

PROTECTING INTELLECTUAL PROPERTY WHO OWNS WHAT?

ABA TechShow 2001

Session C09

Saturday, March 17, 2001 8:00-9:00 AM

Presented and Prepared by:

Natalie Hanlon-Leh, Esq.
Member, Faegre & Benson, LLP
nhanlon@faegre.com
www.faegre.com

and

Seth G. Rowland, Esq.
President, Basha Systems LLC
sg@bashasys.com
www.bashasys.com

PROTECTING INTELLECTUAL PROPERTY WHO OWNS WHAT?

Natalie Hanlon-Leh
Faegre & Benson, LLP
nhanlon@faegre.com

and

Seth G. Rowland
Basha Systems LLC
sgr@bashasys.com

I. HOW MUCH DO YOU KNOW?

On a daily basis, you advise your clients about securing protections for their intellectual property. You may file patents, register copyrights and trademarks, or draft non-disclosures and licenses. But how much do you really know about YOUR intellectual property? Some real life examples to test your knowledge of: “Who owns what?”

A. Web Design Company (SGR)

Transfer of Material from Law Firm Web-site.

1. Background: Law firm retains a web design company ("LegalWebs") to put together its web-site. Law firm puts together a compilation of articles on estate planning, including model forms based on its own files. Articles and forms are edited by LegalWebs and posted on law firm web site. Six months later, the articles and forms show up on www.law.com, a commercial web-site hosted by a LegalWebs affiliate.
2. Issues:
 - a. Who owns the articles and forms?
 - b. Does the web design company have any republication rights in the articles and forms?
 - c. Is the law firm entitled to royalties?
 - d. Does it matter that the forms and articles are republished with attribution?
 - e. Would it be different if Law.com merely provided a click link and placed the article/form in a frame?
 - f. How could the contract between the law firm and web design company have either facilitated or hindered this action?

B. New Media Advertising Company (SGR)
Unauthorized Used of Copyrighted Material

1. Illustration: Law firm retains a new media advertising company ("New Media") to build its web site. Law firm wants a "slick look" with fancy pictures and design elements. Law firm also wants some content – articles that will draw potential clients to the web-site. In a dispute over the bill, the following facts emerge. New Media did a survey of competing law firms and borrowed heavily on design elements of other firms, including pictures, color schemes and "puffing" language. New Media also borrowed several CGI scripts, JAVA applets and ActiveX controls, but rewrote them to suit its needs. For articles, New Media searched through webzines and gathers a collection of a dozen articles. Articles were printed with attribution, but only in fine print, leaving the impression articles were authored by the firm, rather than merely reprinted as a public service.
2. Issues:
 - a. Should the law firm pay its bill?
 - b. Can the law firm "go live" with the web site?
 - c. What elements of the web-site can be used without securing a release from the owner of the IP?
 - Design elements?
 - Pictures?
 - Puffery?
 - CGI, JAVA and ActiveX?
 - Articles from Webzines?

C. The Departing Partner (SGR)
Cleaning out the Precedent File

1. Illustration: Law firm partner has a difference of opinion with his colleagues and resolves to leave the firm. In preparation for setting up a new practice, partner copies to a Zip® disk all files he has authored. Working with the firm's document management system, he finds all files for his clients; and then files for any clients for whom he has done work. He also copies his collection of model agreements and forms. Finally, he copies his address book (personal and firm) and archives his e-mail files. As the *coup de grace*, partner takes his firm-purchased laptop home. Incidentally, partner leaves all his office and client files untouched, pending formal client requests for their files.
2. Issues:
 - a. Where did the partner cross the line?
 - b. What can the partner lawfully take?

- Personal files?
 - Client files?
 - Other client's files?
 - Model agreements and forms?
 - Personal address book?
 - Firm address book?
 - E-mail files?
 - Laptop computer?
- c. Could anything have been done to prevent the copying?

D. Domain Name Poaching (NHL)

Law Firm Names, Trademarks and Domain Names

1. Illustration: Law firm named Doe and Jonas, P.C. opens a website at the URL www.dojo.com, named for its common nickname “DoJo”. Law firm is surprised that they aren’t getting more hits to their website, and they discover that a non-profit anti-lawyer organization is posting law related content at www.doejonas.com. Further investigation reveals that the same firm has taken the names www.doejones.com, www.doejonas.org, www.doe.com, www.doejones.org, www.dowjonas.com, and www.doe.com. The law firm also learns that Doe, Inc., a national deer preservation group has registered and is using www.doe.org for its grassroots anti-hunting website. Finally, the firm learns that some disgruntled former clients are posting insults and other bad things about the firm at www.dojosucks.com.
2. Issues:
 - a. Can the law firm stop these other domain name registrants from using these domain names? If so, which ones? How?
 - b. Should the law firm proactively register similar domain names to preclude potential squatters? If so, how many domain names is reasonable?
 - c. What should the law firm do about registration of the new top level domains: e.g. .biz, .pro, .coop, etc.
 - d. Should the law firm seek a federal trademark registration for its name? Its nickname? other marks?

E. Water and Oil Don't Mix (NHL)

Parting of the ways between an e-tailer and a retailer

1. Illustration: For over 25 years, law firm has represented a well established company Smart Stuff, Inc. which makes educational childrens' toys . The company has just expanded into the world of e-commerce, pursuing a joint venture www.smarttoys.com in conjunction with amaron.com, an established e-commerce retail outlet. Unfortunately, the venture isn't as successful as hoped, and the parties decide to split up midway through their agreed upon 5 year joint venture.
2. Issues:
 - a. Who owns the brand "SmartToys.com"?
 - b. Can the retailer use SmartToys.com after the joint venture terminates?
 - c. The website has a specialized search engine and other tools which were specially developed for SmartToys.com. What rights does the retailer have to use those tools after the joint venture terminates?
 - d. Who owns the data about users who accessed the site? What can each party do with the data?

II. WHAT CAN YOU DO?

The situations described above can and will arise. You should keep on the lookout and be aware of your potential liability. There are a few things you can do, however, to minimize your risk:

A. Draft clear contracts that specify ownership of IP and licenses (NHL)

1. State who owns what in your contracts: Patentable inventions, ideas, innovations, trademarks and service marks, copyrighted materials, data rights and trade secrets.
2. Make sure to include materials which may be developed under the contract as well as those which exist at the time you enter into the contract. Parties should make sure the agreement specifies that it covers future methods of delivery. such as webTV, cable, wireless and broadband access. In the alternative, the parties should specify what happens when the base technology changes or the content must be reformatted to be compatible with new technology.
3. Be specific and complete. Avoid general terms like "digital rights" and "on-line". Address exclusivity, permissions, and restrictions.

4. Data usage provisions should address, among other things, the types of internal use that can be made and sales of the information to third parties.
5. Prepare for the End: Make sure you specify who owns what when the contract terminates.

B. Clearly Display Copyright, Trademark and other notices (SGR)

1. Copyright notice. Puts the infringer on notice that you value and intend to protect the material on your web-site.
2. Visible watermarks
 - Identify the source
 - Mark image in a way that mark can't be removed without destroying the image.
3. Limitations
 - Images and text can be edited. Mark can be cropped or airbrushed.
 - Marks can be distracting or obscure important parts of the image

C. Use Digital Watermarks (SGR)

1. Digital watermark software embeds information about the author/owner into graphic, video, or audio files. Digital watermarks can be combined with tracking services to ferret out all illegal copies on the web. The same software may also be used to screen images for digital watermarks.
2. Digital Watermark must have the following features:
 - Must be unremovable and unalterable.
 - Must not degrade with file duplications
 - Must not perceptively disrupt the original data file
 - Mark is "invisible" to the human eye
3. Watermarking Software and Services
 - Alpha-Tec: www.alphatechltd.com
 - Cognicity: www.cognicity.com
 - Giovanni: www.bluespike.com/giovanni/giovanni.html
 - Digimarc: www.digimarc.com
 - StirMark: www.cl.cam.ac.uk/~fapp2/watermarking/image_watermarking/stirmark
 - Signum Technologies: www.signumtech.com
 - SysCoP: www.mediasec.com/products/index.html
 - unZign: www.cl.cam.ac.uk/users/fapp2/steganography/image_watermarking/unzign/
 - Verance Digital: www.verance.com/digital/index.html
 - MusiCode: www.musicode.com

4. Limitations
 - Difficult if possible to watermark text
 - Image alteration may diminish or strip digital watermark
 - Does not prevent copying
 - Robot search engines cannot reach into password protected sites.

D. Policing and enforcement (SGR)

1. Site Audit: Periodically run a complete audit of you site to determine ownership/license to display all material shown therein.
 - Know source of every image and article
 - Check for link framing
 - Make sure trademark ownership notices are displayed
2. Secure written permission of all copyright holders and/or license to display.
 - Secure copyright permissions in writing.
 - Comply with all requirements of the copyright holder.
 - Make sure copyright permission notices are displayed. (e.g. Reprinted with permission of)
3. Audit Trails
 - Log files
 - Document usage profiles
 - Internet usage

E. Website Audits (SGR)

1. Audit Trails
 - Use of log files, counters, log analyzers and tracking programs.
 - Record clicks and navigation of all users
 - Require site registration to use, and track each user. Counters, trackers and Log Analyzers.
2. Website Log Analysis Tools
 - Access Watch – www.netpressence.com/acceswatch
 - Analog – www.statslab.cam.ac.uk/~sret1/analog
 - HitBox – www.hitbox.com
 - net.Analysis – www.netgen.com
 - NetTracker – www.sane.com
 - Sawmill – www.flowerfire.com/sawmill/
 - SiteTracker – www.sitetracker.com
 - SuperStats – www.superstats.com
 - WebTrends – www.webtrends.com

- WinWhatWhere – www.winwhatwhere.com
- Marketwave Hit List Pro – www.marketwave.com

3. Limitations

- Most tools don't record the actual identity of visitor
- Snooping programs that capture actual identity are of questionable legality

III. FORMS OF PROTECTION FOR TECHNOLOGY AND INFORMATION

These materials will explore the four major types of intellectual property protection in the United States: copyrights, trade secrets, and trademarks. Each of these types of protection will be considered and the key types of provisions in contracts will be identified.

A. Copyright Protection for Content and Computer Software.

1. Copyright law protects original works of authorship fixed in any tangible medium of expression from which they can be perceived, reproduced or otherwise communicated, either directly or with the aid of a machine or device.
2. Copyright protection exists at the moment of creation, and lasts for seventy years after the author's death. If the work is created anonymously or is a "work for hire," the copyright lasts for 95 years from publication, or 120 years from creation, whichever expires first. (These terms were recently extended as part of the Sonny Bono Copyright Term Extension Act; the above terms represent the rules for newly created works – the details for older works are slightly different.)
3. Registration is not needed to obtain copyright protection; however, copyright registration is highly recommended. Registration is required before initiating suit and is a prerequisite for awards of attorneys' fees and "statutory damages" (compensation without having to prove the extent of economic damage or the infringer's profits). In addition, registration provides notice of your rights to others.
4. Copyright notice is not needed for copyright protection. Notice is recommended, however, to defeat claims of innocent infringement and deter infringement. Sample Notice Format:

© 2001 Faegre & Benson LLP

5. Copyright protection initially vests in the author of a work. In the case of works created by employees (but not independent contractors) within the

scope of their employment, the employer is considered to be the author and the copyright owner. In all other cases, if a company wishes to secure copyright ownership, then it will need to enter into a written agreement transferring the copyright.

6. United States copyright law provides for the protection of computer software. This protection prevents someone from making “copies” of another’s computer software. Copyright law does not prevent someone from making computer software having the same purpose or functions of another’s computer software. In the United States, copyright law covers computer software. Court decisions have clarified that the copyright statute extends to source and object code, microcode, applications and operating systems, and code on disk, in RAM or embedded in ROM.
7. Scope of protection provided by copyright law is sometimes ambiguous, especially in the computer software area. There are general rules which help govern the proper scope of protection.
 - a. Copyright only covers the expression of ideas. Ideas themselves are not protected by the Copyright Act.
 - b. Copyright does not extend to elements which are not original to the author. An author cannot copy elements from another source and then seek to use the copyright laws to prevent the copying of those very elements.
 - c. Copyright does not extend to standard elements or to purely functional elements.
 - d. Independent creation is a defense to a claim of copyright infringement. Copyright only prevents copying.
8. To establish a claim of copyright infringement, the plaintiff must prove copying. Proof of direct copying is the best evidence, but difficult to obtain. If there is no evidence of direct copying, a plaintiff must prove access to the copyrighted work and that the defendant’s work is substantially similar to the plaintiff’s copyrighted work.

B. Patent Protection

1. In exchange for an inventor sharing his or her invention with the public, the government may issue a patent which grants to the patent holder an exclusive right to make, use and sell the invention covered by a patent.

2. This exclusive right previously was 17 years from the date of issuance of the patent. For patent applications filed since June 8, 1995, the duration is 20 years from the date of filing.
3. The scope of protection afforded by a patent are determined by its claims. Claims are originally drafted by a patent attorney and are often amended during “examination” of the patent application by the U.S. Patent Office.
4. To be patentable, an idea must be new, useful and nonobvious.
5. To be patentable, an idea must be of a type provided for by the patent statute, i.e. “Statutory Subject Matter.” The statute provides that patents may be granted for “any new and useful process, machine, manufacture or composition of matter, or any new and useful improvement thereof.”
6. The patent statute does not expressly provide for the patenting of computer software. As of the early 1970s, it was unclear whether any invention which involved a computer program constituted statutory subject matter. Courts have subsequently held that many inventions relating to computer software are patentable.
7. The Court of Appeals for the Federal Circuit has recently issued opinions expanding the scope of patentable subject matter in the areas of computers, software and business methods implemented by computers and software.
8. Unlike copyright protection which arises automatically upon creation, obtaining patents is a relatively expensive and time consuming process.
9. In the United States, patent applications are filed in the name of the inventors, not the employer. Typically, however, employees of a company are obligated to assign all rights in patents and patent applications to the company.

C. Trade Secret Protection

1. A trade secret consists of information (i.e., formula, pattern, device or compilation of information) which derives independent economic value from not being generally known and which is the subject of reasonable efforts to keep it a secret.
2. Unlike patents and copyrights, there is no federal statute governing trade secrets. Actions alleging the misappropriation of a trade secret arise under state law. Many states have adopted the Uniform Trade Secrets Act.

3. Trade secret protection has been used to protect databases, mathematical models, computer hardware and computer software.
4. Reverse engineering of a product to a trade secret is allowed. Generally you can decompile any software which you own to discover any trade secrets resident in the software.
5. To avoid the right to decompile software, most software is licensed rather than sold. The license agreement may require that any trade secrets in the software be maintained in secrecy and that the licensee not decompile the software. As a result, if trade secrets are to be maintained in computer software which is delivered to third parties, the software should be subject to an enforceable license agreement rather than sold outright.
6. It is not possible to have both patent protection and trade secret protection on a single invention. When a patent is issued, a complete description of the invention is published making any secret in the invention public knowledge. However, patent applications are maintained in secrecy until a patent issues. It is possible, therefore, to file a patent application on a trade secret and, if the patent claims are rejected, withdraw the application and maintain the invention maintained as a trade secret.

D. Trademarks and Service marks

1. A “trademark” is a word, name, symbol, device or any combination thereof adopted and used or intended to be adopted and used by a manufacturer or merchant to identify his goods and distinguish them from those manufactured and sold by others. 15 U.S.C. § 1127. A service mark is similar to a trademark except that it is used or intended to be used in connection with services rather than goods.
2. Generally, trademark/service mark rights arise from use of the mark in conjunction with goods and services. Additional rights are available if the mark is registered with the U.S. Patent and Trademark Office (“USPTO”), a process known as “federal registration.” Trademark rights are of potentially infinite duration. Trademark and service mark registrations are valid for continuously renewable terms of ten years. However, a mark is protectable only so long as it is used or any non-use is excused. Abandonment of a mark terminates one’s rights in the mark.
3. One of the primary functions of a mark is to indicate source. Hence, a mark should not be assigned unless the assignment includes not only the mark but also the goodwill associated with the mark.

4. Another primary function of a mark is to indicate quality. Consumers expect all goods and services bearing the same mark to be of a comparable quality. Hence the licensing of a mark requires not only a provision allowing use of the mark by the licensee, but also a provision providing sufficient quality control measures. The licensee must be able to insure that the goods and/or services of the licensee sold under the licensed mark are of a quality which is comparable to the quality of the goods and/or services offered by others under that same mark.

IV. SETTING THE RULES: WHAT TO LOOK FOR IN TECHNOLOGY LICENSE AGREEMENTS

A. Interplay with Licenses

1. The various types of intellectual property protection described above allow the “owner” of technology and/or information to prevent others from exploiting such technology and/or information. Inherent in the right to exclude others is the right to allow others to use its technology and/or information. In many instances, the owner wants to do this in exchange for valuable consideration, typically money. A license agreement governs the terms and conditions of such use.
2. License agreements come in many forms: oral or written, express or implied. While certain transactions do not warrant the time and expense of a written license with explicit terms, to the extent that the technology and/or information is valuable, having a written license which addresses all relevant terms is generally desirable, whether you are the licensor or the licensee.

B. Overview of License Concerns

1. A license agreement should set forth not only the key business terms of the transaction (e.g., price, deliverables, maintenance obligations), but should include all of the other details that the business people may be reluctant to focus on.
2. At least three broad concepts require significant input from the business people involved:
 - a. What is each side promising and not promising (the warranties, representations and covenants, and the corresponding disclaimers)?
 - b. What are the remedies if the other party fails to live up to its promises, and what is the exposure should your client fail to live up to its promises?

- c. What is the business risk if these remedies are insufficient?
3. It is important to recognize the relationship between items (a) and (b) above. For instance, a licensor can warrant anything and everything if it knows that the remedy for a breach of a warranty is meaningless. (Of course, if the party making the warranty knows that it false, then fraud claims could come into play.)
4. Item (c) recognizes the implicit point that clients should not rely on the contract to protect their business; technology and business procedures should be set up in a way such to minimize the possibility of problems and the business losses if problems nonetheless arise.) This is especially true if the other party is too small (or otherwise lacks sufficient assets) such that any judgment against the other party would be meaningless.
5. These three broad concepts impact virtually every aspect of the license agreement. These materials, however, will focus on only a few issues. Furthermore, because these issues are often highly intertwined with the particular business setting and/or type of technology, they are presented here in summary fashion rather than in detailed paragraphs. Furthermore, for simplicity, this portion of the materials are presented from the perspective of the licensee, except where noted.

C. Sample Issues for Software License Agreements

1. Non-Infringement
 - a. Identify the scope of the “promise” that the software does not infringe any other party’s intellectual property rights. Are there any exclusions?
 - b. What is the remedy if the software does infringe, or if there is a claim that it infringes? (Typically, indemnity, with an ability by the licensor to terminate and give a refund if it cannot modify the software or procure a license.)
 - c. Define the procedures to follow if there is a claim that the software infringes some other party’s rights.
2. Conformance with Specifications
 - a. Identify the scope of the “promise” that the software will function as desired by the licensee. (Typically, the licensor will promise that the software will operate in substantial conformity with its written specifications.)

- b. What is the duration of this promise? Can this be extended by purchasing maintenance/support?
- c. What is the remedy if this promise is broken? Is the licensee entitled to damages, or does the licensor simply have to fix the software?
- d. What types of errors does the licensor have to fix? How soon must these be fixed? Are there any limitations on whether the fix is in the form of patches, updates, or upgrades?
- e. What if the licensor fails to fix the software, or fails to do so in a timely manner? (A related issue is what is a timely manner.)
- f. What is the impact of “force majeure” events (so called “Acts of God”) on these timelines?
- g. Consider the parallel of these issues in the case of services (e.g., telecom services). In particular, consider the implication of force majeure exceptions on the particular contingency features that led to the selection of this vendor (e.g., multiple telephone lines, UPS and generators).

3. Source Code

- a. Does the licensee get a copy of the source code?
- b. Are all necessary supporting materials also included (e.g., development documentation)?
- c. How often must the licensor update the deposit copy of the source code?
- d. Is the source code being placed in escrow, being given directly to the licensee, or neither?
- e. What are the trigger events for the release of the source code? Are these early enough? (Keep in mind that while quick access is essential to repair a problem, an adequate license is required to avoid infringing the licensor’s intellectual property.)
- f. Is the licensee being given an adequate license to use and modify the source code?

- g. How does the licensee verify that the source code is complete and accurate?
- h. If a third party escrow agent is being used, is this agent sufficiently “on the hook” for failures on its part?

4. Confidentiality

- a. Often, a license will include a confidentiality provision.
- b. From the licensor’s perspective, it will want the source code of the software to be treated as confidential information.
- c. The license will likely include a provision restricting reverse engineering or modifying the software.
- d. Should the licensor also be subject to confidentiality obligations (e.g., with respect to the licensee’s business plans and data)?

D. Remedies

1. Ability to Terminate

- a. At what point(s) can each party terminate the license?
- b. Can the licensor terminate or suspend providing services (such as maintenance) if there is a dispute over whether the licensee is in breach?
- c. Can breaches be cured? How long is the cure period? Are there any exceptions (other than breaches which by their very nature cannot be cured, such as a breach of a confidentiality obligation)?
- d. Is there a termination fee? Does this vary by when the termination occurs or by whether the other party is in breach?

2. Rights upon Termination

- a. Are there any continuing rights to use the software following termination? If this software is incorporated into a product sold/licensed by the licensee to end-users, then a continuing end-user license may be essential.

- b. Is the licensor obligated to help the license migrate to other software? What is the cost for such assistance? Does this depend on why the license was terminated?
 - c. Which provision of the licensee agreement continue in effect?
 3. Damages
 - a. What types of damages are covered and excluded? Does this depend on which type of promise or obligation was breached? Are there any exceptions?
 - b. Does the agreement provide for liquidated damages, or a cap on damages? Does this depend on which type of promise or obligation was breached? Are there any exceptions?

IV. WORK FOR HIRE: PROTECTING INTELLECTUAL PROPERTY WITH EMPLOYEES OR INDEPENDENT CONTRACTORS

A. As noted above, valuable intellectual property can “reside in” employees or independent contractors who develop technology or content. Most commonly intellectual property developed by employees is protected through

- Trade Secrets
- Copyright “work for hire” agreements
- Assignments of patents and other inventions

B. Employees

1. **Copyright.** Companies are in the best position to protect intellectual property developed by employees. Any copyrightable works authorized within the scope of the employee’s employment are considered “works for hire” and belong to the employer.
2. **Patents.** However, a patent is initially the property of the inventor(s) who conceived the invention claimed in the patent. The general rule is that the employee-inventor will own the invention and the employer will merely have “shop rights” which permit it to use the patented technology without a license or paying royalties. Under the law of some states, inventions conceived by an employee are generally deemed to be owned by the employer if the invention was created by the employee within the scope of his or her employment. To assure ownership of patentable inventions,

employees should be required to assign all patentable inventions to the employer.

3. **Trade Secrets.** Because employees may have access to confidential information and trade secrets, employers should require employees who have access to such information to sign confidentiality or non-disclosure agreements. These agreements should include a detailed description of the confidential information which must not be disclosed.
4. **Non-Competition Agreements.** Where working for a competitor would require use of or disclosure of trade secrets, employers should consider non-competition agreements.

b. Elements of an enforceable agreement

Although enforceability will vary greatly in different states, courts generally have established three critical elements to an enforceable non-compete agreement.

1. Consideration

The employee must sign the agreement in exchange for some benefit to which he or she was not already entitled. The best way to satisfy this requirement is to expressly make any offer of employment contingent on the employee signing the non-compete agreement. Non-compete agreements signed after employment has begun must be supported by independent consideration at the time they are signed. In some states, continued employment, without more, is not sufficient to support a non-compete agreement signed after employment begins.

2. Protectable business interest

Non-compete agreements are enforceable only to the extent that they are necessary to protect a legitimate business interest. It is not necessary that information be a trade secret to be protected under a non-compete agreement, but the information must be confidential and not generally known to or ascertainable by the public. Goodwill is also an intangible company asset that can be protected through the use of non-compete agreements.

3. Reasonable scope

a. Temporal

Non-compete agreements must not impose restrictions longer than are reasonably necessary to protect the employer's business interest. This is an issue decided on a case-by-case basis. In each case, the particular circumstances of employment and the market are critical.

b. Geographic

The reasonableness of the geographic scope of the limitations is also an issue decided on a case-by-case basis. Because the law calls for reasonable geographic restrictions, it is advisable to build such restrictions into non-compete agreements whenever possible. However, courts in certain cases will enforce non-compete agreements that have no geographic limits but are instead limited to certain customers or prospects. This is becoming more common with the continued expansion of the worldwide market.

4. "Blue-Pencil" doctrine

Some courts may take an overly broad restriction and enforce it to the extent the restriction is reasonable. However, whether to blue pencil an otherwise unenforceable agreement is left to the discretion of the court, and some courts will invalidate overly broad restrictive covenants entirely rather than rewrite the agreement to make it enforceable.

C. Independent Contractors

The copyright to any works developed by independent contractors will generally be owned by the independent contractor unless a "work for hire" agreement is executed and the work of authorship is one of the nine types set forth in 17 U.S.C. § 101;

- a contribution to a collective work
- a part of a motion picture or other audiovisual work
- a translation
- a supplementary work

- a compilation
- an instructional test
- a test
- answer material for a test; or an atlas

To the extent a work of authorship does not fall within the work for hire exceptions, the independent contractor should be required to assign the copyright to the employer. Where appropriate, independent contractors should also be required in a written agreement to assign inventions and agree to maintain the confidentiality of trade secrets.