

**AMERICAN BAR ASSOCIATION  
SECTION OF BUSINESS LAW  
INTERNATIONAL BUSINESS LAW COMMITTEE**

---

**INTERNATIONAL TRADE LAW FOR BUSINESS LAWYERS  
40 PRACTICE TIPS IN 90 MINUTES**

---

**April 15, 1999  
San Francisco, California**

---

**TIPS FOR COMPUTER AND INTERNET RELATED TRANSACTIONS**

**By**

**Thomas M. Pitegoff  
White Plains, New York  
[www.pitlaw.com](http://www.pitlaw.com)**

## TIPS FOR COMPUTER AND INTERNET RELATED TRANSACTIONS

- 1. Be sure you own the intellectual property rights you intend to own.*
- 2. Be mindful of U.S. laws against the export of encryption software.*
- 3. Protect your source code.*
- 4. Consider global protection of brand names.*
- 5. Consider whether your Web “storefront” is a franchise.*
- 6. Consider the Web in your grant of a marketing territory.*
- 7. Consider developing and hosting Web sites for your licensees, distributors or franchisees.*
- 8. Develop a written policy for the use of your computer network or Web site.*
- 9. Present a clear policy on how you will use personal information collected on your Web site.*
- 10. Pay attention to ethical rules on the use of the Web by lawyers and law firms.*

***1. Be sure you own the intellectual property rights you intend to own.***

Ownership of intellectual property rights is fundamental to a technology venture, yet the problem of confused ownership frequently arises in the real world. Picture this scenario, based on my own experience. The owner of a small software company in the U.S. engaged a colleague in England to assist in programming a software application that had a vast prospective market in England. He paid the English programmer for his time spent on the project. Just when the software was ready to be demonstrated to a large prospective customer in London, the programmer demanded to own a substantial interest in the company. How could he do this? The answer is simple. He created the software. There was no written agreement that the intellectual property rights were to be owned by the company, and there was no agreement to assign this property to the software company. As such, the company did not own more than a single copy of the program and could not sell it to others.

Under the copyright laws of the U.S. and of most countries, the creator of a work is the owner, with certain narrow exceptions, including employees creating copyrightable works as part of their jobs. In order for the company to own the intellectual property rights in the software in the above example, the parties would have to enter into a written agreement stating clearly that the work is “for hire” and the company owns it, and that to the extent the work may not qualify as being “for hire”, the programmer will assign the work to the company. It makes no difference that the company had the idea for the program, or gave the programmer a description of how the program should function, or paid the programmer by the hour.

Another example from my own practice occurred when a large public company, under contract with a small consulting company, decided to have the consulting company write a computer program to be used by certain managers at the large company to facilitate a project that the consulting company had been working on for some time. The parties had a written contract dealing with the overall work; but the contract was silent on the question of the ownership of copyrights in the computer program. The large company thought it would own all the rights in the software, since it was paying for its development. The consulting company, on the other hand, intended to market the software to other large companies without the data it was collecting for the large company. Because the agreement was not clear on the question of who owned the copyrights, the issue became a sticking point and it took several months to negotiate an acceptable solution.

In any software development agreement with an independent programmer, don't forget to include a license to any preexisting or third party components that the programmer may use. Programmers often use bits and pieces of code they own or that may be owned by a third party. The use of this code in the finished product should not inhibit your company's use or sale of the finished product.

The question of ownership of intellectual property rights also arises when a company engages an outside party to create the company's Web site, to create its advertising or to write manuals or other materials.

## ***2. Be mindful of U.S. laws against the export of encryption software.***

The use of encryption software to protect the confidentiality of data is not regulated in the U.S. However, the export of encryption products is regulated. Since 1996, the U.S. Commerce Department has had responsibility for export controls of all encryption products, except those specifically designed or adapted for military application. Approvals for the export of strong encryption software generally require a special export license. Before an exporter can obtain this license, it must agree to designate a key escrow agent and key escrow recovery and security arrangements satisfactory to the Commerce Department's Bureau of Export Control.

The export of encryption software to Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan is prohibited.

In 1998, the Commerce Department eliminated restrictions on exports of most encryption software to certain companies headquartered in 44 countries and their branches worldwide. The easing of these restrictions applies to banks and other financial institutions; insurance, health and medical companies; and to exports of client-server applications and applications tailored to online transactions to online merchants.

Restrictions still exist, however. Notably, for example, the export of mass market encryption software and hardware continues to be restricted.

Whenever your company is engaging another party to do any type of programming, it is a good idea to include a provision in the contract specifically requiring the programmer to comply with all applicable laws, including U.S. export requirements.

### ***3. Protect your source code.***

If your company is creating software for any purpose, be sure that your programmer delivers documented source code and that you maintain this source code and backup copies in safe, secure locations. If the programmer becomes unavailable to work on future versions or upgrades, the source code should be clear enough so that another programmer can readily understand it and work with it.

If the software has commercial value, you should jealously guard its source code from disclosure. Only those with need should have access to it. Anyone who sees it should first sign a confidentiality agreement.

If your company does not own the intellectual property rights to the software, consider entering into a source code escrow agreement. Several companies exist solely for the purpose of acting as source code escrow agents. A source code escrow agreement can give your company access to the source code in the event of bankruptcy or a material breach by the software company.

Finally, in drafting the contract with the creator of the software, be sure that such creator is under a contractual duty not to use the software, or at a minimum, not to use it for a competing purpose.

Confidentiality clauses are very important in both domestic and international technology agreements. Not all countries have laws that allow for the protection of trade secrets. Accordingly, a strong confidentiality clause is essential.

While damages may be recoverable for the breach of a confidentiality clause, injunctions may not be available in some countries. Since there is very little that one can do in some countries after a trade secret is wrongfully disclosed, the best practical means of protection might be not to make disclosure of confidential information at all. The second best non-legal means of protection is to select honorable contract partners.

An increasingly popular way to protect both software and business methods is patent protection. If a patent can be obtained, then it matters far less whether the valuable secret information is disclosed.

#### ***4. Consider global protection of brand names.***

If you have plans to sell your product or service in more than one country, you should consider protecting your trademarks abroad at the earliest possible date. Unless you do so, you may find that your company's mark infringes the rights of another trademark owner in one or more countries. You will then be faced with the prospect of either litigating your rights, having to purchase the mark from the foreign owner or selling your goods or services under a different mark. Your company may have no choice but to use different product names in different countries.

Today, the use of the Internet makes international trademark protection a necessity. Before you sell a product or service under a new brand name, you should engage a search company to do a full trademark search to be sure that your use of the trademark will not infringe the rights of anyone else. If the search results are appropriate and the mark is otherwise registrable, it may be advisable to seek federal trademark registration. You may also want to apply for registration in the countries in which you are most likely to sell goods or services.

Presumably, before initiating any serious discussion with a potential business partner abroad, your company's marketing department will make a determination of whether the same marks used for the U.S. business will work in the foreign market. The mark may have an entirely different connotation in the destination country. If the mark would work from a marketing point of view, it may nevertheless not be available in the destination country. For many companies, this means that the same product or service may have to be sold under a different mark in different countries.

Other special considerations also arise in the international context. In some countries, service marks may not be protectable at all. Not all countries allow for injunctive relief to stop trademark infringement. The relief that is available will affect the way a license agreement is drafted, the forum selected for dispute resolution, and other provisions of the agreement.

An important component of the trademark issue is the question of domain name protection. Trademark searches today include searches of domain names. Companies are increasingly and aggressively acquiring domain names to prevent others from setting up Web sites that compete, satirize or criticize your company or otherwise make it appear in a bad light. Trademark search companies now offer global domain name registration packages.

Any Web-based business will have to face these issues sooner in its business life than other types of businesses.

## ***5. Consider whether your Web “storefront” is a franchise.***

With the proliferation of E-commerce, franchise laws in the U.S. and abroad can easily entangle an unwary cyberbusiness.

The starting point for any discussion of what constitutes a franchise is an agreement under which one company enables another person or entity, for a fee, to do business under a prescribed business format and a specific trademark. On the Internet, a franchisor can take the form of a Web shopping mall, a content provider, a travel or real estate service or Web hosting service, among others. In short, any content provider or hosting service that offers a package that puts the customer in business might be a franchise.

The Federal Trade Commission trade regulation rule on franchising (the "FTC Rule") requires franchisors to deliver an offering circular to each prospective franchisee before the prospective franchisee signs an agreement or pays the franchisor. Roughly one-third of the states in the U.S. have laws similar to the FTC Rule, requiring franchisors to make extensive disclosures to prospective franchisees before franchises are offered or sold. Many of these states also require registration of the offer. Some of these laws may apply in international transactions.

In addition to franchise laws in the U.S., an increasing number of countries have enacted franchise sales laws. Some of these laws are intended to protect franchisees and are modeled, more or less, after the U.S. franchise disclosure laws. In other cases, particularly formerly controlled economies such as Russia and China, the motivation for enacting franchise laws seems to be to legitimize franchising as a way of doing business. Other countries with laws that may specifically cover franchises include Australia, Brazil, Canada, France, Indonesia, Italy, Japan, Malaysia, Mexico, South Africa, South Korea and Spain.

Some Web content providers and hosting services want to avoid the franchise laws. Franchise compliance adds to the cost of doing business. At the outset, it requires preparation of a franchise agreement, audited financial statements, a detailed offering circular, and registration in several states. As an ongoing matter, a franchisor must integrate the franchise disclosure requirements into its method of selling franchises. Compliance requires timely delivery of an offering circular to all prospective franchisees, timely amendments of offering circulars and renewals of registrations, and annual audited financials. Noncompliance can lead to administrative actions and private lawsuits; with resulting penalties, damages, rescission and other remedies.

On the other hand, if a client's planned business has the appearance of a franchise, it is often to the client's advantage to accept that fact and to take the approach of a full-fledged franchisor. Compliance in this manner provides a safe harbor, meaning that the client need not be concerned about being an unwitting franchisor that has failed to disclose. It allows the client to act more freely with potential licensees or customers.

## ***6. Consider the Web in your grant of a marketing territory.***

In many distribution systems, licensees, distributors and franchisees are using the Web to sell or advertise their products or services. Because of the lack of geographic borders in Cyberspace, use of the Web by licensees, distributors and franchisees can create havoc for a licensor, manufacturer or franchisor.

Companies are formulating various approaches to using the Web. In some cases, companies will allow their distributors to set up their own sites and compete with one another in Cyberspace. In others, the licensor, manufacturer or franchisor is setting up sites for its licensees or distributors and limiting their ability to set up their own sites. In still other cases, the licensor, manufacturer or franchisor may reserve to itself the right to advertise and sell through the Internet.

Whatever approach a company takes should be made clear in its contracts with its licensees, distributors or franchisees. This works for new contracts, but it may raise a problem for companies that have existing contracts. The existing contracts may not prohibit or limit the licensees, distributors and franchisees from using the Internet in their businesses. In that case, a company may want to seek ways to induce its licensees, distributors or franchisees to renegotiate their contracts, or it may wait until contracts come up for renewal before renegotiating them.

In those cases in which a company allows its licensees, distributors or franchisees to set up their own Web sites, it is a good idea to monitor the sites and to impose certain requirements to reduce the likelihood of confusion and to limit the company's liability. Your company might require that these sites contain disclaimers and limitations of liability, that they specify the geographic areas in which they do business; and the fact that they are independent companies. It would also be a good idea to have written agreements with the licensees, distributors or franchisees that outline your company's requirements for their Web sites, including an obligation to comply with all applicable laws and to indemnify your company for a failure to do so.

## ***7. Consider developing and hosting Web sites for your licensees, distributors or franchisees.***

Rather than having your licensees, distributors or franchisees post possibly conflicting and confusing sites on the Web, consider acting as the Web developer and hosting service for them. By doing so, your company can exercise a great deal of control over the quality and content of these sites. You can be sure that the pages contain the appropriate copyright notices, disclaimers and explanations of the distinctions between your company and its licensees. From the point of view of the licensees, distributors or franchisees (collectively, the “licensee”), your company may offer better terms and make it easier for them to launch and maintain a Web site than by doing so with others or by themselves.

In addition to designing, programming and posting Web pages for your licensees, your company can establish private Web areas and private newsgroups or bulletin boards that can be accessed only by your company and your licensees through the use of passwords. This would enable your company to provide additional support to its licensees by posting support documents, calendars, company directories and other information useful to your licensees. Private newsgroups allow for a more dynamic means of communication among licensees and between licensees and your company.

Web development and hosting services raise business and legal issues that are best dealt with in written agreements between the licensee and licensor. Among other things, the licensor will want to disclaim and limit the licensor’s liability for infringement based on materials supplied by the licensee, and for consequential damages, downtime, security breaches and more.

A central feature of any such agreement should be a code of conduct for postings and other transmissions on the Web, in newsgroups and by e-mail. Licensors will want licensees to indemnify them for breaches of this code of conduct. This code might include obligations with respect to defamation, obscenity, infringement, confidential information, viruses and Trojan horses, offensive or abusive language, uses not in furtherance of the licensed business, and unlawful activities. The code of conduct should also prohibit anticompetitive agreements, such as price fixing agreements, boycotts of particular suppliers or agreements to allocate markets.

Even with a code of conduct and an agreement by the licensees to adhere to this code and to indemnify the licensor, the licensor should consider closely monitoring the Internet activities of its licensees and its own employees to make sure that no one is using the Internet to conduct unlawful activities that might hurt the licensor, licensees or their customers.

## ***8. Develop a written policy for the use of your computer network or Web site.***

The posting of a Web site instantly turns any business into an international business. While Cyberspace is inherently international, laws are geographically based. This leads to a myriad of questions regarding jurisdiction and conflicts of laws.

One way to avoid the application of undesirable laws is to develop a written policy for the use of your Web site that restricts E-commerce sales to certain jurisdictions. An online posting of the policy limiting sales to specific geographic areas or excluding specific areas can be helpful in avoiding the jurisdiction of the courts in the excluded areas. Your company should then follow its own policies so that it does not “purposely avail” itself of an unfriendly jurisdiction.

It is also a good idea to develop a written policy for the use of your computer network by employees and others. Employees should know that they can have no expectation that their e-mail will be private. They should be admonished against transmitting any data that might infringe or violate the property rights of others, including (a) any text, images, graphics, video clip, audio clip or software protected by copyright or patent law; (b) trade secrets or other confidential proprietary information; and (c) trademarks or service marks.

These policies might include prohibitions against the use of the network for personal use or to transmit anything that (a) constitutes or solicits any illegal activity, such as gambling and anticompetitive activities, such as price fixing, boycotting of suppliers or allocating markets, or any violation of the securities laws; (b) is discriminatory, such as referring in a negative manner to an individual’s race, age, disability, religion, national origin, physical attributes or sexual preference; (c) is abusive, profane, harassing, sexually harassing, intimidating, threatening, offensive, derogatory, hateful or inflammatory; (d) is indecent, obscene or pornographic; (e) is contrary to the interests of the company; (f) is sensitive or proprietary information of the company, including business plans, customer lists, unpublished financial information and the like; (g) is inaccurate, libelous or defamatory, or that discloses private or personal matters concerning any person; (h) is a virus, worm, “Trojan horse” or any other harmful, contaminating, destructive or disruptive element; (i) a political message, charity request or petition for signatures; (j) a testimonial or name or picture of any person for the purpose of advertising or promotion without that person’s written permission; or (k) a password, a credit card number, a social security number, a PIN or the scanned copy of anyone’s signature.

The fact that the Web instantly facilitates international business simply means that companies will confront international questions sooner than they might have in the past. The international nature of Cyberspace, however, does not require that a locally-based business suddenly become international. Specific Web site policies can shield the site owner from the application of unintended laws from unfriendly jurisdictions.

**9. Present a clear policy on how you will use personal information collected on your Web site.**

The collection and use of information on consumers is a controversial Cyberspace law issue today. The Federal Trade Commission has been encouraging companies to post notices on their Web sites explaining to consumers how personal data collected on the site will be used. The FTC has also taken the position that misrepresentation of a Web site's privacy policy can constitute a violation of the Federal Trade Commission Act. In the case of *In re GeoCities Inc.*, FTC File No. 9823015 (February 5, 1999), the FTC approved a consent order requiring the company to place a "privacy notice" on the Web site's home page and a link on any page that collects personal identifying information labeled as follows: "Notice: We collect personal information on this site. To learn more about how we use your information click here."

The European Commission issued a draft Directive on data privacy in 1990, reasoning that data should not lose its privacy protection when flowing into a country with a lower standard of privacy, and that Member States should not be able to block data flow from other Member States on privacy grounds. After five years of debate, the Council and the Parliament of the EU adopted the Directive in 1995, requiring Member States to conform their national laws to the Directive by October 25, 1998. The Directive requires that such national laws prohibit the exchange of data between European database operators and companies in other countries that do not have adequate data privacy protection.

Because the United States would be one of those countries, officials of the European Union and the United States have been working on an agreement that would allow for the continued flow of such data between the EU and the U.S. The U.S. is seeking assurances from the EU that U.S. companies adhering to certain privacy principles would have safe harbor protection against challenges under the EU directive. Presumably, U.S. companies follow the requirements of the Federal Trade Commission with respect to privacy will not run afoul of the EU requirements. It remains to be seen what specific requirements will result from these negotiations. U.S. banks and other financial institutions are seeking safe harbor protection from EU regulation on the basis that they are already heavily regulated by the U.S. government.

***10. Pay attention to ethical rules on the use of the Web by lawyers and law firms.***

The use of the Web by lawyers is very common today, and there is far less fear of misuse of the medium today than there was as recently as one year ago. E-mail, in particular, has greatly facilitated international business transactions both for lawyers and their clients. Nevertheless, some jurisdictions impose stricter rules than others, and it pays to be cautious.

For example, different jurisdictions have taken different views on the use of unencrypted e-mail in attorney-client communications. The risk of disclosure of confidential information can jeopardize the attorney-client privilege. Accordingly, some states may require client waivers. The New York State Bar Association Committee on Professional Ethics, however, has concluded that “lawyers may in ordinary circumstances utilize unencrypted Internet e-mail to transmit confidential information without breaching their duties of confidence ....” (Opinion 709 - 9/16/98.) For especially sensitive information, however, more secure means of communication may be appropriate.

On Web sites, lawyers should clearly indicate the states in which they are admitted to practice. While lawyers licensed in one state may appropriately render legal services to clients in another state in many circumstances, such interstate services may sometimes constitute the unauthorized practice of law in the other jurisdiction. *See Birbrower, Montalbano, Condon & Frank v. Superior Court of Santa Clara County*, 70 Cal. Rptr. 2d 304 (Cal. Sup. Ct. 1998).

Law firms should make it clear on their sites that information provided is of a general nature and does not create an attorney-client relationship.