

TECHNOLOGY LAW IN COLORADO:
AN ADVANCED APPROACH
SEMINAR 12/12/03

I. LEGAL CHALLENGES FOR LICENSING INTELLECTUAL PROPERTY

Presented by Robert L. Allman, Esq.

TECHNOLOGY LAW IN COLORADO:
AN ADVANCED APPROACH

I. LEGAL CHALLENGES FOR LICENSING INTELLECTUAL PROPERTY

A. Copyright in the Digital Environment

1. Work-Made-For-Hire - Who Owns the Rights to the Copyright?

Understanding the Work Made for Hire Doctrine is key to understanding the protection of intellectual property rights and software and other technology. It has been, in the past, frequently litigated, and it has certainly presented surprises to the innocent but unwary employer. Copyrights, absent agreement, belong to the creator of the product if that creator is an independent contractor.

Copyright ownership resides with the independent contractor under the theory that a person is presumed to own one's work, absent written agreement to the contrary. In other words, the presumption of ownership rests with the contractor. As such, the employer who hires out the development of software, for example, must have a written agreement assigning the ownership rights to that product to the employer. This documentation can take various formats, some lengthy and some not, but should contain rights of assignment even if it does not specifically reference the concept of "work made for hire."

Presented by Robert L. Allman, Esq.
Allman & Mitzner, LLC
535 16th Street, Suite 727
Denver, Colorado 80202
(303) 293-9393
(303) 293-3130 (fax)
rallman@allman-mitzner.com

The concept of work made for hire is that if this sort of presumably custom work is being made for you, it is incumbent upon the hiring party to set the terms under which the intellectual property rights are transferred. It is interesting that in the employer/ employee context, however, the presumption is the opposite, and it is presumed that the employer owns the work, since the employee presumably produced the work under the employer's supervision.

Documenting your independent contractor agreements is extremely important when dealing with the sale of the company and any other transaction that would require documentation of your company's ownership of its intellectual property. It has become standard to have each employee also agree to an inventions assignment agreement, as it is simply good practice to do so. It can also be used to document confidentiality and non-compete issues. In addition, it is always necessary to have a written assignment of patent rights for the company's protection, and thus the Work for Hire Doctrine, in practical terms, has been incorporated into the overall assignment of intellectual property rights.

Considering the development of software-related patents, the inventions assignment agreement has only grown in importance. These written agreements have become so prevalent and commonly recognized as an issue in corporate transactions that the absence of such a written agreement can be very difficult to overcome.

A few suggestions, if you have issues with failing to have an independent contractor execute such an agreement. First, try to prevent contractor's use of at least some of your key information - it may include trade secrets. This may make it more difficult for the contractor to license the product. If the contractor produced only a portion of the product, the company may have arguments about whether the contractor is a joint author. You could decide that you are better off re-doing the product in a clean environment, that is, that you are not simply taking the work done by the contractor and infringing upon it in a derivative manner. If all else

fails, perhaps a fee or licensing fee can be negotiated, which accomplishes the same purposes.

2. Monitoring Linking and Framing

Linking and framing have been a hot topic since the outpouring of websites and the commercial transaction of website business. A link, also called a hypertext link or hyperlink, allows a visitor to a website to click on and to then access another website. Typically, linking does not include the actual storing of the information on the linking website (known as caching), and it is intended to presumably facilitate the obtaining of additional information without having to search for that website.

The primary problems occur if the linking gives the user some indication that the link is somehow authorized by or related to the particular website if it is not. This type of bootstrapping of publicity or utilizing of another's good name can be frowned upon depending upon how it is done. If the linking is on the order of "other interesting websites," clearly done for purposes of providing additional information or simply being of service to related goods or materials, it typically does not pose a problem. However, if placed upon the website in such a way as to suggest that there is some sort of closer alliance, or to utilize a trademark of that company without authorization, this could be seen as a problem of infringement, either of copyright or trademark, or possibly a false advertising claim under the Lanham Act.

A form of linking could create Lanham Act liability if it is done in a way that would appear to be deceptive, as in creating a false impression with consumers. Most of the cases on this issue have been in the trial court level, with little appellate guidance. The Ticketmaster v. Microsoft Corp. case (C.D. Cal., filed April 28, 1997), involved allegations of this type of claim where it was alleged Microsoft made it appear as if its entertainment website was affiliated with Ticketmaster. The case was settled - so has little precedential value other than the obvious practicality of suit avoidance behavior for others. Ticketmaster Corp. v. Tickets.com, Inc., 54 U.S.P.Q.2d 1344 (C.D. Cal. 2000) held that hyperlinking, by

itself, is not copyright infringement. In Ebay v. Bidder's Edge, Inc., 100 Fed.Supp.2d 1058 (N.D.Cal. 2000), Bidder's Edge posted listings from Ebay's auction site directly on the Bidder's Edge website by way of linking. The court held this to be an unauthorized form of trespass.

The issue of framing is similar to linking, except that framing will allow the user of a website to view content from other sites without leaving the first site. Essentially, the user stays on the original site and framing arguably makes it easier for the consumer to believe that the sites are more closely related. Again, the issues in framing have been addressed primarily in the context of trademark infringement and, in those cases, the trademark rights may be upheld if used unfairly.

It would appear that it will be increasingly difficult, with sophisticated consumers, for linking or framing, in and of themselves, to lead to much dispute so long as the websites doing the linking and framing have some sort of disclaimer or it is otherwise obvious that these are not related sites.

Metatagging, the process of using metatags - codes which are embedded in hypertext language used in websites which are picked up by search engines - could be used in a deceptive manner, and if infringing upon trademarks, unfair use may be enjoined. Playboy Enterprises v. Calvin Designer Label, 985 Fed.Supp. 1220 (N.D. Cal. 1977) (metatags which embedded the marks of Playboy and Playmate were enjoined).

B. Legal Issues and Strategies Involving Software and Other Patents

Within the context of technology law, software copyrights and possibly patent rights become a company's stock in trade which require legal protection. A central concern of any policy regarding issues and strategies must first rest upon protecting those rights.

The first areas of protection are internal, that is, having employees, contractors and third parties execute appropriate invention assignment rights, non-competes and confidentiality agreements, suitable to the task. In other words, such

protective agreements should be modified to suit the particular transaction. In addition, a company policy should be in place to monitor deadlines for filing, the need for updating of copyrights and patents to take into account new developments, and the use of protective devices in order to make it more difficult for infringement or retaliation by the disgruntled employee.

Any transaction involving software should be reduced to writing. In any transaction in which multiple parties may be involved in accessing copyrighted or patented information, the respective parties' rights and responsibilities should be documented in writing. Licenses should be consistent and provide for revocation in the event of breach.

Do not agree lightly to escrowing source code or other materials, particularly when you are not sure whether or not you will have a long term relationship. The placing of software in escrow may be a point of contention for a subsequent purchaser of the company or an entity mainly interested in your property. Any escrow agreement for source code should have very strict conditions for first, the requirement of such escrow, and second, the distribution of source code held in escrows.

The key point in using intellectual property is that, as changes are made and the products evolve, the company should take care to also supplement its protection.

C. Trademark Risk - Trade Dress Protection, Domain Names and Trademark Dilution

Trade dress is a form of trademark protection which extends to the look and feel, and packaging of the product. Trade dress protection is more subjective than most trademark litigation, in that it is based upon concepts of consumer confusion and a packaging look which leads the consumer to, without really thinking about it, unconsciously believe that the products are the same or related. Trade dress issues can conceivably arise in a website look, for example, that

may be too close to a competitor's or which would appear to be giving the impression of actually being that competitor's website. At least, understand the general trade dress concerns and consider whether one website may reasonably be confused for another, or trigger a consumer response of another.

There can be some confusion over the issue of domain names as opposed to a trademark. While one can obtain an available domain name without any scrutiny other than whether that name has already been taken, such a domain name may also infringe a valid trademark. A name which is simply close to that of a trademark name may also infringe, even if it is not particularly confusing to the consumer, if it would be seen as diluting the goodwill that has been generated by the trademark.

The Madrid Protocol, which was signed into law on November 2, 2002, will allow for the international registration of marks, which establishes a procedure for registering trademarks in countries which have agreed to the Madrid Protocol. The specific requirements are beyond the scope of this presentation; however, it is essentially based upon having a valid national trademark and then allowing for a central registration of trademarks, something like a registration of a foreign judgment. There will be some problems interfacing with other countries' requirements and different takes on trademark requirements, but it is an effort to provide some uniformity in an area that has historically not been particularly accessible to small entities given the cost, time and expense.

Some cases of interest: In Promatek Industries Limited v. Equitrac Corporation, 300 F.3d 808 (7th Cir. 2002), the court found that in comparative advertising, using a competitor's mark may be permissible, but to use it in a metatag is not allowed because of its potential for customer confusion. In Kelly v. Arriba Soft, Inc., 280 F.3d 934 (9th Cir. 2002), the court found that Arriba was not a passive conduit, but created a direct link to copyrighted images that led to the unauthorized display of Kelly's copyrighted images.

Cybersquatters are not protected by registering spelling variations of a registered domain name. Shields v. Zuccarini, 254 F.3d 476 (3rd Cir. 2001). In Brookfield Communication, Inc. v. West Coast Entertainment Corp., 174 Fed.3d 1036 (9th Cir. 1999), the court held that the unauthorized use of a trademark in metatags constituted trademark infringement.

As to trade dress protection, it is not necessarily clear whether that protection would apply to the look of a website. However, fair use could include a critical website, such as in Bally Total Fitness Holding Corp. v. Faber, 29 Fed.Supp.2d 1161 (C.D. Cal. 1998).

D. Trade Secrets - Enforcement and the Inevitable Disclosure Doctrine

The concept of trade secrets was once less a part of commercial and corporate transactions. In modern times, however, trade secrets have become increasingly important when dealing with customers, prospective customers, employees, contractors, and interested third parties. Colorado has the Uniform Protection of Trade Secrets Act, and is relatively liberal in applying protection for trade secrets. Apart from a description of trade secrets which is beyond the scope of this outline, suffice it to say that virtually any technology related information can be considered to be the trade secrets of a company. One can argue about customer lists, certain types of financial information, general know-how or business procedures, but if the trade secret is part of a computer program, source code or database design, it will be protected.

Given the advent of confidentiality agreements and the common requirement that a hiring employer take care not to receive the trade secrets of a new employee, the Inevitable Disclosure Doctrine came into being. While it has been discredited in some state court decisions, it does retain viability in that it would appear to be human nature that a person who has held a very sensitive position in

one entity, who is now going to work for a competitor, will be hard pressed not to disclose trade secret information intrinsic to one's success at work.

Anyone wishing to bring a claim under the Inevitable Disclosure Doctrine has a high burden of proof. The circumstances would seem to require an unusual degree of specialization or unique knowledge, the relationship between the former employer and the new would need to be particularly close, and the impact upon the employee has to be carefully considered in that it cannot simply be a means to prevent employment.

The case of Pepsico Inc. v Redmond, 54 F.3d 1262 (7th Cir. 1995) addressed the Inevitable Disclosure Doctrine and upheld an injunction for a specific type of work that the former employee would have otherwise performed for the new employer. It is interesting that the injunction in this case, and others, has a time limit upon it where, afterwards, presumably the former employee is free to engage in those activities, apparently without trade secret restrictions. In EarthWeb Inc. v. Schlack, 71 Fed.Supp.2d 299 (S.D.N.Y. 1999), remanded 205 F.3d 1322 (2nd Cir. 2000), the court simply looked to the non-compete agreement and, since the non-compete did not cover the circumstance, the court did not want to substitute "inevitable disclosure" for a failed contracting effort. Given the general prohibition against the disclosure of trade secrets, the issues would ordinarily seem to be resolved in that fashion. Trade secret restrictions should assist in the "inevitable disclosure" setting.

Typically in trade secret protection, the former employee is free to engage in any employment activity so long as the trade secrets are not utilized. One would hope that the new employer would be sufficiently creative to avoid this circumstance.

If the inevitable disclosure claim is going to be pursued, it would also appear fair for it to require payment to that enjoined employee. It does appear to give rise to constitutional issues, including prior restraint, and the stronger case is

one in which the Inevitable Disclosure Doctrine has been negotiated in the employment agreement.

E. Infringement Issues - Risk Avoidance, Liability and Loss Mitigation Strategies

The best method of risk avoidance is to first understand the risk. While that may seem obvious, it is not necessarily so. There are certainly occasions when we are unaware that there is a risk, and so have not taken any steps to guard against it.

For example, in hiring an employee from another company, it is not commonplace for that employee to sign forms which represent that there either are no trade secret agreements, or that the employee had no access to any trade secrets that would in any manner relate to the new employment. You may find later that such representations turn out to be untrue or that you have simply not questioned the employee on that topic.

So, the first step in risk prevention is first to recognize those risks which may come to the company. The first is likely to be from new hires, particularly if that employee may be bringing trade secret or other protectable information to the new company and the new company unwittingly incorporates that information.

Second, documenting the rights and responsibilities of employees would appear to be the most common means of risk prevention. Being sensitive to the fact that the company has its own stock in trade, that it does not need to utilize the stock in trade of others, and that the company's stock in trade belongs to the company and not to the employee, need to be part of company culture.

Outside strategy, in terms of websites, advertising, communications with others and new product development, needs to be done with an understanding that it may be advantageous for a competitor to claim infringement. Accordingly, development initiatives should be documented early and great care should be taken that the products developed are indeed those of the company and not rip-offs of

rotected technology. Utilize care in trying to meet a competitor's product or method of operation so that what you utilize is unique to you and not simply a derivation of a competitor's.

With regard to products, consider having an outside review of products before distribution. In licensing that product, consider issues such as remedies, enforcement, limitations of liability, and the nature of the forum.

Do review insurance issues, including advertising injury coverage, and additional endorsements for coverage of your product. If there is a claimed loss, involve your professional advisors in addressing the problem.

If you do receive a claim and it appears to have legitimacy, consider modifying your behavior promptly. If the infringement is unintentional or isolated, consider immediate response and retraction, even if the question is close, so long as it concludes matters rapidly and without embarrassment. Part and parcel of mitigating a loss is having engaged in some prior exercises of potential problem areas and contemplating the best manner of proceeding.

Have a plan in place, both preventive and responsive, so that the actions taken are done in good faith if a claim is received. If there is a close call on a trademark or trade name, document the steps taken to see that, at least in your view, there is no infringement. If there are issues of product infringement, consider offering to have the products reviewed by a third party, with an agreement that the product will be modified if it is seen to indeed be infringing.

Litigation in the technology world may actually be inevitable. That litigation, however, should not be an event which stops the company in its tracks. Maintain some flexibility, a willingness to fix what may be wrong, and a healthy regard for maintaining boundaries between what is yours and what might be theirs. A few copyright cases of interest to illustrate the range of copyright protection and the strategic nature of infringement claims: In Matthew Bender & Co. v. West Publishing Company, 158 F.3d 693 (2nd Cir. 1998) (cert. denied), Matthew Bender was allowed to reprint West decisions even though they utilized the West pagination,

as the West pagination did not embody any original creation. County of Suffolk v. First American Real Estate Solutions, 261 F.3d 179 (2nd Cir. 2001) found that states and state subdivisions may own copyrights. This case found county tax maps to be copyrightable by a county. Greenberg v. National Geographic Society, 244 F.3d 1267 (11th Cir. 2001) held that a digital collection of photographs was more than a republishing of its magazine, and that the digital collection constituted a new product in a new medium. In Gardner v. Nike Inc., 279 F.3d 774 (9th Cir. 2002), Nike granted Sony a license to utilize a Nike created cartoon character in an exclusive license which did not address Sony's (the licensee) right to assign or sublicense to a third party. Sony's assignment to a third party was held to be invalid on the basis that an exclusive license does not imply rights to sub-license. Bouchat v. Baltimore Ravens Inc., 241 F.3d 350 (4th Cir.) cert denied, 532 U.S. 1038 (2001). In this case, an artist sent drawings of a new logo to the stadium authority by fax. The Baltimore Ravens logo appeared to be similar to the plaintiff's drawing. Plaintiff filed a copyright application and brought a lawsuit for infringement. Proof at trial showed that the chairman of the stadium authority shared office space with the team's owner, and the court found that to be sufficient proof of the team's access to the drawings. In denying certiorari, the United States Supreme Court allowed a \$10 million damage award against the Baltimore Ravens to become final.

TECHNOLOGY LAW IN COLORADO:
AN ADVANCED APPROACH
SEMINAR 12/12/03

II. TAKING A CLOSER LOOK AT E-COMMERCE TRANSACTIONS AND
ENFORCEABILITY OF ELECTRONIC AGREEMENTS

Presented by Robert L. Allman, Esq.

TECHNOLOGY LAW IN COLORADO:
AN ADVANCED APPROACH

II. TAKING A CLOSER LOOK AT E-COMMERCE TRANSACTIONS AND
ENFORCEABILITY OF ELECTRONIC AGREEMENTS

A. The How To's of Structuring E-commerce Transactions and
Enforceability of Electronic Agreements (Including Strategic Alliances
and Joint Ventures)

E-commerce transaction agreements can encompass a variety of forms. This outline seeks to look at common forms of transactions, including consumer transactions, and those transactions involving joint ventures and other forms of relationships which the e-commerce vendor may choose in order to expand business.

1. Consumer Issues

When dealing in e-commerce, it is of utmost importance for the website information to be clear, to have legal disclaimers, to include consumer consent, to provide for license terms, return of product rights, privacy protection, and other elements unique to the transaction. The website becomes the contract and each statement made within the website might be considered a representation or warranty.

Presented by Robert L. Allman, Esq.
Allman & Mitzner, LLC
535 16th Street, Suite 727
Denver, Colorado 80202
(303) 293-9393
(303) 293-3130 (fax)
rallman@allman-mitzner.com

From an operational standpoint, the use by a consumer of a website is the fundamental transaction and must be treated appropriately. The dates of changes in websites should be noted and stored so that, in the event of a later dispute, the exact language and look of the website can be duplicated.

Affirmative use by the consumer of the website's abilities to either accept, click "I agree," or other affirmative steps, can only help the company in making sure that the consumer has understood the transaction. Although many websites contain legal issues or a warranty section, the actual purchasing section should require reference to those pages or at least a reference that the consumer knows they are there and has had the opportunity to review them.

The website has legal effect likely greater than an oral contract and less than a custom written contract, but it is a form of contract nonetheless. The agreement should be clear, be written in plain language and, with the use of color, important points can be highlighted. Affirmative acceptance of terms has become an accepted prerequisite for website agreements. The more obvious the nature and details of the transaction, the more the website contract will be enforced.

Case of interest: Click wrap and similar forms of licensing should provide for an affirmative acceptance and clear notification to the consumer. Specht v. Netscape Communications Corp., 306 F.3d 17 (2nd Cir. 2002) found consumer consent to be sufficiently obvious. Consideration should be given to any warranty contained in any license, particularly with limitation of remedy issues and time constraints on any claims. Disclaimers of warranty should be carefully worded and addressed to the specific nature of the software.

2. Strategic Alliance / Joint Venture

Strategic alliances and joint ventures are common in e-commerce settings. One problem that may arise in the e-commerce setting is that there may be a lack of documentation as to the nature of the strategic alliance or joint venture. Although the strategic alliance agreement will ordinarily state that the parties are not engaged in a joint venture, the impact between the participants may be relatively

the same regardless of the form taken. The joint venture is a short term or limited purpose partnership, and the parties are presumably working a little more closely together than with a strategic alliance. The strategic alliance tends to put together parties with slightly diverse but complementary products or services, where it is hoped that the combination will produce a synergy or demand where the sum is greater than its parts.

Strategic alliance is a more commonly encountered business transaction in e-commerce, and may be the trickiest. The issue is really that of having the parties outline not only what they intend to accomplish, but also what they are willing to do for the other. So, rules to follow for strategic alliances - (1) take care in determining what each strategic partner is to accomplish, including what each will not do or say; (2) do not confuse customers that they are dealing with one and the same company, make it clear that the customer has the advantage of being part of a team, but the entities are separate; (3) in combined website marketing or references, describe the entities in a way that makes it clear that they are separate but assisting each other.

Consider methods of terminating the strategic alliance or set a time for its running its course; have a formula for sharing revenues generated by the strategic alliance, or have a system of payments established which encourages each strategic alliance member to utilize the services of the other.

Having an agreement which keeps the parties' trade secrets protected, clearly identifies each party's respective intellectual property, protects key customers, and allows for a transition in the event the alliance is dissolved is very useful. Consider the circumstances in which indemnity may be called for, and address those in advance.

Limit hiring of one party's employees by another, and consider limitations on competition. Address some simplified remedies in the event of a party's failure to perform, even if the remedy is simply dissolving the strategic

alliance. Consider whether the strategic alliance will burn any bridges in any related business communities, and attempt to mitigate negative results.

As is obvious from the statements above, the key for strategic alliance is to outline the relationship between the parties, and how they shall act as to each other both during and after the alliance. Identify those areas in which joint effort will be undertaken, and protect each participant's assets from infringement by the other.

It is probably useful to perform some due diligence on any strategic alliance partner, including business reputation, existing or potential lawsuits, standing in the business community, and whether the alliance partner would appear to still be a good one if all of your company's dreams come true within the next five years.

B. Software Transactions and the Uniform Computer Information Transactions Act (UCITA)

The concepts of UCITA should likely be followed by participants in this industry, if only because it does provide a uniform method for electronic transactions, and it does provide the opportunity for a court, when faced with little precedent, to look to UCITA for guidance.

UCITA was intended as a form of Uniform Commercial Code for technology transactions. It has recently been rejected by several states and its future is unclear. A primary purpose was to allow for the approval of click wrap or standard forms of licensing, and does require an acceptance by the consumer. The general concepts appear to be relatively established, but the warranty limitations are troublesome for consumer advocates. For example, in Kilcek v. Gateway Inc., 104 Fed.Supp.2d 1332 (D. Kansas 2000), the court held that UCITA would not apply to a hardware transaction because it is intended to apply to the sale of computer programs and copies, but not to a sale of the computer, providing a common sense result for a consumer claim.

While consumers may argue that UCITA takes away many of their rights, such as by strict enforcement of shrink wrap and click wrap agreements, much of what is contained within the Act is common sense and does apply a type of Uniform Commercial Code attitude to e-commerce transactions.

C. Examining the Relationship Between the Uniform Electronic Transactions Act (UETA) and E-Sign

The Uniform Electronic Transactions Act (UETA) was developed in 1999 as part of the development of uniform state laws. It sets forth procedural requirements, and is not intended to change the substantive rules of contracts. It essentially grants the same legal force and effect to electronic records and signatures as it does to paper records and handwritten signatures. Approximately 40 states have enacted it. Under UETA, the click acceptance of “I agree” creates a contract. The Electronic Signatures in Global and National Commerce Act (ESIGN) was also intended to assist in electronic commerce. It is intended to allow electronic signatures used in an electronic transaction the same legal effect as an ordinary signature.

UETA and e-sign are efforts at solving a common problem. The issue is really that of being able to document an accurate signature and/or verification of same. The use of faxed signatures, faxed legal documents, and electronic filing of legal documents, have all contributed to a general acceptance that e-signing will become of common usage. Issues may still arise in areas where a signature would appear to be necessary and those, such as internet credit card transactions, where it may not be. Where bill paying and banking have become commonly done in electronic format, fair results should not be a great technological or legal leap.

Under any circumstances, where a party reasonably relies upon an electronic signature or some form of e-signing, there is no reason to expect that promissory estoppel could not be utilized to avoid fraud or other unfair practice.

D. Jurisdictional Issues in Cyberspace

1. Emerging Case Law Interpreting Jurisdiction

It should be noted that any issue of jurisdiction in cyberspace does need to follow ordinary concepts of jurisdiction. That is, if in personam jurisdiction is required, then some affirmative act or course of conduct or significant contacts within the jurisdiction is ordinarily required. Every state's long arm jurisdiction statute does require some form of transaction of business or other conduct within the state, unless there is an agreement as to venue.

It is unclear whether click-on agreements as to venue would be necessarily enforceable, although one has to believe that as web-based business becomes more prevalent, courts would likely find that, given relative sophistication of website users, such agreements would be enforceable.

It seems obvious that operating a website within your home state utilizing a corporation based within that state will confer that state's jurisdiction. However, the mere presence of a party on the web is not sufficient to confer jurisdiction under a minimum context text. Zippo Manufacturing Company v. Zippo dot com, 952 Fed.Supp. 1119 (W.D. Penn. 1997).

If what is required is in rem jurisdiction only, that is, a form of jurisdiction over property - for example, disputes over a property right such as a domain name, may be brought under the Anti-Cybersquatting Consumer Protection Act (ACCPA), with minimum jurisdictional contacts. The ACCPA does allow for in rem jurisdiction by the providing of notice if personal jurisdiction is not able to be obtained by service, and also an action may be brought in the jurisdiction of the registrar of the domain name. It has been held that an in rem action must be brought in the jurisdiction where the domain name registry is located. Fleet Bosten Financial Corp. V. Fleet Boston Fin.com, 138 Fed.Supp.2d 121 (D. Mass. 2001). This issue comes up in the cybersquatting context if the entity or individual responsible for the conduct is not able to be located for personal service. Foreign judgments

have also been recognized, but they will be required to comply with United States law. Yahoo, Inc. v. La Ligue Contre, 169 Fed.Supp. 21,11,81 (N.D. Cal. 2001).

The tension lies in determining how traditional the contacts need to be within the jurisdiction in order for personal jurisdiction to ensue. The basic test of whether one is transacting business within the state or has some form of continuing contacts beyond mere incidental contacts have long been jurisdictional issues. The website may be considered to be akin to a national publication (Heart Corp. v. Goldberger, 96 Civ. 3620 (S.D.N.Y. February 26, 1997)). In Hall v. LaRonde, Cal.App.4th 1342 (1997), the California state court found that email communications may form the basis for the assertion of jurisdiction. In Compuserve, Inc. v. Patterson, 89 Fed.3d 1257 (6th Cir. 1996), the Sixth Circuit found that Ohio had jurisdiction over a Texas resident who had entered into a contract with Compuserve, where the contract was simply done electronically. The issue of whether email can be jurisdictional is certainly of interest, and if containing slanderous or defamatory materials, it is hard to imagine that it would not provide the basis for jurisdiction.

2. Can Non-Compete Clauses be Effectively Enforced?

Enforcing non-compete agreements, which are traditionally supposed to have geographic limitations, are troublesome when commerce is national and/or international in scope. The general rule of enforcement is that the restriction must be reasonable given the competitive activity. A trend in non-competes is to identify customers or areas of competition which may be of national or international scope, but doing so while leaving open competition for those entities or activities not specifically named. This may be particularly effective for the enforceability of non-competes signed by lesser managerial employees, for example.

Another enforcement problem is whether non-compete agreements are really effective in an electronic economy, where it is difficult, at times, to even find the proponents of the offending electronic material, and where the use of offshore companies is prevalent.

What is the future of non-compete agreements? They will be with us for a long time. The geographic restrictions will increasingly become less important and defining areas of competition by customer or context will become the norm.

TECHNOLOGY LAW IN COLORADO:
AN ADVANCED APPROACH
SEMINAR 12/12/03

IV. UNDERSTANDING OPEN SOURCE LICENSING
Presented by Robert L. Allman, Esq.

TECHNOLOGY LAW IN COLORADO:
AN ADVANCED APPROACH

IV. UNDERSTANDING OPEN SOURCE LICENSING

A. Intellectual Property Protection and Licensing Concerns

Open source licensing has revolutionized the development of software products. Championed and brought into the mainstream by Netscape, Linux and others, it enables developers to utilize common software building elements and, at least in theory, to have a common language of communication and collaboration. It has, however, produced concerns regarding commercial use of the open source license where the license interacts with privately developed software.

Although there are a variety of open source code licenses, some are truly open and require little discussion, as they allow the user any use, and impose no restrictions. Commonly used is the GNU General Public License, also referenced as the GPL. The manner in which the proprietary program connects to the open source is significant in any business strategy contemplating open source usage. In the GPL or GNU format, determine the nature of the connection, that is, are the new program and the open source essentially one program, or is the new program not dependent on open source. Under the GPL concept, a “separate work” is not subject to any GPL or GNU license requirements, so “separateness” is essential to protect proprietary code. In addition, if the the proprietary program does

Presented by Robert L. Allman, Esq.
Allman & Mitzner, LLC
535 16th Street, Suite 727
Denver, Colorado 80202
(303) 293-9393
(303) 293-3130 (fax)
rallman@allman-mitzner.com

not use any open source code and is not derived from the open source, then it may also be seen as distinct. The Lesser General Public License (LGPL) might be used to minimize or avoid the connectivity problem between the proprietary and open source programs so that the proprietary program does not become subject to the open source requirements.

The method of connection must be carefully considered and must embody the concept of being a separate work, not a derivative work. Unfortunately, the issues have not been clarified by court decision. In Progress Software Corp. v. My Sqlab, 195 Fed.Supp.2d 328 (D.Mass 2002), the issues of proprietary programs interfacing with a GPL open source program could have been addressed, but matters were resolved without a precedent decision.

Under any circumstances when using a software license or licensing a software product, a key concern is that the license specify the nature, scope and use of the product. It is important for the license to specify the extent of sublicensing or other business transactions that may or may not be contemplated within the context of the license.

A typical software license is going to carefully delineate the actual software licensed, whether it includes updates, the basis for payment of royalties, the term of the license, and enforcement issues. The open source license adds a new element to licensing concerns in that the open source license is intended to mean just that.

Open source may mean that it is freely available, or it may mean that any changes that one makes to the software which is subject to the open license are to be provided to the open source entity and made available for others to use. It is generally intended to be communal and collaborative. However, as with any license, it is subject to its own terms.

The open source license typically will provide that if you then license this open source program or any modifications which you have made to it, to another for fees, then the royalties received must be paid to the open source entity. That

might not fit the business development model for the company, and unless the company's business model is purely service oriented, it would otherwise provide a disincentive to utilize open source licensing.

Structuring the license for a software product utilizing open source product requires careful consideration of the pricing and method of licensing of that product to a paying customer.

Typically, the license of product is only for that proprietary product which is developed by the company, which interacts with the open source license, but has not modified the software nor utilized it except as an independent platform.

The customer, in utilizing the open source, can download its version of the same open source, and the company's services are to install an interface to that open source, charging a fee for the installation service and the proprietary software which properly belongs to the company, and related services.

In general terms, care should be exercised in not melding the two, so that the privately developed company software is a stand-alone product which then works upon the open source product simply as a form of operating system. Passing off of the open source as one's own is not allowed, and would trigger the royalty payment obligations and possible other penalties under most, but not all, open source licenses.

B. Open Source Code - What Are the Legal Risks?

The legal risks for open source code are touched on above, and they are primarily those contained within the open source license. As with any other product, in accepting the open source, one accepts the licensing terms. It may be difficult, depending on the development process, to recognize that which is open source and which is privately developed and, if so, the entire product might be seen to be open source under the terms of the open source license.

While certain open source entities may be less bent on enforcement than others, any use of open source licensing requires a careful delineation between

that which is truly open source and that which is proprietary. A company audit of intellectual property might include whether open source licenses are applicable and whether they have been complied with, and/or whether the privately developed standalone products have remained sufficiently “stand alone.”

Because this type of software building has become more prevalent, programmers have become more adept at this component style approach. It may assist the company, however, to have this approach reviewed by an outsider and to make certain that any updates or changes to the licenses be reviewed. This could be part of a due diligence investigation.

The good side to open source is that it expedites and economizes development. It also provides for an increasing potential for interactivity between software and operating systems of all sorts. Among its virtues is that it can inspire the building of products that otherwise would have been too expensive for an individual or a small group to undertake.

The author of the open source may want some form of recognition and/or compensation, if only to keep the open source fresh and innovative. However, there needs to be a documented delineation between the open source that may be being provided to a customer at no charge, and the proprietary component for which there will be a charge. A process for making sure that the open source software is being properly licensed or transferred to a non-paying customer is key.

The open source licenses are available online. They can and should be reviewed and updated. When engaging in an independent software development project, the use of open source should be discussed, and rules of engagement with open source created. In simple terms, the first rule is likely to be that the open source will not be modified and that any add-ons will be independent product and not derivative products from the open source. This is a good area where business, legal and technical personnel need to have an involvement and understanding of the software development process.

C. Practical Tips for Representing Open Source Clients

Any client that either develops open source products or utilizes same needs to have rules of engagement. From the standpoint of the developer, the rules of engagement are set forth in the software license, and for the user, the rules of engagement are when and how to use the software license, and a review of the license itself.

There are a variety of open source products. If you are a developer and you wish to use the open source to speed up the development of your product, take care that you are not simply creating an imitation of that open source. It is intended to be used as a tool, and your own product should be separately functional. Perhaps it can be utilized with other open source products and its functionality is self-contained. Open source was not intended to provide a free way for companies to make money with little effort.

The pure open source client does need to have a feel good attitude about making product available at no cost. It may also have a business plan to derive income from services or related products. Open source might be a “loss leader” and a method of opening customer’s doors.

D. How Does Open Source Licensing Affect Mergers or Company Policies?

The unwitting merger participant which begins to utilize software without realizing that it is primarily open source, and does so in a commercial setting, could find itself very unhappy. Any merger will likely have a lengthy due diligence process and, within that process, an analysis of the proprietary software and/or use of open source is appropriate.

Similarly, company policy should outline the steps and procedures to utilize when engaging an open source license. The terms of the open source should be reviewed by technical and legal personnel.

Falsely placing copyright or even seeking patent protection on products utilizing open source could prove embarrassing and expensive. The concept of open

source, as it has become more prevalent, will and has impacted due diligence in the software world. Open source provides remarkable tools, reflecting the flexibility and potential of the software industry.

TECHNOLOGY LAW IN COLORADO:
AN ADVANCED APPROACH
SEMINAR 12/12/03

VII. HOT TOPICS IN COMPUTER AND INTERNET LAW
Presented by Robert L. Allman, Esq.

TECHNOLOGY LAW IN COLORADO:
AN ADVANCED APPROACH

VII. HOT TOPICS IN COMPUTER AND INTERNET LAW

A. Digital Millennium Copyright Act (DMCA) Prohibitions on Reverse Engineering and Anticircumvention

The Digital Millennium Copyright Act (DMCA) prohibits circumvention procedures which would otherwise allow a user to avoid copying or circumventing a work such as by decrypting, descrambling, or other method of bypassing a technological protection on a copyrighted work. It is also intended to prohibit manufacture or distribution of software or other technology that is intended to circumvent. Reverse engineering is not authorized if its intent is to facilitate prohibited circumvention.

The DMCA also provides for remedies and rules regarding internet service providers and copyright owners who may be subject to claims of infringement. There is a safe harbor provided under certain circumstances where the service provider is not an active or knowing participant in the infringement. These defenses include circumstances where the transmission is made by a third person other than the ISP, the transmission is done automatically without intervention by the service provider, the service provider is not taking action to select the recipients, the copies are not maintained by the service provider, and the

Presented by Robert L. Allman, Esq.
Allman & Mitzner, LLC
535 16th Street, Suite 727
Denver, Colorado 80202
(303) 293-9393
(303) 293-3130 (fax)
rallman@allman-mitzner.com

service provider is not modifying content. The service provider does have to designate an agent for receiving notices of claims in order to take advantage of the safe harbor provisions.

The DMCA also addresses protection where the service provider has unwittingly stored materials which may constitute copyright infringement. The concepts of DMCA are based upon punishing knowing behavior, and exempting certain forms of unintentional violations. In ALS Scan Inc. v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001), the defendant website owner failed to respond to a demand to remove infringing materials, and could not rely upon a claimed defective notice for its failure to act. In Universal City Studios v. Corley, 273 F.3d 429 (2nd Cir. 2001), Universal prevented the distribution of circumvention software and also held that this did not violate the First Amendment.

B. The Use of Litigation to Prevent Trespassing and Spam - Is It an Effective Deterrent?

The trespassers and spam artists will continue to be among us so long as they remain anonymous, hard to reach, and otherwise judgment proof. Absent technological change in the manner of blocking these intrusions, the freedom of the internet favors the spammers. Litigation can be extremely effective if the offending party is known, has assets, and is actually engaged in business. Such a defendant is not a moving target, and litigation can be worthwhile.

It is suggested that in litigation, including injunctive relief, individuals be named who have participated in these ventures so that it is not merely the company that is enjoined, so that the principal players, particularly technology employees, must participate in the action.

On a slightly different level, but also related, are those spammers or hackers who are disgruntled former employees. If they can be identified with particularity and, even if judgment proof, a strong deterrent can be made with appropriate injunctive remedies.

Colorado's Anti-Spam Act is an interesting approach, but it is not frequently utilized and, absent possessing a significant number of email offenses, a single individual is not inspired to bring the claim. Treaties with those countries hosting offshore spammers, and making the companies who benefit by the spam liable for the spam, may be a good start, but the answer would still seem to lie with technological development and possibly a more intuitive method to block unwanted messages.

C. Should Networks be Allowed to Filter Content?

This issue of network filtering would seem to depend upon the extent of the network, and the nature of the communication. If we are considering ISP providers in a general sense dealing with public subscribers, the rules of filtering, as long as they are clearly stated, would seem to be acceptable.

If it is a library system, one gets into first amendment issues of interest, but ones which may have certain practical solutions based upon the age of the user and simply the setting of rules of conduct within the library system. In the workplace, there can be little doubt but that network filtering is accepted and the rules effectively conveyed to the employees.

The conflict involves the freedom to communicate and under what circumstances it may be limited. While we may have societal norms, these may not always coincide with constitutional protection. It would seem to be difficult and not fruitful to produce some sort of uniform law in this area.

Given the prevalence of computers and online access in other settings, it is difficult to believe that schools, libraries, and other public institutions should be required to provide any particular or pre-defined level of internet access.

D. Communications Torts Online - Who is Liable?

Ordinarily, the innocent ISP or website is not going to be responsible for a communication tort such as defamation. If the website is simply passing on information that it receives then, like a news publishing source, there must

ordinarily be an element of willful intent or malice. Where an individual proceeds to utilize emails or other forms of communication in order to defame another, there would seem to be no reason not to enforce the ordinary defamation rules against that individual. Absent affirmative assistance or ratification by the ISP, there is little basis to impose liability.

The problem becomes that of policing by the ISP and the extent to which it needs to go to verify accurate information. Appropriate disclaimers are helpful to the ISP or website, but there can certainly be concerns with repeat offenders, and a failure to rectify obvious errors.

From the litigation standpoint, a plaintiff's attorney may well want to bring a claim against the larger entity rather than being limited to its remedies against an individual defendant. Enforcement issues will evolve as websites and digital communication become more sophisticated, and the innocent re-publishing defense will be weakened.

The future of computer and internet law will continue to combine traditional legal concepts with the demands of new technology, taking into account the societal need for advancement, prosperity and security.