INTELLECTUAL PROPERTY AND SOFTWARE AUDITS

Susan E. Colman

1. Introduction

There is a classic cartoon in *The New Yorker* magazine published, in fact, on December 8, 1928, which provides us perhaps with the most scintillating view of intellectual property audits from the perspective of business owners. Mother and young daughter are seated at the dinner table with plates of food before them. The mother says: "It's broccoli, dear." The young tyke snarls out in response: "I say it's spinach, and I say the hell with it."

It appears to be axiomatic that the more often we are offered opportunities to protect ourselves and our businesses, those things that, like broccoli and spinach, are "good for us," the more often we dig in our heels and try to resist them. This resistance can emanate from any number of circumstances, not the least of which is immediate cost and continuing cost over time. And, there is always the time-worn mantra offered up as an excuse: "We've not yet been on the receiving end of any complaints, so we must be doing something right – why stir up a hornet's nest?"

Well, the hornet's nest can be stirred up at a moment's notice, and the stings which result can cost businesses far more than it would cost to protect themselves in advance, and indeed, far more than they could ever imagine. The legal process is fraught with a combination of objectivity and subjectivity. Even on a good day, when the law and the facts are resolutely on your side, you may still not get what you want, and the entire process itself will be very expensive.

Therefore, it is incumbent upon businesses and their legal advisors to pay very close attention not only to determining what intellectual and proprietary property they have in their possession, but also to who actually owns it, if it can be protected on both a national and worldwide basis and what offensive and defensive measures can be taken to assure that a business has done all it can to keep itself in business and be competitive. But merely paying attention to this is not enough. Successful

businesses must do more than that. They must establish programs throughout their companies which will identify and monitor intellectual property at every single stage of every single project they have. Businesses must indeed go back to the walls in the cave – all the way from project definition, to project development, to project implementation – manifested on the inside in intellectual property identification and ongoing protection, and on the outside in strong, truly protective license agreements. This is the definition of proactive asset management, and it is key to the success of any business.

This paper will set forth the particularities and peculiarities of the primary components of intellectual property and the offensive and defensive postures which companies might take to protect themselves. It will also assist companies in looking at computer software in a way which may allow them to stand on firmer ground, whether that software is home-grown or is brought in from the outside. Furthermore, and particularly in the software area, if a company is a systems integrator, there are even more challenges in regard to intellectual property protection. This paper will also explore proactive approaches companies should consider with respect to protection of their intellectual property, and proactive approaches to take if they potentially might be on the receiving end of a legal challenge by others. Proactive approaches in this way might allow companies to perhaps mitigate or otherwise avoid altogether costly and uncertain litigation.

Please be aware that this presentation will have a focus on the United States legal system. Nevertheless, companies currently doing business globally or those which are intending to do so should already be practicing the art of juggling more than one legal system, in order to protect themselves to as high a degree as possible.

2. The basics

The basic components of intellectual property are patents, copyrights, trademarks (which must now include domain names) and trade secrets. The only one of these which has a strict statutory basis is patent protection. While copyright protection has a statutory basis, the enforcement of copyrights in the United States relies on a formal scheme not used in the rest of the world. Trademark protection has both a statutory and common law basis. Trade secret protection has a basis purely in common law, and its enforcement is strictly governed by contract.

We shall take each of these components at a time. Some of this discussion will also take into account the business models created in response to the tremendous growth in e-commerce due to the Internet. It is additionally important to understand at this juncture that to obtain or not to obtain legal protection for any intellectual or proprietary property a company may have is purely a business decision, and can be proactive in itself. But that business decision can have profound implications for the ongoing health and competitive edge a company needs in an electronic and aggressive global marketplace.

2.1 Patents

Patents protect ideas. For a certain, fixed period of time the holder of a registered patent exercises a monopoly. And this is a *negative* monopoly. That is, the rightful owner of a patent can *exclude* all others from making, using or selling the invention protected under the patent. To this extent, however, obtaining a patent for an invention is much more difficult than obtaining copyright or trademark protection, even if the latter two protect much different things.

In the United States, patents have been issued increasingly for computer software and even business methods. Outside the United States, patent protection for software is a bit more difficult to obtain, as typically it must be claimed in express conjunction with an actual, physical apparatus. In fact, just recently the European Union refused to entertain the notion of accepting patent protection for software as such. Nevertheless, the European Patent Office will still grant software patents in spite of the failure of that proposal to harmonize the patent laws across the EU. In the United States, software patents can stand on their own so long as the stringent requirements for patent protection generally are met. Business method patents appear to remain a U.S. phenomenon.

The patentability, at least in the United States, of software and business methods is important for those involved in the creation or vendor end of e-commerce. Because it may be relatively easy to reverse engineer Internet technologies, patent protection will be more easily enforceable and, indeed, enforced, than trade secret protection (which will be discussed later in this article).

It is vitally important to pay attention to the "nuts and bolts" of patent protection, and to distinguish the requirements between the United States and the rest of the world. The United States is the only country in which an inventor has *one year* from the date of *disclosure* of the invention, *public use* of the invention or *sale* or *offer of sale* of the invention, during which to file a patent application in the U.S. Patent and Trade-

mark Office. When that one-year period expires, the patent rights are deemed waived if no application is filed. But in the rest of the world, there is no so-called "grace period." Instead, there is what is known as *absolute novelty*. That means if there is publication of or about the invention anywhere in the world prior to filing an application, any and all patent rights have vanished. Furthermore, since most patent offices outside the United States publish patent applications 18 months after filing such publication may very well trigger the start of the one-year period in the U.S. during which an application must be filed.

As of this writing, the proposed changes to the U.S. patent law includes a 9-month post-grant opposition period during which others may submit evidence of any kind to the U.S. Patent and Trademark Office (PTO) to traverse the granting of the patent. The Federal Rules of Evidence apply and the standard of proof is by "preponderance of the evidence," the lowest standard available. In federal court, however, the standard of proof rises to "clear and convincing" evidence, which can be much more difficult to sustain.

Patents generally, wherever in the world they may be filed, are typically very expensive to obtain and to maintain. Certainly, they constitute valuable assets, and revenue can be generated by means of licenses and infringement litigation, although the latter can be problematic. Since litigation, at least in the United States, tends to be extremely expensive and equally time consuming, an infringement case must by necessity be very strong, or it may not be worth the financial while to go forward with such a lawsuit. But, clearly, patents may be used offensively to limit competition (remember, it's a *negative* monopoly). If used in this way, however, other brave souls out there may very well be aggressive right back, and challenge the integrity of the patent itself. More than one patent over the past century have been revoked.

A patent in the United States is governed exclusively under federal law. There are no laws among the 50 states which govern patents, although contracts and licenses involving patents would fall under state law. Both patents and copyrights have their origins in the U.S. Constitution, where in Article I, § 8, cl.8 is granted to Congress the power "*[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries. . . .*" In other words, the Constitution limits Congress from issuing patents which would essentially remove existent knowledge from the public domain or to restrict free access to already available materials.[1] The limited monopoly provided by patents acts as

[1] Graham v. John Deere Co., 383 U.S. 1 (1966).

an incentive to continued innovation and thereby to investors to take on risks of the considerable costs attendant to the time, research and development of innovation.[2]

If the inventor doesn't want to disclose his or her invention to obtain a limited monopoly, the only recourse is to keep the invention secret as a trade secret. Trade secrets, as will be discussed later, can be pretty powerful protection. But a trade secret is vulnerable to disclosure and reverse engineering. Once the secret is no longer secret, the protection is lost.

Who can file for a patent? In the currently proposed changes to the patent law, the United States is to join the rest of the world in allowing the *first to file*, rather than the first to invent, as had been the case since the original patent laws came into effect. This means that, while previously in the U.S. it was the date of conception of the invention which took priority, it will now be the actual date of filing the application which governs.

The duration of a patent is generally 20 years from the date of application (the first application if there is more than one for an invention). There are statutory exceptions to this, however. Patents which were issued on or before June 8, 1995 typically will expire 17 years from the date the patent was issued *or* 20 years from the date of filing, whichever is longer.[3]

Under U.S. law, an invention or discovery of "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof…"[4] can be patentable subject matter. It must be original and inventive. In addition, there is the requirement of non-obviousness, and the invention must have utility (*i.e.*, it must be useful).

What about computer software? Jurisprudence in the United States over the past 20 years has evolved from treating mathematical algorithms as a part of the "laws of nature" to changing the analysis so as to look at the entirety of the patent claims by the time the 1990s came around. It would appear that purely mathematical software applications would not be considered patentable subject matter. A very important case in the Court of Appeals for the Federal Circuit established that software-related inventions would be unpatentable only to the extent that they represent "merely abstract ideas constituting disembodied concepts or truths that are not 'useful.'"[5] However, when an algorithm is

[2] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974).
[3] 35 U.S.C. § 154(c)(1).
[4] 35 U.S.C. § 101.
[5] State Street Bank & Trust Co. v. Signature Financial Group, Inc., 149 F3d 1368 (Fed. Cir. 1998), cert. denied, 525 U.S. 1093 (1999).

applied in a "useful way" a software invention may indeed be patentable. Even if an underlying algorithm might not be protectable, a computer program using that algorithm might be.

In the United States today utility patents (as opposed to design patents) may issue, where all the statutory criteria are met, for: (1) the underlying process or steps performed by the computer program; (2) the hardware on which a software program is run (as an apparatus or a system); and (3) an article of manufacture (where, for example, software is distributed on a CD-ROM). Design patents may also issue for the ornamental design of a software program. The U.S. Patent and Trademark Office (PTO) issued new guidelines in 1996 for patent examiners, specifically directed to facilitate an increased issuance of patents for software.[6]

The *State Street* case actually did more to shake up the patent world when it allowed for a more flexible approach to software as patentable subject matter. What it did was pave the way for the patentability of *business models*. In that case, the invention at issue was a data processing system which permitted an administrator to monitor and record financial information flows (for example, daily asset allocations, income, expenses and related information) and allowed for several mutual funds to pool their resources. As a result of that case, methods for conducting business online are potentially patentable.

Regardless of whether or not e-commerce related inventions can be patentable subject matter, in order to actually obtain a patent, the requirements of novelty and non-obviousness must be fulfilled. There can be no "anticipation" of the invention elsewhere. It cannot be known or used by others in the United States, or patented or described in a printed publication anywhere in the world. This is "prior art" and is a question of fact in the examination process at the Patent Office once an application is filed. Needless to say, the drafting of a patent application should take into account the prior art available, if only to distinguish the immediate invention from all those which came before it. Each element of the invention, as claimed in the application, would need to be found in a single prior art reference for the patent to be found invalid for purposes of anticipation. However, if all prior art is knowingly not disclosed in a patent application, this could trigger sanctions for the applicant and/or applicant's attorney, in the form of the ultimate patent's being deemed unenforceable and the granting of attorney's fees to the other side in a litigation action. Not only that, but for a publicly traded com-

[6] See U.S. Patent & Trademark Office, Examination Guidelines for Computer-related Inventions (Feb. 1996).

pany, such bad faith activity could very well invoke the punitive sanctions of the Public Company Accounting Reform and Investor Protection Act of 2002 (also known as the Sarbanes-Oxley Act) in the United States.

Elsewhere in the world, as mentioned earlier, there is a requirement for *absolute novelty*. It essentially means that if the invention is breathed on, the inventor may be out of luck. Therefore, it is crucial that an invention be kept under wraps until such time at least that an application is filed. It is very important to take into account in this regard the actual process of reducing the invention to practice, and to take further legal steps to obtain more extensive protection in the form of non-disclosure agreements (NDAs) when approaching third parties to, for example, develop or manufacture the invention. This is especially true when universities are used for this purpose. Universities, almost by definition, are publishing machines – it's how they receive grants for further research. An NDA with a strict prohibition against publishing *anything* about the invention is too important to ignore. Once it sees the light of day, any patent rights can be seen flying away into the sky, like birds on migration, never to return (these birds *never* return!). And only those persons with a "need to know" the essentials of the invention should have access to it. An actual inventor does not want someone else filing for the invention in front of him or her.

Non-obviousness is another requirement for obtaining a patent. Obviousness is defined in the U.S. Patent Law as where ". . .the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains."[7] Merely insubstantial improvements will not be sufficient to fulfill this requirement. Commercial success, however, certainly plays a part in the analysis, although it still may not be a prevailing argument in court.

Finally, the invention must have utility to some degree ("a useful invention"). The Supreme Court put it very well: "A patent is not a hunting license. It is not a reward for the search, but compensation for its successful conclusion."[8]

[7] 35 U.S.C. § 103.

[8] Brenner v. Manson, 383 U.S. 519 (1966).

2.2 Copyrights

While patents protect ideas, copyrights protect the *expression* of an idea. It is a much different kind of protection and has a longer duration.[9] Under patent law, because the patent holder can prevent anyone else from making, using or selling the invention, the lack of access to or knowledge of the invention at any time cannot be used as a defense in an infringement action. Under copyright, however, independent creation of a copyrightable work can always be used as a defense.

In accordance with the U.S. Copyright Act[10] copyright protection attaches upon the fixation of an original work of authorship in any tangible medium of expression, whether currently known or developed in the future. Such fixation must be capable of being perceived, reproduced or otherwise communicated, either directly or with the assistance of a machine or device.[11] There are 8 different categories of copyrightable works: (1) literary works; (2) musical works, including any accompanying words; (3) dramatic works, including any accompanying music; (4) pantomimes and choreographic works; (5) pictorial, graphic and sculptural works; (6) motion pictures and other audiovisual works; (7) sound recordings; and (8) architectural works.[12]

The Copyright Act also strictly defines what is not a copyrightable work: "In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work."[13]

The U.S. Copyright Act endows the owner of a copyright with six *exclusive rights*: "(1) to reproduce the copyrighted work in copies or phonorecords; (2) to prepare derivative works based upon the copyrighted work; (3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease or lending; (4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly; (5) in the case of literary,

[9] For works created on or after January 1, 1978, the duration of copyright protection for an individual is for the life of the author plus 70 years after the author's death; for anonymous or pseudonymous works, or works made for hire, the term of duration is for 95 years from the year of first publication, or a term of 120 years from the year of its creation, whichever comes first. 17 U.S.C. § 302.

[10] 17 U.S.C. §101 et seq.

[11] Id. at §102(a).

[12] Id.

[13] Id. at §102(b).

musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and (6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission."[14]

In the Internet world, there may be an overlapping of rights as set forth in §106 of the U.S. Copyright Act. The copyright owner has exclusive rights to reproduce his or her work(s). The actual act of posting on a web site or electronic bulletin board may very well constitute a reproduction. But it may also be considered a distribution, a public performance or a public display. Courts have been, of course, inconsistent in this area, and much of infringing activity as to §106 rights represent issues of fact.

As for ownership of a copyright, especially in the business world, it actually depends on a number of factors. The U.S. Copyright Act defines a "work made for hire" as: (1) a work prepared by an employee within the scope of his or her employment; or (2) a work specially ordered or commissioned for use as a contribution to a collective work, as a part of a motion picture or other audiovisual work, as a translation, as a supplementary work, as a compilation, as an instructional text, as a test, as answer material for a test, or as an atlas, if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire. For the purpose of the foregoing sentence, a 'supplementary work' is a work prepared for publication as a secondary adjunct to a work by another author for the purpose of introducing, concluding, illustrating, explaining, revising, commenting upon, or assisting in the use of the other work, such as forewords, afterwords, pictorial illustrations, maps, charts, tables, editorial notes, musical arrangements, answer material for tests, bibliographies, appendixes, and indexes, and an 'instructional text' is a literary, pictorial, or graphic work prepared for publication and with the purpose of use in systematic instructional activities."[15] This means that unless there is a written instrument to the contrary, an independent contractor holds all rights and ownership to the work he or she created. All companies should definitely take notice of this, particularly if they use an independent contractor to create a web site (or, indeed, anything else), which many companies do nowadays.[16]

[14] Id. at §106.
[15] Id. at § 101.
[16] See also, CCNV v. Reid, 490 U.S. 730 (1989). This is a U.S. Supreme Court case which specifically set forth the criteria for determining whether someone is an employee or an independent contractor for copyright purposes.

Most of the countries in the world are signatories to the Berne Convention or the Universal Copyright Convention. This generally means that copyrightable works originating in one member country are enforceable in the other member countries. That being said, there remains the doctrine of *national treatment*, whereby the standard of enforceability is dictated by the laws of the country where the enforcement shall take place. Thus, to a great extent, copyright protection in the global universe may remain at the mercy of the legal idiosyncrasies in place outside the country of origin. This is an important issue for companies to consider, particularly in the area of software protection.

One of the other key issues arising out of the *national treatment* discussion, and related to the enforceability of a copyrightable work, is the one of *original work of authorship*. It is the position of the United States Copyright Act that an original work of authorship strictly means that the author is the author – that is, nobody else originated the work. In other countries, however, the term "original" requires a subjective analysis of essentially whether the work is "good enough" to be protected, and measures a level of creativity not existing under U.S. law. The question remains: Who, or what judicial body, is to pass such judgment? What any two or more people deem to be "good enough" is likely to be all over the map, based on individual tastes and cultural experiences, not to mention, perhaps, political or social agendas. A copyright owner outside the United States can very well be in for a rude awakening.

In order to prove copyright infringement under U.S. law, the plaintiff must prove ownership of the copyright and copying by someone else. Copying must further be proven by showing access to the copyrighted work and substantial similarity to the original work. It is through this template that all companies, particularly those engaging in the creation or integration of computer software, must pass their employees or independent contractors. This is because computer programmers tend not to stay in one place for very long, and they also tend to take with them, at least in their heads, what they have worked on throughout their careers. A strict vetting process must take place by companies wishing to employ (or contract with) programmers to perhaps be in a better position to avoid potentially infringing situations.

Copyright protection of computer software as a literary work has been available for more than two decades now. During the 1980s more and more people were acquiring computers, and the legal community, which had predictably lagged behind, had to get going to try to put some legal constructs in place for protecting software. After the initial acceptance of copyrightability for computer software, in the form of source code, object code and firmware, more fine tuning has taken place in the courts

which in some cases is making it a bit more difficult to apply the U.S. Copyright Act to certain forms of computer software. For example, in 1992, an important case was decided which illuminates just this point. *Computer Associates Int'l, Inc. v. Altai, Inc.*[17] analyzed the scope of copyright protection with respect to non-literal structural elements of a computer program. Literal elements were not at issue here, the law already having been well established. The court in this case established a new analysis for substantial similarity, one of the elements of determining copyright infringement (after proving access to the work by the alleged infringer): *Abstraction – Filtration – Comparison*. The explanation given by the court in its decision is pretty well thought out, although a number of practitioners in the field did not like the opinion when it first appeared. We are all much more used to it now, although it remains controversial, and it is, indeed, the law.

It is also well established that the fixation of a work in computer RAM satisfies the law, for purposes of determining copyrightability. It is further the case that data transmitted over the Internet likewise satisfies this element of the law when it is sent or received, so long as the data represents a work of authorship, and not, say, mere numbers or facts. While the data is in transit between sender and receiver, however, the fixation requirement will be met only if temporary copies are made. Moreover, a work or software posted on an electronic bulletin board has been determined to create a copy on the hard drive of the computer where the bulletin board is operated. Uploading and downloading are both considered to be activities by which copies are created. In addition, posting software to a web site has been held in one instance to create an infringing copy on the hard drive of the computer which hosts the site.

As for browsing on the Internet, the court in *Religious Technology Center* v. *Netcom On-Line Communication Services, Inc.*,[18] stated that digital browsing should be considered a fair use, and characterized such activity as "the functional equivalent of reading, which does not implicate the copyright laws and may be done by anyone in a library without the permission of the copyright owner."[19] However, a fair use defense needs to satisfy a number of elements to be successful, and is an issue of fact. Nevertheless, it is important to bear in mind the possibility of an ISP's or a corporate employer's being sued for contributory or vicarious liability based on acts of subscribers or employees (hence, the need for

[17] 982 F2d 693 (2d Cir. 1992).
[18] 907 F.Supp. 1361 (N.D. Cal. 1995).
[19] 907 F.Supp. at 1378 n.25.

comprehensive Internet and email policies in companies and government agencies).

What about the act of linking to another web site? That in and of itself does not constitute copyright infringement, but the argument of encouraging or facilitating others' infringing activities thereby might be used. The Digital Millennium Copyright Act (DMCA) might be helpful to ISPs in helping them to avoid copyright liability for linking or caching, which will be discussed later.

Consider at this point the issue of licensing copyright protected works. Licensors are typically very careful about the rights granted to a third party by a license, and the granting of a license to distribute the work, but not to display it publicly, might pose some problems for a licensee who wishes to distribute the work online. How does copyright law enter into the picture on the Internet, especially with respect to multimedia? And multi-ownership? The Internet comprises a whole array of multimedia works. This means that one particular work may comprise text, film, video and audio, as well as photographs, graphics (including animation or not), all of which is stored in digital form.

When any element of a work on the Internet is owned by someone other than the web page owner, and which is not in the public domain (*i.e.*, "out of copyright"), clearance must be obtained from the owner of that element to avoid potential litigation. Clearance basically means permission, and permission may be granted by license (express or implied), or by creating the work oneself or as a work made for hire.

Obtaining clearance can be very complex, because the rights to each prior work, no matter how minor, may be owned by any number of different parties up and down the chain. For example, one company may have the exclusive right under license to distribute a work, while another company may have the exclusive right under a different license to reproduce it. Further, the rights to more than one copyright might be involved, which complicates the situation even further.

Traditional copyright law is always being tested with respect to the Internet. It is so easy to copy a work and send it to any number of users worldwide. Digital works can be easily manipulated and modified, and traditional copyright law focuses on "fixation" of a work. The digital form of works on the Internet allows for new kinds of searching and linking, and can generate new hybrid multimedia works. Can hypertext be protected by copyright? Again, a multimedia work can comprise all sorts of things, which in the old days would be separated out as literary works, audio-visual works, performance works, a sound recording, etc. And, when there is transmission of a work over the Internet, that would

constitute a reproduction distribution, a public performance and/or public display.

Web sites as a whole offer a wide range of copyright protection opportunities: content, compilations, software user interfaces and the underlying software operating the web site. Content is protected the same as anything not on a web site would be protected. It basically is what it is. Literary works, photographs, sound recording, etc., can be protected no matter where they reside.

Compilations, which include databases, are protectible to the extent the selection and arrangement of the factual material therein is creative and original.[20] With respect to software user interfaces, it is the "look and feel" which is likely to control in the case of an infringement, rather than the literal code or content (although if the code has been copied, there may be some threshold of enforcement in accordance with the abstraction-filtration-comparison standard set forth in the Computer *Associates v. Altai* case discussed earlier). Nevertheless, protection of the "look and feel" may be somewhat problematic anyway, since however the web site looks is generally determined by the browser which is used to get at it. Besides, much of a web site may include what is called scenes a faire.[21]

Another statutory basis for copyright protection in the Internet realm is the Digital Millennium Copyright Act (DMCA)[22] enacted in 1998. It is indeed a controversial law, and the kinks in the system are still being worked out. The part of the DMCA which is appropriate for this discussion is Title II of the Act, The Online Copyright Infringement Liability Limitation Act. This section affords copyright owners with another set of remedies when confronting online infringement. Further, the Act also changes the standards by which ISPs, OSPs[23] search engine services, portals, destination sites or the like which qualify as "Service Providers"

[20] For a great many years, protection was given to databases based on the effort it took to compile and present the information ("sweat of the brow"). In 1991, the Supreme Court essentially wiped the sweat off the brow, which means effort is no longer taken into consideration when conferring (or not) copyright protection for databases. The case is Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991).

[21] Scenes a faire (an Americanized French without the accent marks) represent "expressive elements of a work of authorship [which] are not entitled to protection against infringement if they are standard, stock, or common to a topic, or if they necessarily follow from a common theme or setting." Mitel, Inc. v. Iqtel, Inc., 124 F3d 1366, 1374 (10th Cir. 1997). Think of scenes a faire as, for example, a plot in a novel. How the plot is expressed is generally copyrightable, but the plot idea itself is not.

[22] 15 U.S.C. §1125(d).

[23] OSP means "online service provider." This may include companies and nongovernmental entities such as libraries and schools which provide access to the Internet.

under the Act, might be liable (or not) for third party copyright infringement.

Escape from liability, or at least some liability limitation, under the Act depends on satisfaction of four threshold prerequisites in regard to copyright infringement based upon: (1) transitory digital network communications (*i.e.*, transmitting, routing and providing connections to infringing material); (2) system caching; (3) user storage of information; or (4) information location tools (*i.e.*, linking or references to infringing material. There is also a broad exemption under any legal theory for (5) the disabling of access to or removal in good faith of the allegedly infringing material. But this broad exemption is more likely to be successful if the requirements regarding the other categories are met.

The threshold requirements include the requirement that the Service Provider must adopt and reasonably implement a policy of terminating accounts or subscriptions of repeat infringers, and all account holders and subscribers must be informed of this policy. Companies should also strictly include such language in policy explanations to employees. Furthermore, standard technical measures must be accommodated and there can be no interference with such measures. Service Providers must designate agents to receive the statutory demand letter (the *Notification*) and they must also comply with specific rules for removing or blocking access to the allegedly infringing content. In cases where content is removed in response to a Notification, Service Providers must also comply with procedures governing Counter Notifications, whereby they would potentially replace or restore access to content previously removed in response to the original Notification.

It would appear that Service Providers face a greater risk of third party liability for user storage than for transitory digital network communications, system caching or linking. Because compliance with the DMCA is not compulsory, and because satisfying the requirements of the threshold prerequisites are likely to be overly burdensome to smaller Service Providers, not all of them will comply to limit their liability.

A copyright owner, on the other hand, has an advantage over the Service Providers in that he or she can act swiftly and relatively inexpensively to have infringing material removed from a web site; the time consuming and more expensive burden of returning the material to the web site is placed on the party putting forth the Counter Notification, and not on the copyright owner.

Finally, it is important to look at the formalities of obtaining a registration for copyright in the United States. As a result of the United States' becoming a signatory to the Berne Convention, so-called "formalities"

such as a copyright notice and registration are no longer required. Nevertheless, I always counsel my clients, whether in the United States or anywhere else in the world, to take advantage of such formalities. There are a number of reasons for this. First, the copyright notice (the symbol © and the year of creation, along with the name of the author (which may also be pseudonymous)) serves the purpose of giving notice of authorship to others. It costs nothing to implement. Second, there are a number of advantages to obtaining a formal registration of a work in the U.S. Copyright Office: (1) for works created in the U.S., the registration provides entre into the U.S. federal courts to file infringement actions; (2) statutory damages are available, which is especially useful when actual damages cannot be ascertained or when they might be too low; and (3) attorney's fees may be awarded, which alone justifies the registration. Third, a registration is very inexpensive to obtain. Most importantly, a copyright registration serves as *prima facie* evidence of the validity of the registration. The burden shifts then to the defense to rebut that presumption.

2.3 Trademarks

Trademark law in the United States has its legal underpinnings in the Lanham Act,[24] enacted in 1946 and amended several times since then. Before we look at the profound developments engendered by the Internet regarding trademarks, it is best to look briefly at trademark law on the *terra firma* of offline use.

A trademark is used to distinguish goods and services in the marketplace, and to identify such goods and services in the minds of the purchasing public with their source. Trademarks also accrue good will, which is a very valuable, yet intangible, asset for a company to have. It strengthens the mark and thereby strengthens its enforcement in case of an infringement. Good will can also be construed as commercial impression. The current caché name for this is *branding*.

The U.S. Supreme Court in a 10-year old case provided the following language: ". . . trademark law, by preventing others from copying a source-identifying mark, 'reduces the customer's costs of shopping and making purchasing decisions,' for it quickly and easily assures a potential customer that this item – the item with this mark – is made by the same producer as other similarly marked items that he or she liked (or disliked) in the past. At the same time, the law helps assure a producer that

[24] 15 U.S.C. §1051 et seq.

it (and not an imitating competitor) will reap the financial, reputation-related rewards associated with a desirable product."[25]

There exist common law rights in trademarks and service marks in the U.S., but federal registration is the preferred way to go. While "Intent to Use" (ITU) applications may be filed at the Trademark Office, ultimately a trademark registration will not issue unless and until the mark is used in interstate commerce. That means that, unlike in some countries, a mark cannot be reserved and held without use.

In order to be truly effective, a mark should be "strong" and distinctive. The Trademark Office prefers marks which are *arbitrary and fanciful*. Suggestive marks are generally registrable, as well, although their enforceability may not be as strong. Marks which are purely descriptive will never obtain a registration, nor will marks deemed to be generic. A mark such as KODAK for cameras and camera equipment is a wonderful example of a strong mark. So is XEROX for photocopiers and photocopy equipment. The danger is when people start using the mark in general terms ("Oh, I'll just go 'xerox' that for you."). If that goes on for too long, the mark becomes generic and will have no trademark significance. The Xerox Corporation ended up spending magnitudes of several millions of dollars in advertisement and other campaigns imploring people to use the term "photocopy" instead of "xerox." The company seems to have won the war, although there are still plenty of people who use the word "xerox." Two examples of generic marks for words in English are "cellophane" and "escalator." Unfortunately, companies seem to like descriptive marks – those marks which describe their goods and/or services or their qualities or characteristics. The Trademark Office will not register descriptive marks, and it is quite difficult to persuade these companies that imaginative marks are better.

The term "secondary meaning" is used to refer to distinctiveness in the marketplace. For example, if a mark deemed to be "merely descriptive" is used in interstate commerce for at least five (5) years, there is a presumption that the mark has acquired secondary meaning. At that time, such a mark may very well be eligible to obtain a registration. However, a formal application must be filed.

The Trademark Law in the United States sets forth items excluded from registration on public policy grounds:

- marks which consist of or comprise immoral, deceptive or scandalous matter;[26]

[25] Qualitex Co. v. Jacobson Products Co., 514 U.S. 159, 163–164 (1995) (citations omitted).
[26] 15 U.S.C. § 1052.

- marks which may disparage or falsely suggest a connection with persons, living or dead, institutions, beliefs, or national symbols, or bring them into contempt, or disrepute;[27]
- marks which constitute a geographical indication which, when used on or in connection with wines or spirits, identifies a place other than the origin of the goods and is first used on or in connection with wines or spirits by the applicant on or after one year after the date on which the WTO Agreement enters into force with respect to the United States;[28]
- marks which consist of or comprise the flag or coat of arms or other insignia of the United States, or of any state or municipality, or of any foreign nation, or any simulation thereof;[29]
- marks which consist of or comprise a name, portrait, or signature identifying a particular living individual except by his or her written consent, or the name, signature, or portrait of a deceased President of the United States during the life of his widow, if any, except by the written consent of the widow.[30]

When a registration issues, the owner of the registration is entitled to a presumption that it has the exclusive right to use the mark in commerce on the goods or services set forth in the registration – this is a nationwide right, whether or not the owner of the registration is using the mark in all 50 States. The registration is also *prima facie* evidence of the validity of the registered mark, which can be rebutted in case of a dispute (typically infringement). Common law marks (those not registered) or a mark registered on the Supplemental Register (where a lot of merely descriptive marks reside, and which provides far fewer rights than the Principal Register (which is preferred)) are not entitled to this presumption.

State registrations, where typically the mark is only used within the borders of a particular State and thus would not be entitled to federal registration anyway, may be advantageous in an Internet dispute. Nevertheless, a State registration provides no particular advantages over common law rights in federal court or in a domain name challenge.

For a federal registration, the shortest time frame currently from date of application to issued trademark registration is typically just a little over one year, so long as there are no problems regarding the prosecu-

[27] 15 U.S.C. § 1052(a).
[28] Id.
[29] 15 U.S.C. § 1052(b).
[30] 15 U.S.C. § 1052(c).

tion of the application through the Trademark Office. Sometimes there are informalities to address, but the most usual time killer, with no guarantees, is a legal battle. The Examining Attorney may raise a legal argument and cite previously registered or earlier filed applications against an application. The most common argument is "likelihood of confusion," which is the standard of review for registrability. Sometimes counter-arguments can be successful, and sometimes they can't. Typically, in the U.S. Trademark Office the Examining Attorneys do not generally have a technical background. That means that marks associated with technology, and most certainly software, do not have an easy time traveling through the prosecution labyrinth. Sometimes I'm successful, and sometimes I'm not. An appeal to the Trademark Trial and Appeal Board (TTAB) (an administrative court within the Department of Commerce) can be more of an economic issue than an issue on principle. An appeal from the TTAB to federal court can cost even more. A company has to be pretty wedded to a particular mark to stay in it for the long haul. Large companies have deeper pockets than smaller companies, and can thereby afford the bigger legal battles.

The problem with trademark use on the Internet is that the time frames are much more compressed. A mark which might easily acquire distinctiveness offline could become generic very quickly online. It takes due diligence and eternal vigilance to keep a mark safe and secure, with ownership intact, when it is moving at the speed of cosmic light over the Internet. It is important for companies, no matter what their size, to acquire and solidify their rights in their marks for terms used over the Internet.

Likelihood of confusion takes on a number of new dimensions with respect to the Internet. Not only can it attach to the words or slogans or designs themselves, but it can attach to similarities between goods and services, domain names which market them, or even to web sites promoting them. Owners of famous marks have the advantage of bringing an action under the Federal Trademark Dilution Act, which does not require a showing of likelihood of confusion.

In determining likelihood of confusion, which is generally a question of fact, courts typically look at several criteria, which are by no means exhaustive. When of record, the following factors must be considered: "(1) The similarity or dissimilarity of the marks in their entireties as to appearance, sound, connotation and commercial impression; (2) The similarity or dissimilarity and nature of the goods or services as described in an application or registration or in connection with which a prior mark is in use; (3) The similarity or dissimilarity of established, likely-to-continue trade channels; (4) The conditions under which and

buyers to whom sales are made, i.e. 'impulse' vs. careful, sophisticated purchasing; (5) The fame of the prior mark (sales, advertising, length of use); (6) The number and nature of similar marks in use on similar goods.
(7) The nature and extent of any actual confusion; (8) The length of time during and conditions under which there has been concurrent use without evidence of actual confusion; (9) The variety of goods on which a mark is or is not used (house mark, 'family' mark, product mark); (10) The market interface between applicant and the owner of a prior mark: (a) a mere 'consent' to register or use; (b) agreement provisions designed to preclude confusion, i.e. limitations
on continued use of the marks by each party; (c) assignment of mark, application, registration and good will of the related business; (d) laches and estoppel attributable to owner of prior mark and indicative of lack of confusion; (11) The extent to which applicant has a right to exclude others from use of its mark on its goods; (12) The extent of potential confusion, i.e., whether de minimis or substantial; (13) Any other established fact probative of the effect of use."[31]

The so-called "stream of commerce" is different online from offline. Because the Internet has such an immediacy about it, the likelihood of confusion between marks for similar goods and services can run very high very quickly. If a likelihood of confusion assertion can be distinguished by an articulation of disparately different channels of trade offline, an online presence can only muddy the waters even further and ultimately disintegrate different channels of trade as we know them. The stream of commerce is readily and continually available to the world population which goes online.

Advertisements on a web site can confuse the situation even more, especially when such an advertisement uses a variation of a mark which is too obvious to avoid confusion. Traffic will then be diverted, and confusion will arise. The use of metatags to access web sites can also be a source of confusion and unfair competition, which will be discussed later.

Because there are so many facets to the Internet, all of intellectual property could be affected by it. For example, simply linking from one site to another may very well lead to trademark infringement or unfair competition liability. Further, what cannot be actionable under U.S. copyright law (for example, headlines in a newspaper or magazine) could be

[31] Application of E. I. DuPont DeNemours & Co., 476 F.2d 1357 (Cust. & Pat.App., 1973).

actionable under the unfair competition section (typically Section 43) of the Lanham Act.

But the mere, yet unauthorized, display of a plaintiff's trademark on someone else's web site gives rise to claims in trademark law, unfair competition or even false designation of origin. This often arises in so-called phishing expeditions, where the nefarious among us try to steal someone's identity (and more importantly, their money) by posing as a legitimate business and even seeming to lure the unsuspecting into their lair by using the marks of legitimate businesses in "offering" free goods in exchange for private information. Those legitimate businesses may not have a clue about what is being done in their name using their trademarks.

These are all very fact-based situations. The facts will give you the information you need to know to decide whether or not you have a case, or can defend against one. With respect to trademark law and linking, the analysis will include whether or not the link creates customer confusion or muddies up the image of a company's trademark or which may otherwise cause deceit, be fraudulent or be simply unfair. An example of linking which would possibly cause contributory trademark liability is where a company links its site, and thereby sends traffic, to a site where pirated goods are sold.

There are defenses to an action for trademark-related liability due to linking, which include fair use (where the mark is not necessarily being used in the trademark sense), where the mark is descriptive as to the goods or services being offered, or where it describes its geographic origin. Furthermore, the use of a mark in comparative advertising (which is legal in the United States) or for promotion to identify competing goods or services would not be considered actionable. This activity is likely, however, to be actionable in other countries, and companies doing business internationally would be wise to pay attention to this issue. Where infringement has been established, some courts in the U.S. have prohibited linking. Other courts have considered linking to be evidence of intent. It clearly depends upon whether the mark in question is actually being used as a mark in the trademark sense, or merely as an identifier of the company to which is the linking occurs. This point should be considered in regard to a link via a company logo or slogan, as well as via a simple word mark.

It is one thing to link to a site, but it is another thing altogether to link to content. Making what is called "deep linking" and avoiding the home page of another site, not your own, has been litigated extensively in the United States, and the deep linker ends up losing. This is also known as a content link. It is more or less piggybacking on someone else's site and

making the user think that the content linked to is yours or at least affiliated with you. Deep links without attribution to the site linked to, can cause a great deal of consumer confusion, which is the linchpin of a trademark infringement action. Of course, the other side of this coin is when a linked-to site does not have the benefit of favorable search engine placement and therefore does not get a lot of traffic. In this case a deep link could be beneficial. But under these circumstances, it would be better to get linking permission from the potential linked-to site before such linking actually occurs. Furthermore, the site doing the linking ought to pay attention to its own responsibilities to consumers and protect itself from implied affiliation with, or implied endorsement of, the linked-to site's products or services.

There could also be potential liability for use of frames[32] and in-line links.[33] The problems occur in circumstances where there might be competing products or services suddenly appearing on one site due to these linking mechanisms. Content can also become distorted, resulting in dilution and/or unfair trade practices. Framing without more ought not to be a problem, but if there is more, a legal battle could ensue.

Metatags consist of HTML code used by search engines (and invisible to the user) in determining which sites correspond to the keywords entered by the user. Description metatags are intended to describe a web site; Keyword metatags appear to contain keywords relating to the contents of the web site. Metatags are basically index words. Since the essential purpose of having a web site is to attract as much traffic as possible, it is important to have as many of these index words as possible inserted into a web page. But metatags have also been used for more evil purposes. If a third party trademark, or marks or terminology closely associated with a competitor, are used by another company as metatags essentially to detour the traffic to its own site, or to boost the prominence of its site when a search engine is fired up, it would be exposing itself to tremendous liability for trademark infringement or dilution or unfair competition.

To discover what is hidden in metatags, click on "View" when a web site is displayed, and look at the *document source* or *page source*. If there

[32] A frame is a function permitting a computer screen to be divided into two or more simultaneously viewed web pages, each of which has full web page functionality. Internet and Technology Law Desk Reference, Michael D. Scott, Aspen Publishers, 2004 Edition.

[33] n-line linking within a web page causes content from another web site to be automatically loaded onto the original web page. To the user, the content from the second web site appears to be part of the first web page. Id.

is anything in that location which could trigger a question of infringement, the ball starts rolling there.

2.4 Domain Names

We are now going to enter a very challenging area of conflict within the Internet arena – trademarks and domain names.

A domain name functions as an address on the Internet. It consists of at least two parts: the top level domain name and the secondary level domain name. The top level comprises what might be called an identifier, such as a .com, .gov, .org, .edu, .net[34] or .[country abbreviation] (such as .ug for Uganda, .se for Sweden, .ca for Canada). This top level identifier is preceded by the second level, which can be an amalgam of alphanumerics and/or symbols. Domain names are typically registered with, or assigned by, a domain name registration authority.

Domain names can consist of trademarks, and this is where much of the legal action has taken place. There have been too many instances to count where unscrupulous persons have hijacked the (typically) famous trademarks of large (and small) corporations and essentially ransomed them back to their owners for exceedingly large sums of money. Some might even call this a form of extortion. The term *cybersquatting* has been coined for this activity, and the U.S. now has the Anticybersquatting Consumer Protection Act[35] to attempt to deal with the problem.

Businesses tend to use their names or the trademarks of their products or services as domain names. This allows users to find them more easily on the Internet. However, some domain names infringe on the rights of other third parties, which may lead to litigation or other proceedings to rectify the situation. One extra-judicial remedy is an administrative proceeding by Network Solutions, Inc., a domain name registrar, to place a domain name on "hold" until true ownership can be determined. Other remedies are available through other registrars in accordance with the rules set forth by ICANN[36] in its Uniform Domain Name Dispute Resolution Policy. But this proceeding works *only* if the domain name was registered in bad faith.

[34] These are also known as "generic top level domains."

[35] 15 U.S.C. § 1125(d).

[36] Internet Corporation for Assigned Names and Numbers, which is a non-profit California corporation, created in 1998, and which governs the assignment of Internet domain names, the allocation of Internet Protocol (IP) address space and management of the Domain Name System (DNS) and Internet 'root' server under the auspices of the U.S. Department of Commerce.

Domain name disputes by far take up most of the civil lawsuits filed in the United States for Internet-related issues. The value of a domain name can be viewed as even more powerful than a "mere" trade name. A domain name may simultaneously identify the name of a business, its Internet address and the services it offers. The marketing value on the Internet is much higher than in the offline world, and domain name disputes appear to be inextricably intertwined with trademarks. But trademarks are typically confined within a country's borders (or if registered in more than one country, within the borders of several countries). Domain names, on the other hand have no such confines, because, after all, the Internet recognizes no borders. While a great deal of time has passed by now for companies to go forth and protect themselves further, it would be time and money well spent to obtain domain name registrations in as many gTDLs (and even ccTDLs) as possible to thwart anyone else with greedy eyes on its valuable marks. Even mere variations on a trademark can be registered as a domain name by someone else.

The Anticybersquatting Consumer Protection Act provides a cause of action in cases where there is a bad faith intent to profit from another's mark through domain name registration, trafficking in or use of a domain name. Significantly, it provides for *in rem* relief, as well as extra-judicial remedies from domain name registries and registrars. This is useful, since many of these characters who engage in such activities in bad faith do so anonymously or pseudonymously and can be very difficult to locate.

Plaintiffs need not show a use in commerce (unlike in regular U.S. trademark cases). Bad faith intent must be established, and this is where the facts matter a great deal. A defendant may rebut a plaintiff's showing only by the demonstration of both a subjective and objective lack of bad faith.

For claims brought under 15 U.S.C. §§ 1114 or 1125(a) or (d), the Anticybersquatting Consumer Protection Act grants a blanket exemption from damages under the Lanham Act to registries, registrars and others "for the registration or maintenance of a domain name for another absent a showing of bad faith intent to profit from such registration or maintenance of the domain name."[37] These entities may also not be subject to injunctive relief unless they fail to comply with the requirements for extra-judicial relief imposed upon them in connection with procedures for *in rem* relief. Therefore, it would appear that injunctive relief would be granted only if the entity described here has not promptly deposited with the court, in an action which has been filed

[37] 15 U.S.C. § 1114(2)(D)(iii).

regarding the disposition of the domain name, documents sufficient for the court to establish its control and authority in regard to the disposition of the domain name; where the entity has transferred, suspended, or otherwise modified the domain name during the pendency of the action (except in response to a court order); or the entity has willfully failed to comply with a court order.[38]

2.5 Trade Secrets

The uniformly accepted definition of a trade secret under United States law is: "A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."[39] There are also various State statutes which more or less provide the same legal language. Clearly, a trade secret *must be kept secret*, and it must be, and be considered to be, of value to the owner.

But if a secret is exposed to the light of day, the protection vanishes. The exception to that is if there has been an unlawful misappropriation of trade secrets. Nevertheless, the strength of a trade secret is governed by the mechanisms put in place by a company to keep that trade secret a secret. This is very important in a contractual situation involving the company's own employees, whether in management or not, and any third parties, including their employees, not to mention subcontractors. The chain of secrecy must never be broken, or the cat is out of the bag for good.

In fact, the way trade secrets and other confidential matter are kept secret can affect how a possible infringement or misappropriation can be handled by a court. For example, if one has a system for determining who in the company has the right to know what the secrets are, and under what circumstances, how the secrets are kept from others in the company, and the like, then the courts are more likely to be satisfied, so to speak, that the company hasn't been sloppy in the way it protects its trade secrets. It is also very important to have a writing between a company and its employees which includes definitive language that states the existence of trade secrets and confidential material, and that it is forbidden to steal or otherwise misappropriate them.

With respect not only to employees, but also to licensees and other third parties, it is absolutely not required to disclose any trade secrets in

[38] 15 U.S.C. § 1114(2)(D)(i)(II).
[39] Restatement of Torts § 757, Comment b (1939).

order to protect them. It is, however, necessary to disclose their *existence*. In such a situation, the company can demand that the other party or licensee take the same strict measures that the company takes itself to protect its trade secrets. The company can proscribe the other party in the contract from reverse engineering the product in order to determine the substance of the trade secret. If an independent third party enters into a business relationship with the other party involving the subject of the trade secret, then that third party shall be under the same protection obligations as the other party. Alternatively, the other party shall take measures to protect the trade secret from the third party entirely. Clearly, the more diligent the company is in protecting its trade secrets, the better position it shall be in. On the one hand, the company can avoid disclosure and infringement or misappropriation, and on the other hand if there is an infringement or misappropriation, the company can protect itself better in court by maintaining that it has done everything possible to protect its trade secrets.

The legal determination of what exactly comprises a trade secret, as articulated in the Restatement of Torts, provides that the courts should consider (1) the extent to which the information is already known by others; (2) the extent of measures taken to guard the secret; (3) the value of the information to the plaintiff's business or competitors; and (4) the ease or difficulty with which the information could be properly obtained or duplicated by others.

There is another reason for being diligent with written and detailed agreements. Trade secrets, especially in connection with technology like software, can be the life blood of a company. A company must guard against gratuitous carelessness in the treatment of its trade secrets.

How often does a company use Non-Disclosure Agreements when it presents new products or services? When going after capital, for example, the company has to describe in extreme detail its products or services. A company should consider taking along an NDA to the meeting, which should provide that the presentation and any disclosures are for the express purpose of obtaining investment capital and for no other reason. The nightmare can be that the bank manager's brother-in-law is doing or is thinking of doing exactly what the company is doing. Under these circumstances, an NDA is essential.

While the vulnerability to disclosure is always a whisper away generally, the pervasive presence of the Internet should serve to make us all a bit more jumpy with respect to the protection of trade secrets. There are many steps which a company should take to protect itself, as mentioned earlier, which include making provisions in contracts and licenses such that the subject of the contract or license comprises trade secrets and

that those trade secrets *must* be protected by the other party. Because the Internet allows such supersonic immediacy of information dissemination, special care must be taken to protect trade secrets inside a company, as well as outside the company.

The use of the Internet in marketing can present a critical danger to companies which have a marketing group wanting to blurt out as much as possible on the company's web site. Before the company knows it, all its trade secrets and other confidential information can be out on the web site for the entire world to bathe in and misappropriate with impunity. That being said, some companies are not going to be as diligent as they ought to be. Therefore, from a competitive point of view a company is always going to be curious about its competitors – what they do and what they might think of the company as a competitor itself. Thus, a company should consider having an employee surf the net several times a day, going to other companies' sites competitive with the company in all ways, including all products and services, both current and prospective. A company can obtain good information to help it compete on an even better footing. A bonus is that by surfing in this way, a company can detect infringement by others in the copyright and trademark areas. Several of my clients do this regularly and have subsequently found quite a bit of infringement, which we were able to handle in due course.

But, what if a company is too small to use an employee in this way? Consider outsourcing this task to a third party to perform instead. And remember to provide in the agreement with the outsourcing company the strong measures for protecting trade secrets. Also, be aware that the outsourcing company may represent the competition, as well. A company can contract out of possible conflicts, but it is important to protect oneself as much as possible. If this sounds entirely too paranoid, the question must be asked: What value do you set on your company? How important is it for the economy, locally and globally? Companies must learn to protect themselves!

Trade secret law, on any level, does not prohibit the exercise of reverse engineering, which is essentially taking the finished product and working backwards to find the elements or obtain the process used in its development or manufacture. Nevertheless, provisions can be set forth in contracts or licenses which prohibit reverse engineering generally. In regard to computer software, such provisions prohibit decompiling, disassembling and the like to get the source code from the object code. *But*, this kind of provision may not be used with respect to parties residing in European Union signatory countries. Under no circumstances where an EU country is involved may reverse engineering with respect to software

be prohibited by contract. Never. This, of course, does not go down well in the United States. It would appear, however, that the reverse engineering allowance, so to speak, in the EU is focused on the occasional need to reverse engineer for the sole purpose of interoperability of software.

2.6 Software Protection

2.6.1 Software Audits

Software can be looked at in two different ways. Looking at it in a strict commercial sense (*i.e.*, what is useful for companies to have in order to operate), companies can either avail themselves of what can be called "off the shelf" software or of specifically customized software. Off the shelf software can be acquired at neighborhood stores, or more increasingly downloadable off the Internet. This kind of software takes a "one size fits all" approach and may only have to be adjusted for particular user settings and operating system platform accommodations. It is generally relatively inexpensive.

Customized software typically is obtained after lengthy and sometimes painful negotiations, and it can come with a price upwards of several hundreds of thousands of dollars, and sometimes more. This kind of software is an extremely valuable asset. However, it is vitally important to the company obtaining the software to understand that unless the software development agreement says otherwise, it is getting a *license to use* the software, and not title to and ownership of the software. This is true also with respect to the off the shelf variety of software.

Problems arise, particularly in the absence of a written corporate policy with employees, when employees gratuitously bring in software from home or otherwise download software onto their computers at work. Companies should not only have firm restrictions in place which prohibit that kind of activity, but they should also periodically scan their employees' computers to see whether there is any pirated software on the system. The use of software without a license is a seriously risky issue, and flies in the face of a self-protective, proactive approach to running a business. Performing regular software audits, along with strong company policies against pirated software will go far in allowing companies to avoid expensive, time consuming litigation.

2.6.2 Open Source Software

As has already been discussed, computer software can be protected to a great extent by patents and copyrights. However, there exists a monster

in the closet known as *open source software*, about which companies need to recognize and pay heed.

Open source software has been around for several years, and has important implications in regard to contracts, licensing and intellectual property. One of the more visible examples of open source software is the Linux operating system, which was developed to compete with Unix.

Two cases in the United States in the past several years have articulated some definitions of open source software. In *Universal City Studios, Inc. v. Reimerdes*[40] the court defined it this way: "[A] software development model by which the source code to a computer program is made available publicly under a license that gives users the right to modify and redistribute the program. The program develops through this process of modification and redistribution and through a process by which users download sections of code from a web site, modify that code, upload it to the same web site, and merge the modified sections into the original code."

In *United States v. Microsoft Corp.*[41] the District Court in that particular antitrust case stated: "Since application developers working under an open-source model are not looking to recoup their investment and make a profit by selling copies of their finished products, they are free from the imperative that compels proprietary developers to concentrate their efforts on Windows . . . Fortunately for Microsoft . . . there are only so many developers in the world willing to devote their talents to writing, testing, and debugging software *pro bono publico*. A small corps may be willing to concentrate its efforts on popular applications, such as browsers and office productivity applications, that are of value to most users. It is unlikely, though, that a sufficient number of open-source developers will commit to developing and continually updating the large variety of applications that an operating system would need to attract in order to present a significant number of users with a viable alternative to Windows."

There are advantages and disadvantages to open source software. From a practical viewpoint for both companies which are not software developers (at least not open source software developers) and government agencies, open source software is inexpensive and has reasonably efficient interoperability with other software within the company or government agency, so it is relatively easy to use, as well. Since there are no intellectual property constraints (by design), open source software presents just an infrastructure issue. That also means that there are no

[40] 111 F.Supp.2d 294, 305 n.6 (S.D.N.Y. 2000) (footnotes omitted).
[41] 65 F.Supp.2d 1, 14-15 (D.D.C. 1999) (Finding of Fact 51).

royalties to pay, and the formats are standard, rather than closed and proprietary. With open source software, it is easier to maintain and upgrade to newer versions and it appears to present fewer security problems, although that issue will always be debatable. Apparently in Germany, the government agencies all use exclusively open source software.

But what if a company has proprietary modules it wishes to embed in an open source system? There appear to be two very divergent views on this. Those who strictly follow the GNU Public Library License[42] (which governs open source software – more on this later) and those who are actively part of the Free Software Foundation would rather disallow the use of proprietary modules. The other view, as espoused by Linus Torvalds (the originator of Linux), has made it clear that it finds proprietary loadable modules to be acceptable.

But let's get back to basics. The rationale behind the General Public License is the following: "The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software – to make sure the software is free for all its users."[43]

The Open Source Initiative, established as a result of open source development of the Netscape browser's Mozilla project (in 1998), emerged from an initial Open Source Definition, which has evolved over time to include the following rights and obligations (this is not an exhaustive list):[44]

- No fee or royalty may be imposed on redistribution.
- The source code must be made available.
- The licensee must have the right to create derivative works and modifications.
- The license may require modifications to be distributed as the original version plus patches containing the modifications.
- The licensor cannot discriminate against any user or group.
- All rights granted in the original license must be granted in any redistribution of the code.
- The license applies to the software as a whole and each of its components.
- The license may not restrict other software that is distributed with the licensed software.

[42] This apparently stands for: GNU's Not UNIX.
[43] Preamble to GNU General Public License.
[44] The Open Source Handbook, Michael Overly, pp. 5–6 (Pike & Fischer, Inc. 2003).

Open source software is not in the public domain, nor is it the same thing as Shareware or Freeware. Shareware is still proprietary, and after a trial period, the user is expected to pay a license fee in order to continue using the software. Freeware is also proprietary to the extent that there is no access to source code, nor may derivative works be created, although there is no license fee paid. So, how can you make a living from open source software? Typically, this occurs through charging for implementation, customization and support services. Even if open source software is essentially free with open source code, one size is still unlikely to fit all, and some customization will be needed. There are also the really cool accessories sold in conjunction with an open source program, like t-shirts and coffee mugs. And, of course, written documentation including user's guides is available, which tends to be a bit more expensive than coffee mugs.

But there are clearly legal implications to the use of open source software, as alluded to earlier. I don't plan to go into any real detail regarding open source license agreements here. Rather, I will attempt to highlight some of the legal issues which may arise when open source software is used in an organization.

In the closed source software world, where proprietary software is kept (let us hope) proprietary, through the function of patents (where appropriate), copyrights and trade secrets, further due diligence, as discussed earlier in this paper, is also usually taken by having the programmer employees (or independent contractors under engagement contract) sign a document strictly requiring them to hold their work confidential and, if an independent contractor, assigning all rights to the party who engages him or her. There are additionally usual controls on access to, and use of, third party software programming, as well as prohibition against the copying of code of any size from the Internet or from other sources unapproved by the employer and then using it in any application the employees or independent contractors are developing. Since licenses typically have indemnification and hold harmless clauses in them regarding infringement of third party software, it is imperative that closed source software developers be very careful generally, and even more so in regard to open source software use in regard to their proprietary products. In this regard, a proprietary software developer ought to consider doing the following:[45]

Isolate the development of any proprietary software, by prohibiting incorporation of any third party software (especially where a third party

[45] The Open Source Handbook, Michael Overly, p. 28 (Pike & Fischer, Inc. 2003).

software is of the open source variety), without express management review and approval.

Distribute proprietary software on media completely separate from any media where open source software may reside. This should avoid any unnecessary ambiguity which may arise otherwise.

Minimize the contact proprietary code may have with open source code. What the software developer of proprietary code does *not* want to have happen is the disclosure of the proprietary code. The risk can be diminished by separating the proprietary code into two different parts: one which interfaces with the open source code, and the other which interfaces with the programming which is *not* related to the open source code. The former should be developed as a separate, discrete module, which can only be used with open source code. Otherwise, the GNU General Public License may operate on it all.

What if you don't know if you have open source software on your system? For companies and government agencies a regular, periodic scan of all systems should include searches for not only illegal software (*i.e.*, software not under license), but for open source software, the use of which could compromise any third party or in-house proprietary software also in use. There are many large commercial software applications out today which probably contain several (or more than merely several) open source components. If an organization is contemplating obtaining a license to use such a software package, it would be wise to request a "*no open source*" warranty. That is, the license should clearly state that the product contains no open source software. But if it is disclosed that there are open source components, the licensee should ask the vendor about the fee structure, and look for ways to lower the fees. Further, in any license for commercial software, and especially where no open source software is desired, a definition of "open source software" should be included in the license agreement, along with a warranty provision that there is "no open source software" included in the product.

2.6.3 Systems Integration

A systems integrator is almost like a conjoined twin – it essentially takes its own product and integrates it with a product belonging to a third party to end up with a different, yet related, product altogether. The final product has elements belonging to each owner. The intellectual property issues come into play in very interesting circumstances, and companies would do well to investigate these issues while still in the planning stages of the integration.

For example, consider that Product A and Product B separately do not infringe any third party's patent. But as integrated, a patent infringement could take place. It is up to the company and its legal counsel to decide, as a business decision, whether or not to conduct a patent search (in whatever country deemed important) to see if there is any danger on the horizon.

From a copyright standpoint, it would be prudent for the systems integrator to ascertain whether it has the authorization from the owner of Product B to integrate that product with its own Product A, thereby, perhaps (but not necessarily), creating a derivative work. The owner of a derivative work (if not the copyright owner of the underlying work), *if authorized*, is the owner of that derivative work. But that owner still needs permission to use the underlying work as a basis for the derivative work, and that can occur via a license. Should the license terminate or otherwise expire, the derivative work may ultimately be unusable. Therefore, a systems integrator and its legal counsel should be very careful to determine the lay of the land before going forward.

Another interesting issue for systems integrators is that they essentially wear two different hats – on the one hand, with respect to the third party software which they intend to integrate with their own, they are in the role of a licensee, with all of its obligations; on the other hand, with respect to the integrated product, they are in the role of a licensor, with all of its rights. These respective obligations and rights cannot conflict if the company is to be successful. All license arrangements, in either role, must pay heed to each role, so that the systems integrator doesn't get caught in the middle.

2.6.4 Source Code Escrow

Typically, when software is delivered to a user, even if it is customized for a particular company for a particular set of uses, the deliverable is in *object code*, unless the license says otherwise. If changes need to be made or if maintenance needs to be done for any reason, it is the *source code* which is used to make these changes. This is because the source code is what is more understandable to programmers, while the object code is more understandable to the computer. Vendors are generally loath to convey the source code, because it can be so readily pirated by others.

Source code escrow is basically an issue belonging to the user, and not the vendor. Computer software has been insinuated into our lives long enough for us to know that it tends to have a very short life span. It would seem that we are all encouraged to upgrade our systems on a yearly basis (if not more often). If we don't do that, life tends to go on.

But what happens if the vendor decides not to support the software any longer? Or what happens if the vendor gets acquired by, or merges with, a company which no longer wants to support the software. And what if the vendor gets into financial difficulty, or even goes bankrupt?

The purpose of source code escrow, then, is to provide a safe, controlled place, with independent third party escrow agents as custodians, for source code to reside until a triggering event occurs whereby the source code may be given to the user for the user to use for maintenance and/or related purposes. However, ownership and title to the source code *never* conveys to the user. There are many boiler-plate source code escrow agreements, all of them negotiable, which can identify the triggering events, as well as spell out the source code maintenance issues required for the escrow. The software must be kept regularly up-to-date and must be and remain completely functional for the user's purposes. Furthermore, the accounting done in this regard by the escrow agent can provide very valuable evidence for purposes of compliance with the Sarbanes-Oxley Act in the United States.

3. Now what?

It cannot be stated strongly enough that in order to maintain a competitive edge and be safe while doing so, companies must practice a due diligence heretofore not required. Or at least not assumed to be required.

While many companies have insurance protection generally, they should explore with their insurance provider the necessity of, and possible barriers to, insurance protection for intellectual property, including data and trade secrets. Whether a loss may be due to natural causes or to infringement or misappropriation, a company can end up disappearing along with its data and intellectual property if protective measures are not taken in advance. Most companies wait until the loss is incurred before contacting their insurance providers. That in itself is the diametric opposite of proactive behavior.

It is up to companies regularly to obtain a valuation of their intellectual property in order to overcome any such barriers. Unfortunately, it is very, very difficult to place a value on an intangible. Intellectual property rights apply to property which is not static, and the value of which may change as the use to which it is put changes, or even where in the statutorily protective period it may then currently reside. For example, and as discussed earlier in this paper, while patent infringement may occur at any time, it is pretty axiomatic that within the last three or so

years of a patent term, infringers come out of the woodwork and infringe with impunity. They rely on the typical fact that the patent holder has neither the money, the time nor the tenacity to fight an infringement action. Therefore, the value of patent rights may depend on how far from the expiration of patent rights the use is. Another example is if a copyright is not registered (for United States authors), or if there is only common law use of a trademark without registration (if registration can be obtained). The value of each may change depending on how it is or is not legally protected.

4. Conclusion

The electronic world in which we live and operate our businesses offers advantages and disadvantages. For a company to be competitive and remain competitive, it must know what it has in the form of intellectual property and computer software. It must know who actually owns such property, and it must protect what it owns. It must also be amply and proactively prepared in a defensive posture to stay out of trouble.It is incumbent upon companies to be smart about their businesses. Furthermore, it ought to be abundantly clear by now that the broccoli and spinach which companies have so assiduously avoided for so long are too good for them to be rejected altogether. Indeed, spinach, like knowledge, is power, and it is as active as it is proactive.