.R. 1552, the Internet Tax Non-Discrimination Act. The Act extends the moratorium on new, special, and discriminatory Internet taxes and Internet access taxes originally enacted in October 1998 as part of the Internet Tax Freedom Act (47 U.S.C. 151). The new legislation extends through November 1, 2003.

Special State Law Considerations

Electronic and Digital Signatures and E-SIGN

As the Internet grew in popularity, many states quickly moved to enact legislation pertaining to electronic and digital signatures. When E-SIGN took effect in October 2000, the question that then arose was whether E-SIGN preempted such state laws on the subject. Preliminarily, it is clear that E-SIGN preempts state laws that conflict with or frustrate E-SIGN's basic policy, as spelled out in Section 101(a)(1) and (2), that electronic signatures and records cannot be denied legal effect solely because they are in electronic form. However, E-SIGN clearly does not preclude other laws that do not conflict with the validation principles contained in Section 101 of E-SIGN.

In 1999, to combat problems that could arise when parties from two jurisdictions entered into an electronic transaction, the National Conference of Commissioners on Uniform State Laws recommended the Uniform Electronic Transactions Act (UETA) for enactment in all states. UETA recognized electronically-based transactions and records as the "functional equivalent" of paper transactions where the parties agreed to use electronics. In formulating E-SIGN, the drafters clearly took UETA into account. Indeed, Section 102 of E-SIGN specifically recognizes UETA and acknowledges that individual states, through the enactment of UETA, can modify, limit, or supersede the effect of the validation provisions in Section 101 of E-SIGN without federal preemption. However, the state must enact UETA in its "pure" form (without modification) and express its intention to supersede E-SIGN. Still, because UETA only applies when the parties agree to use electronics, E-SIGN would apply in cases where there was no mutual agreement. Thus, these "opt-out" provisions provide for uniformity of state law, even though the provisions in UETA may differ from E-SIGN. E-SIGN also provides that a state may modify, limit, or supersede the validation terms of Section 101 if the state law specifies the alternative procedures for use of electronic signatures or records and those procedures are consistent with E-SIGN and do not validate only a particular type of technology. Therefore, online businesses should note that, although E-SIGN must be followed, individual states could enact additional laws affecting electronic signatures.

E-mailing and "Spamming"

Although Congress has failed to enact any legislation specifically regulating unsolicited, bulk, commercial e-mailing, many laws have been passed at the state level. In July 1997, Nevada became the first state to enact an anti-spam law. The following states have also passed spam laws: California, Colorado, Connecticut, Delaware, Idaho, Illinois, Iowa, Louisiana, Missouri, North Carolina, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Virginia, Washington, and West Virginia. The statutes in these states are variously worded and provide a wide range of protection against unsolicited, commercial e-mail. The anti-spam laws in the

following states require "opt-out" instructions, and most also require that the opt-out requests be honored: California, Colorado, Idaho, Iowa, Missouri, Nevada, Rhode Island, and Tennessee. The anti-spam legislation in the following states applies to e-mails that are delivered to a resident of that state via a provider's facilities or equipment located in that state: California, Colorado, Connecticut, Illinois, Iowa, Oklahoma, Tennessee, and Virginia. The anti-spam legislation in Delaware and Rhode Island applies to e-mails originating outside the state if the recipient is located in that state and the sender is or should have been reasonably aware that the recipient is a resident of that state. North Carolina's law applies to e-mails sent into or within the state. In Washington and West Virginia, the anti-spam laws apply if a message is sent from within the state or if the sender knows that the recipient is a resident of that state. The following states require unsolicited, bulk, commercial e-mail to have certain labels in the subject line, such as "ADV" (advertisement) or "ADLT" (adult): California, Colorado, Nevada, Pennsylvania, and Tennessee.

Internet Sales Tax

In *Quill Corp. v. Heitkamp* (1992), 504 U.S. 298, the United States Supreme Court found that states cannot require out-of-state retailers to collect sales taxes unless they have a physical presence, or nexus, within the state. Thus, online sellers do not have the power to collect tax on Internet sales to customers in other states, as such taxes are considered an interference with interstate commerce. However, if an online business is selling **TANGIBLE PERSONAL PROPERTY**, it is likely required to collect [SALES TAX](#) in the state where its inventory is located or where it has a "bricks-and-mortar" store. Also, although no state may require out-of-state e-businesses to collect and remit taxes on sales to its residents, states may still require residents to remit such taxes themselves. Such a tax is referred to as a "use" tax. The difficulty is that it is nearly impossible for states to enforce such laws, so states have no choice but to rely on the honor system in collecting use taxes.

States have complained about their lack of ability to collect sales tax for Internet purchases, citing lost taxes as high as \$13 billion for 2001. However, exclusively online e-tailers argue that if they are required to collect sales taxes and pay them to the proper taxing authorities, it will be extremely difficult to comply with nearly 8,000 state and local taxing jurisdictions, each with different rates and rules. One proposal that the National Governors' Association (NGA) has countered with is for the establishment of a "trusted third party," which would calculate and collect for the online businesses the appropriate local and state sales taxes. However, the NGA's [LOBBYING](#) efforts to allow states to tax such online purchases from remote sellers has yet been to no avail, as indicated by the passage of the Internet Tax Non-Discrimination Act.

Additional Resources

101 Things You Need to Know About Internet Law. Bick, Jonathan, Three Rivers Press, 2000.

The E-Business (R)Evolution: Living and Working in an Interconnected World. Amor, Daniel, Prentice Hall, 2000.

Internet Law and Business Handbook: A Practical Guide. Brinson, J. Dianne, and Mark F. Radcliffe, Ladera Press, 2000.

Websites

[About.com](#)

URL: <http://law.about.com/cs/cyberspacelaw/>

Alan Gahtan's Cyberlaw Encyclopedia

URL: <http://www.gahtan.com/cyberlaw/>

Bitlaw

URL: <http://www.bitlaw.com/>

Findlaw for Legal Professionals

URL: www.findlaw.com/01topics/10cyberspace/index.html

Gigalaw

URL: www.gigalaw.com

The Internet Law Journal

URL: <http://www.tilj.com>

The John Marshall Law School

URL: <http://www.jmls.edu/cyber/index/index.html>

Megalaw

URL: <http://www.megalaw.com/top/internet.php3>

Nolo Law for All

URL: www.nolo.com

Spam Laws

URL: <http://www.spamlaws.com/>

Copyright Notice

©2010 eNotes.com, Inc.

ALL RIGHTS RESERVED.

No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means graphic, electronic, or mechanical, including photocopying, recording, taping, Web distribution or information storage retrieval systems without the written permission of the publisher.

For complete copyright information, please see the online version of this work:

<http://www.enotes.com/everyday-law-encyclopedia>