THE LAW OF THE INTERNET IN CALIFORNIA

WILLIAM E. LEVIN

LEVIN INTELLECTUAL PROPERTY GROUP

LAGUNA BEACH, CALIFORNIA

IBLS MATERIALS

PART 1. INTERNET LAW OVERVIEW

1. IMPORTANT INTERNET TERMINOLOGY

1. Internet

In the Twenty-First Century, most lawyers have at least some familiarity with the Internet and its special argot, but terms are still often lip synched as buzz words without complete comprehension of what they really mean. Though there are certainly many lawyers who are not yet Internet mavens, or savants in all of its parlance, if there is a lawyer in the crowd who has not heard of the Internet and have some passing understanding of what it entails, that lawyer would certainly soon get the moniker of Rip Van Lawyer after his or her many years of intellectual slumber.

The term "Internet" and related terms have been defined and described in various judicial opinions throughout the United States. See, e.g., Reno v. ACLU, 521 U.S. 844, 117 S. Ct. 2329, 138 L. Ed.2d 874 (1997); Hearst Corp. v. Goldberger, 1997 WL 97097, *1 (S.D.N.Y. 1997); American Civil Liberties Union v. Reno, 929 F. Supp. 824, 830-45 (E.D. Pa. 1996);); EDIAS Software Int'l Ltd., 947 F. Supp 413, 419-20 (D. Ariz. 1996); Martitz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328, 1330 (E.D. Mo. 1996); Playboy Enterprises, Inc. v. Chuckleberry Pub., Inc., 939 F. Supp. 1032, 1035-37 (S.D.N.Y. 1996); Religious Tech. Center v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361, 1365-66 (N.D. Cal. 1995).

The California Supreme Court recently embraced some of these definitions in its landmark decision addressing personal jurisdiction over those who post items on Internet web sites, in Pavlovich v. Superior Court, 2002 WL 31641714 (Cal. 2002), involving efforts by the DVD Control Association to enjoin the posting of the decryption software DeCSS by a Purdue University student on an Indiana web site: "'The Internet is an international network of interconnected computers' which 'enable[s] tens of millions of people to communicate with one another and to access vast amounts of information from around the world.'" Id. at *1, quoting Reno v. American Civil Liberties Union, 521 U.S. 844, 117 S. Ct. 2329, 138 L. Ed. 874 (1997). The Court further noted that "[w]ith its explosive growth over the past two decades, the Internet has become 'a unique and wholly new medium of worldwide human communication.'" Pavlovich, supra at *1 (citation omitted).

According to one leading definition: "The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked

networks. It is thus a network of networks." American Civil Liberties Union v. Reno, 929 F. Supp. 824, 830 (E.D. Pa. 1996). "The Internet is a 'decentralized, global medium of communications—or 'cyber space'—that links people, institutions, corporations and governments around the world.... These communications can occur almost instantaneously, and can be directed either to specific individuals, to a broader group of people interested in a particular subject, or to the world as a whole." Hearst Corp. v. Goldberger, 1997 WL 97097, *1 (S.D.N.Y. 1997).

Judge Klein, in one of the decisions involving the federal government's attempts to regulate Microsoft Corporation, stated: "The Internet is a huge global network which interconnects smaller networks of companies, permitting users on one network to communicate with and transfer information to users on many separate networks. The computers connected to the Internet range from Intel-compatible PC's and Apple Computer Corporation's Macintosh PCs, to high-powered computer workstations and large mainframe computers." U.S. v. Microsoft Corp., 1997 WL 656528, * 4 (D.D.C. 1997).

Another court observed that "[t]he Internet is a cooperative venture, owned by no one, but regulated by several volunteer agencies." MTV Networks v. Curry, 867 F. Supp. 202, 204 n. 1 (S.D.N.Y. 1994).

The Internet is also known by other terms, such as "the information superhighway," See, e.g., Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328, 1330, 40 USPQ2d 1729 (E.D.Mo. 1996), although it is not technically the same as the World Wide Web.

2. Cyberspace

Cyberspace is another Internet related term which is widely used in different contexts. In one sense, it is wherever it is that computers talk to each other, in the space that exists between them. One commentator described it, in 1995: "As commonly used today, cyberspace is the conceptual 'location' of the electronic interactivity available using one's computer. Cyberspace is a place 'without physical walls or even physical dimensions' in which interaction occurs as if it happened in the real world and in real time, but constitutes only a 'virtual reality.'" William S. Byassee, Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community, 30 Wake Forest L. Rev. 197, 220 n. 5 (1995)(citations omitted).

3. Top level domain names

Top level domains are the suffixes which attach to the second level domain names, such as ".com," ".org," and ".net." There are a host of other top level domain names, including various abbreviations for different countries, and a plethora of recently approved new top level domain names, such as ".biz."

4. Second level domain names

Second level domain names are where most of the trademark and trade name disputes arise, since these names are often either equivalent to the name of a well-known company, a fairly unknown company, or a term which tries to be descriptive of something, a generic term, or a person's name. For example, many law firms now use the name of their law firm as their second level domain name. This author's firm name is Levin Intellectual Property Group, hence the web site www.levinipgroup.com. Here,

levinipgroup is the second level domain name. One Internet pirate with particular chutzpah embarked upon the dubious scheme of registering the names of well-known law firms, but soon met with the inevitable lawsuit, in which multiple gargantuan law firms joined, though the case was filed in New York.

The Ninth Circuit has defined the "second level domain name" as "a term or series of terms (e.g. entrepreneurpr) that is followed by a top level domain name, which frequently describes the nature of the organization (e.g., '.com' for 'commercial' enterprises or '.org' for 'organization')." Entrepreneur Media, Inc. v. Smith, 279 F.3d. 1135, 1146 n. 12, 61 USPQ2d 1705 (9th Cir. 2002), citing, Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036, 1045 (9th Cir. 1999).

5. Metatags

The term "metatags," while once largely unrecognizable argot invisible to all but true Internet savants, has now become firmly entrenched in the lexicography of Internet cases, and is a "buzz" word that most lawyers have heard, even if they don't know exactly what a metatags is and how it works. One fairly non-technical, California judicial description is that "[m]etatags are Hypertext Markup Language ('HTMP') code which describe the contents of an Internet web site to a search engine." Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382, *1 (N.D. Cal. 2001), *citing*, Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036, 1045 (9th Cir. 1999). The practical marketing significance of metatags is described below. California case law often emphasizes the role of metatags in directing Internet traffic to a particular web site as the result of an Internet search: "Metatags are hidden code used by some search engines

to determine the content of websites in order to direct searchers to relevant sites." Playboy Enterprises, Inc. v. Welles, 279 F.3d 796, 61 USPQ2d 1508 (9th Cir. 2002)(the metatags "playboy" and "playmate" used as metatags on the web site of Terri Welles, former Playmate of the Year).

6. URL

A URL, short for "Universal Resource Locator," is the address of a particular web site, such as www.goooogle.com, the web site for a popular Internet search engine. "Websites have distinct addresses, commonly referred to as Universal Resource Locator ("URL") addresses." GTE New Media Services Inc. v. Ameritech Corp., 21 F.Supp.2d 27, 33 n. 4 (D.C. 1998).

7. HTML

Most computers users don't need to know, in current days, how to use HTML or hypertext markup language, which is now fairly transparent in computer interfaces. "In order to transfer data across networks of different computers, individuals must use a single format for data files that is recognizable by all of the interconnected (and different kinds of) computers. The need for a common file format led to the development of a special language hypertext markup language ('HTML') for writing and displaying documents to users on the Internet." U.S. v. Microsoft Corp., 1997 WL 656528, *4 (D.D.C. 1997).

8. World Wide Web

Although many individuals commonly use the terms "Internet," and "World Wide Web," (or just "Web" for short) interchangeably, they are not quite this fungible. There are various ways of describing the World Wide Web, but is not equivalent to the Internet itself, but instead sprang out of the Internet.

The California Supreme Court recently cited the following definition: "'The best known category of communication over the Internet is the World Wide Web, which allows users to search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to the designated sites. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world." Pavlovich v. Superior Court, 2002 WL 31641714, *1 (Cal. 2002). quoting Reno v. American Civil Liberties Union, 521 U.S. 844, 852, 117 S. Ct. 2329, 138 L. Ed. 874 (1997). In another leading case, the court indicated: "As HTML documents proliferated on the Internet, they became known collectively as the World Wide Web ('the Web')." U.S. v. Microsoft Corp., 1997 WL 656528, *4 (D.D.C. 1997).

9. Web site

A web site is the unique identity of its owner, and constitutes the owner's presentation to the world at large, as well as to customers, potential customers, vendors, and interested individuals. One's web site may contain text, images, photos, artwork, links to other websites, videos or movies, audio portions, streaming video, and many other graphic and aural combinations. It is the way companies do business and market themselves in the 21st century. A web site is also a source of essential information about

one's business, and can even be tantamount to a vanity license plate, such as web sites which incorporate an individual's name, famous or not, into the URL.

In more technical terms, "[c]ollections of HTML documents put out by a single became known as websites." U.S. v. Microsoft Corp., 1997 WL 656528, *4 (D.D.C. 1997). "On the Web, 'documents, commonly known as Web 'pages,' are ...prevalent.' These pages are located at Web sites and have addresses marking their location on the Web. If a Web page is freely accessible, then anyone with access to a computer connected to the Internet may view that page." Pavlovich v. Superior Court, 2002 WL 31641714, *1 (Cal. 2002)(citations omitted).

10. Web browsers

A web browser is the programwhich allows the user to access the Internet and a particular web site. Most people use either Netscape Communications Corp.'s application, Netscape Navigator, or Microsoft's competing software, Internet Explorer, though there are also other browsers such as Mosaic or the Hot Java software of Sun Microsystems.

The evolution of web browsers was described in one of the cases involving the government's challenge to Microsoft's trade practices:

> "As the Web grew in size, users needed a convenient method of searching for, retrieving, and viewing HTML documents on the Web. In response to this need, a group of software engineers at the National Center for Supercomputers Applications developed a software application that provided the interface for accessing and reviewing HTML documents. This application, which is stored on the user's computer, became known as an

> Internet browser. When a user wishes to view an HTML document, the browser transmits the request for the particular HTML document to another computer on the network called a Web server. When the browser receives the HTML document from the web server, it processes the HTML codes in the document and displays the resulting text, graphic images, and other content on the user's computer screen."

U.S. v. Microsoft Corp., 1997 WL 656528, *4 (D.D.C. 1997).

A. HOW THE INTERNET WORKS

As Magistrate Judge Peck stated in one Internet opinion: "The computer-literate who are already familiar with the Internet may wish to skip to the next section." Hearst Corp. v. Goldberger, 1997 WL 97097, *1 (S.D.N.Y. 1997). Some would posit that the Internet works like magic, akin to a magician employing a black box or pulling a rabbit out of a hat, or possibly more like the Wizard, really an old man pushing a lot of buttons behind the stage, in the Wizard of Oz, using smoke and mirrors and manipulating reality. Actually, perhaps more important in many ways that the mechanics of Internetology (a neologism, the author thinks), is the simple fact that unlike many other things in our world today, the Internet really does work. It does what it was designed to do, and more, including making information available for sharing around the world at a low cost. It even enables lawyers to do research on www.westlaw.com, rather than having to buy now largely antiquated software that needs upgrading every few microseconds or so. Internet access is a powerful tool in the hands of those who know how to use it, and equalizes the playing field between scads of lawyers and a single Internet maven.

According to one federal court judge in New York: "In order to understand the personal jurisdictional issues in this case, it is necessary to understand the Internet." Hearst Corp. v. Goldberger, 1997 WL 97097, * 1 (S.D.N.Y. 1997). This statement applies with equal force to many cases involving Internet issues. Comprehension of the Net is the sine qua non to Internet law, in California or anywhere. Indeed, any lawyer who seeks to handle

an Internet case had first become familiar with the Internet, by personally using it as much as possible.

One Colorado federal court in 1996 described the basic functioning of the Internet in this manner:

> "Any internet user can access any website, of which there are presumably hundreds of thousands, by entering into the computer the internet address they are seeking. Internet users can also perform searches on the internet to find websites within targeted areas of interest. Via telephone lines, the user is connected to the website, and the user can obtain any information that has been posted at the website for the user. The user can also interact with and send messages to that website. Upon connecting to a website, the information is transmitted electronically to the user's computer and quickly appears on the users' screen. This transmitted information can easily be downloaded to a disk or sent to a printer."

Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328, 1330, 40 USPQ2d 1729 (E.D.Mo. 1996).

B. NAVIGATING THE INTERNET

There are a wide array of means by which one can navigate the Internet, or "surf the Net" as it often called in the vernacular. "Individuals have a wide variety of avenues to access cyberspace in general, and the Internet in particular." American Civil Liberties Union v. Reno, 929 F. Supp. 824, 832-33 (E.D. Pa. 1996). The best way to experience these navigational options is, of course, to meander over to your computer, even if you

don't personally use it for word processing or similar functions, and jump onto the Internet superhighway. In a way, it's like driving a car. Once you've done it enough, it becomes second-hand in nature, to the point where the mechanical steps barely rise to the conscious level. But at the beginning, each miniscule move is subject to a great deal of thought and trepidation. And, after you have become proficient at driving, you almost never forget how to drive, no matter how long since last you drove. On the other hand, trying to describe to a neophyte how to drive a car and what it feels like, borders on the impossible, particularly if they are not behind the wheel while you are giving this exposition.

So, surfing the Net is something you need to do as often as possible, until you feel quite proficient at it. A caveat: Net surfing can become quite addictive and leads to compulsive behavior at times, such as propounding endless searches when you should be doing something billable instead. In mitigation, surfing the Internet will make you so creative in your approaches to problems that you will concoct numerous ways to bill the time you spend doing it. In reality, a good Internet search can save many hours of legal or factual research, and find things which could never be found by less conventional paths. For example, the author was recently involved in a potential lawsuit against Planet Hollywood, which was known to be in some phase of bankruptcy. Rather than hiring a bankruptcy lawyer to scour the bankruptcy courts' files to learn what the status of the proceeding was, and other germane information, a search on a search engine like www.google.com, combining key words like "Planet Hollywood" and "bankruptcy" quickly disclosed everything necessary to know, and up to the minute. Of course, there are

specialized bankruptcy and legal web sites where one could have gone instead to excavate all the desired nuggets of information.

Conventional navigation techniques include using search engines, utilizing known web sites, or "guessing" at the correct web site. "To navigate the Web, users may type in the known address of a home page or type one or more key words, using a commercial search engine to locate sites on subject matters of interest to them. Web pages commonly include 'links' that lead to information located elsewhere on the Internet." BCI Telecom Holding, Inc. v. Jones Intercable, Inc., 3 F. Supp. 2d 1165, 1771 (D. Col. 1998). The Ninth Circuit described the normal search engine process in a case involving the unconventional use of thumbnail images produced in response to a search: "When a user wants to search the internet for information on a certain topic, he or she types a search engine into a search engine, which then produces a list of web sites that have information relating to the search term. Normally, the list of results is in its text format." Kelly v Arriba Soft Corp., 280 F.3d 934, 938 (9th Cir. 2002). Internet search engines are the great equalizer of knowledge. For example, if an attorney receives a medical report using a lot of medical mumbo jumbo, or any technical terms of art from any industry, in a matter of a few minutes the attorney can have access to all of the leading medical or other literature explaining those terms and citing the most recent studies involving them. Anyone can have the resources of an expert in any particular field in a nanosecond using the Internet.

There is, of course, the old standby of simply typing in the name of the company or trademark of the product to see if you end up on their web site, and this is a navigational tool commonly used by many. Even the Ninth Circuit has opined upon the consistency of

this navigational practice in its Internet law decisions. For example, "Internet users searching for a company's Web site 'often assume, as a rule of thumb, that the domain name of a particular company will be the company name [or trademark] followed by '.com.'" Entrepreneur Media, Inc. v. Smith, 279 F.3d. 1135, 1146, 61 USPQ2d 1705 (9th Cir. 2002), *quoting* Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036, 1045 (9th Cir. 1999).

Unfortunately, it is not always successful, either because the company in question did not obtain the necessary domain name for itself, or some third party did, innocently or otherwise. Even a single letter wrong can also produce an entirely different result.

There are a number of ways actually to connect to the Internet. "In terms of physical access, there are two common methods to establish an actual link to the Internet. First, one can use a computer or computer terminal that is directly (and usually permanently) connected to a computer network that is itself directly or indirectly connected to the Internet. Second, one can use a 'personal computer' with a 'modem' to connect over a telephone line to a larger computer or computer network that is itself directly or indirectly connected to the Internet." American Civil Liberties Union v. Reno, 929 F. Supp. 824, 832-33 (E.D. Pa. 1996). Another method is for an individual to access the Internet "though commercial and non-commercial 'Internet service providers' that typically offer modem telephone access to a computer or computer network linked to the Internet." Id. Of course, these days computer modems might be considered somewhat antidiluvian in view of the speed of such devices as DSL lines, and cable modems hookups or "broadband" connections. A Colorado district court described the advent of cable

connections versus telephone lines: "The transmission methodology used to develop the Internet has been telephone lines. Cable television developed through the use of coaxial and fiber optic cables capable of sending signals much faster than the copper wire used in local telephone lines. The use of broadband cable to access the Internet communication system provides the advantage of speed and avoids the need for a dedicated telephone line." BCI Telecom Holding, Inc. v. Jones Intercable, Inc., 3 F. Supp. 2d 1165, 1171 (D. Col. 1998). And, as wireless technology continues to develop, a lawyer or his client, or the judge deciding the case, may well be using a wireless keyboard and mouse, with a computer connecting to the Internet via a wireless connection to an Ethernet or other network.

There are also a number of ways to communicate using the Internet, ranging from the now ubiquitous electronic mail, or email as it is called in the vernacular, akin to sending a letter by regular mail, but with dispatch via the Internet, to using the "World Wide Web." Even a young child can now use the Internet to communicate, particularly with an adult's help, such as by going to www.lego.com, picking possible holiday or birthday gifts, and then sending a "wish list" to one's parents, grandparents, and other relatives. (The author's son, Sean, at 4 years old, did this, from a selection of "Bionicle" robots, and requested, perhaps presumptuously, the custom message "Thank you," to be sent with the Wish List. But it worked quite well). Internet shopping is rapidly replacing a significant deal of traditional "brick and mortar" shopping, and many retailers use their Internet to complement their real world stores, with their web site functioning as a shopping adjunct to their own retail outlets, such as www.barnesandnoble.com or www.rogersgarden.com.

D. CHALLENGES FOR THE FUTURE

Infringement issues relating to intellectual property issues on a web site can lead to a host of tort and other claims being asserted in either federal court. It should be anticipated that creative lawyers will find more and more types of claims which can be asserted when Internet competition or web site conflicts are at issue. The Internet is and will remain a litigation hot bed for the foreseeable future.

As recently as late November 2002, the California Supreme Court recognized that "the so-called Internet revolution has spawned as host of new legal issues as courts have struggled to apply traditional legal frameworks to this new communication medium. Today, we join this struggle and consider the impact of the Internet on the determination of personal jurisdiction." Pavlovich v. Superior Court, 2002 WL 31641714, *1 (Cal. 2002). The "host of new legal issues" relating to the Internet for the foreseeable future will include personal jurisdiction questions, encryption and decryption technologies, privacy and defamation concerns, and an almost unlimited of twists on the normal intellectual property law issues related to patent, trademark, copyright, trade dress, trade secret, unfair competition, and false advertising subjects.

Parties to Internet disputes typically are asserting broader and more varied types of legal claims in their suits. For example, in one recent Northern District of California case, where the defendant copied some of Plaintiff's metatags, thereby diverting Internet traffic to its web site instead, the plaintiff asserted seven different legal claims in its first amended complaint, including: 1) Misappropriation; 2) Federal trademark infringement; 3) False advertising and false designation under the Lanham Act; 4) Trademark infringement and

unfair competition under California law; 5) Copyright infringement under federal law; 6) Civil trespass; and 7) Conspiracy. Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382 (N.D. Cal. 2001). Trade secret claims are being asserted based on such things as posting of decryption programs. See, e.g., Pavlovich v. Superior Court, 2002 WL 31641714 (Cal. 2002)(misappropriation of trade secrets by posting on a college student organization's web site the DeCSS program for decrypting the CSS technology used to preclude copying of DVD's).

Internet challenges will also arise due to the geometric growth in the use of the Internet. The number of users of the Internet, or the traffic, continues to grow at staggering rates. Thus, in 1996, one court observed that "[i]t is estimated that there are 20 to 30 million users of the internet. Today, there are around 9,400,000 computers that have present capability to access the internet." Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328, 40 USPQ2d 1729 (E.D.Mo. 1996). Of those 9.4 million computers, some 60% were then located within the U.S., not counting "personal computers that people use to access the Internet using modems. Reasonable estimates are that as many as 40 million people around the world can and do access the Internet; that figure is expected to grow to 200 million Internet users by 1999." Hearst Corp. v. Goldberger, 1997 WL 97097, *1 (S.D.N.Y. 1997), citing, American Civil Liberties Union v. Reno, 929 F. Supp. 824, 830 (E.D. Pa. 1996).

At the same time that the case law involving Internet torts is exploding, Internet law is still largely an unchartered frontier in which the courts will continue to struggle with new issues, new concepts, and new technologies, while striving for uniformity and consistency in

the judicial approach to Internet problems. But the following statement is still fairly typical when addressing Internet issues: "The Court has found no cases that address the specific requirements for making a prima facie case of unjust enrichment in the context of the Internet where the alleged infringement is the use of trademarked terms in metatags." Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382 , *9 (N.D. Cal. 2001). Or, as the California Supreme Court stated in November 2002: "[W]e have never considered the scope of personal jurisdiction based solely on Internet use...". Pavlovich v. Superior Court, 2002 WL 31641714, *7 (Cal. 2002).

It can be expected that as additional courts and jurisdictions struggle with unchartered or recently discovered Internet issues, more splits of authority will occur in California and elsewhere, including amongst the various federal circuits.

II. INTELLECTUAL PROPERTY ISSUES ON THE INTERNET

A. TRADEMARK REGISTRATION AND PRACTICE

a. Metatagging

According to one leading Ninth Circuit definition, "Metatags are Hypertext Markup Language ('HTMP') code which describe the contents of an Internet web site to a search engine." Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382, *1 (N.D. Cal. 2001), *citing*, Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036, 1045 (9th Cir. 1999).

The Northern District of California delineated the two different types of metatags with two discrete functions in Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382, *1 (N.D. Cal. 2001). "There are two types of metatags: 1) 'Description' metatags,

which are 'intended to describe the we site;' and 2) 'Keyword' metatags, which are 'at least in theory...keywords relating to the contents of the site.'"[1]

Metatags serve an important marketing function because they drive traffic from those searching the Internet to one particular site based on the number and frequency of metatags used by the web site owner. " 'The more often a term appears in the metatags and in the text of a web page, the more likely it is that the web page will be 'hit' in a search for the keyword and the higher on the list of 'hits' the web page will appear' in search engine results." Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382, *1 (N.D. Cal. 2001), *quoting*, Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036, 1045 (9th Cir. 1999).

Internet users often will not read or go to all of the results of a typical web search, but often will only review the first few hits, then click on one or two at most. Hence, being in the top portion of the results list is very valuable from a commercial standpoint, and companies, such as legalmatch.com, a law firm marketing organization, will pay search engine companies considerable sums of money to list them at the very top of search results using specified keywords.

The use of metatags which incorporate or infringe upon another's trademarks may be actionable in California. See, e.g., Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382 (N.D. Cal. 2001)(potential customers ended up on defendant's web site when using search engines due to presence of metatags from Plaintiff's web site).

---

[1] Citing, Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036, 1045 (9th Cir. 1999).

The law of trademark infringement is not yet well-settled in the arena of metatags. See.e.g., Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382U, *9 (N.D. Cal. 2001)(: "The Court has found no cases that address the specific requirements for making a prima facie case of unjust enrichment in the context of the Internet where the alleged infringement is the use of trademarked terms in metatags.").

b. Linking

Linking is the practice of connecting from one web site to another web site using a "hyperlink," which, when "clicked" on, takes the person clicking on the hyperlink to the web site denoted by the hyperlink. For example, going to the "resources" sections of many web sites provides a location on the web site where various hyperlinks are presented for connection to other web sites addressing similar subject matters, like a bibliography in a written work, although these linked web sites may not otherwise be utilized on the web site where the hyperlinks are found.

To illustrate, on the author's www.levinhawes.com web site, going to the "Resources" section by clicking on that button on the left of the home page, would take one to a group of links to various intellectual property law web sites, such as the web sites of the United States Patent and Trademark Office, the Copyright Office, the World Intellectual Property Organization (WIPO), the National Inventor's Hall of Fame, various legal publishers, and many others. Such "Resource" pages, with their various links to other web sites, can itself draw Internet traffic to the web site of the company with links to the other web sites, as a source of information. Such pages can also be used for marketing purposes as well as general information. Thus, if a potential client, or almost anyone, asks

the author for a copyright form, rather than asking office staff to send one out, the inquirer is directed to visit the author's web site, and go to the link in the Resources section to the U.S. Copyright Office, where not only all of the forms are available, but instructions and other useful information. Naturally, the person who visits www.levinhawes.com might see other items of interest to them on that web site, and eventually contact the author or his law firm for assistance with intellectual property law matters. Certainly, that individual has immediate access to information about the author, his law firm, its cases, its publications, its attorneys, and various intellectual property law articles, far more than a mere business card, or even slick brochure, could ever convey. By going to the various web sites of intellectual property law firms and other sources of intellectual property law, and simply following the various links, one could obtain virtually all the information ever needed on any intellectual property law subject matter. Using technical terms in Internet searches, such as "trade dress," and following the hits and various links on those sites, enabled the author to obtain unlimited free legal research and market research for his book, Trade Dress Protection (West Group 1996).

According to one federal court: "A hyperlink is a link that connects one website to a second website on the Internet. By 'clicking' on a designated space on the initial website, a subsequent website can be referenced. The designated space can be a picture, highlighted text, or other indication to take a person viewing the initial website to a second website. Hyperlinks are commonly placed on existing websites, thus, allowing Internet users to move website to website at the click of a button without having to type in URL addresses."

GTE New Media Services Inc. v. Ameritech Corp., 21 F.Supp.2d 27, 33 n. 5 (D.C. Cir. 1998).

One of the hot Internet legal issues is whether permission is needed to link to the web site of another and, if so, under what circumstances. What are the rules? The courts are just beginning to struggle with the answers to these questions.

One California trial court granted a preliminary injunction to prevent distribution or posting on defendant's web site of the DeCSS decryption program but refused to issue the requested preliminary injunction preventing defendants from "linking to other websites which contain the protected materials as such an order is overbroad and burdensome." DVD Copy Control Association, Inc. v. McLaughlin, 2000 WL 48512 (Cal. Sup. Ct., Santa Clara 2000). The Court noted that "links to other websites are the mainstay of the Internet and indispensable to its convenient access to the vast world of information. A website owner cannot be held responsible for all of the content of the sites to which it provides links." Id. at *4.

The Ninth Circuit has held that "inline linking" of images from another web site violated the copyright of the owner of the linked web site and was not a fair use. Kelly v Arriba Soft Corp., 280 F.3d 934 (9th Cir. 2002). As the Ninth Circuit described it, a user of Arriba's search engine would double click on the thumbnail image, and be taken to "the 'Images Attributes' page [which] contained the original full-sized image imported directly from the originating web site, along with text describing the size of the image, a link to the originating web site, the Arriba banner, and Arriba advertising." Id. at 938. This process, importing those images from other web sites, is called "inline linking." "The image

imported from another web site is displayed as though it is part of the current web page, surrounded by the current web page's text and advertising. As a result...the user typically would not realize that the image actually resided on another web site." Id. at 938-39. The Court held that this inline linking violated the public display rights of the owner of the images under copyright law, as a question of first impression. Id. at 945.

c. Framing

Framing, according to the Ninth Circuit, was described as resulting when a visitor to a defendant's web site encountered the following: "[B]y clicking on the 'Source' link or the thumbnail [a smaller image made from a larger one] from the [search engine] results page, the [defendant's] site produced two new windows on top of the Arriba page. The window in the forefront contained the full-sized image, imported directly from the originating web page. This technique is known as framing. The image from a second web site is viewed within a frame that is pulled into the primary web site's web page." Kelly v Arriba Soft Corp., 280 F.3d 934, 939 (9th Cir. 2002).

In Kelly, the Ninth Circuit noted that "[n]o cases have addressed the issue of whether inline linking or framing violates a copyright owner's public display rights," then, after discussing several analogous cases, found that it did because "Arriba actively participated in displaying Kelly's images by trolling the web, finding Kelly's images, and then having its program inline link and frame those images within its own web site. Without this program, users would not have been able to view Kelly's images within the context of Arriba's site. Arriba acted as more than a passive conduit of the images by establishing a direct link to the copyrighted images." Id. at 947.

d. Keywords

Accordingly to commercial parties offering keywords, such as "patents" for sale, "keywords are simple phrases that replace domain names (www.abc.com). Keywords are entered into the Address bar just like domain names (no www. Or dot extensions)." December 16, 2002 email from naturallanguagedirect.com to the author. According to this commercial source, the keyword "bank" is registered to Wells Fargo Bank, "airlines" to American Airlines, and "birthday cards" to Hallmark, and the trend for keywords to be used in the Address bar has grown from 1 out of 50 persons in 2001, to 1 out of 13 in 2002. It claims that "[t]here have been over 35,000 Keywords and phrases sold to over 6,000 companies" apparently by this one vendor alone. Id. Those wishing to know more concerning the sale of keywords may also go to www.KeywordTrader.com.

e. Content Rights Issues

The issue of whether the content of Internet web sites or communications on the Internet should be regulated, and, if so, under what circumstances, presents any number of controversial issues, implicating traditional First Amendment concerns over freedom of speech.

One area is which conflicts with First, and possibly Fourth, Amendment rights has already arisen is in the government's efforts to regulate encryption software, discussed in detail below. Government attempts to regulate or prohibit speech which relate to the contents of the speech are subject to strict constitutional scrutiny under the First Amendment. See Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750, 108 S.Ct. 2138, 100 L.Ed. 2d 771 (1988). "[C]ontent-based restrictions [are] subject to the strictest

constitutional scrutiny," in contrast to "content-neutral restrictions meriting less exacting scrutiny." Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132, 1145 (9th Cir. 1999).

Any licensing regime is "always subject to facial challenge as a prior restraint where it 'gives a government official or agency substantial power to discriminate based on the content or viewpoint of speech by suppressing disfavored speech or disliked speakers...". Bernstein, supra at 1139 (9th Cir. 1999)(citations omitted). Although the issue facing the Ninth Circuit did not require it to pass upon whether the EAR regulation of encryption software at issue was "content neutral," it felt constrained to comment that "the EAR regulations are very different from content-neutral time, place and manner restrictions that may have an incidental effect on expression while aiming at secondary effects." Id. at 1145. Accordingly, while not reaching that far, the decision seems to suggest that the Court would strike as content regulations those which are directed specifically at encryption source code.

f. Domain Name Issues

The Ninth Circuit reversed the trial court's grant of a summary judgment to the owner of the ENTREPRENEUR magazine mark, holding that factual issues required a trial as whether the defendant's mark ENTREPRENEURPR and the domain name entrepreneurpr.com infringed on the ENTREPRENEUR mark. However, the use of the mark ENTREPRENEUR ILLUSTRATED for a publication was found to infringe upon the other magazine's mark, and the summary judgment was upheld on that ground. Entrepreneur Media, Inc. v. Smith, 279 F.3d. 1135, 61 USPQ2d 1705 (9th Cir. 2002).[2] In determining that there were factual issues as to likelihood of confusion, the Court that

[2] This author was consulted by the defendant and advised he and his appellate counsel in connection with this case, but did not appear formally in the action.

because the defendant's web site name was not identical to the registered mark, "a consumer trying to reach [plaintiff's] Web site by typing in its magazine's name followed by '.com' would *not* reach [defendant's] Web site. Nor would a simple spelling error or typographical error likely lead a consumer attempting to access [Plaintiff's] Web site to [Defendant's] web site. This observation concerning the functional similarity of domain names is largely dispositive." Id. at 1146-47 (emphasis in original). Accordingly, the Ninth Circuit reaffirmed its previous theme that likelihood of confusion on the Internet is an animal of a different color: "Similarity of marks or lack thereof are context-specific concepts. In the Internet context, consumers are aware that domain names for different Web sites are quite often similar, because of the need for language economy, and that very small differences matter." Id. at 1147.

In avoiding a likelihood of confusion holding based on its previous collapsing, in Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999),of the likelihood of confusion elements into primarily a similarity of marks and similarity of services/products analysis, the Entrepreneur Media court distinguished Brookfield on the basis that, unlike the present case, it involved identical marks: MOVIEBUFF vs. moviebuff.com: "The precise identity was critical, we noted, because Internet users searching for a company's Web site 'often assume, as a rule of thumb, that the domain name of a particular company will be the company name [or trademark] followed by '.com.'" Entrepreneur Media, Inc. v. Smith, 279 F.3d. 1135, 1146, 61 USPQ2d 1705 (9th Cir. 2002), *quoting* Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036, 1045 (9th Cir. 1999).

Another confusion guideline for domain names is that dissimilarity cannot be shown by capital letters or their absence "because 'Web addresses are not capsensitive' and therefore will appear in print without case differentiation." Entrepreneur Media, Inc. v. Smith, 279 F.3d. 1135, 1147, 61 USPQ2d 1705 (9th Cir. 2002)(citation omitted) (comparing mark ENTREPRENEUR with domain name EntrepreneurPR).

Recent California federal law suggests that previous cases may have placed too much emphasis on the mere fact that both parties to a trademark or domain name dispute use the Internet as a marketing channel. "*Some* use of the Internet for marketing, however, does not alone and as a matter of law constitute overlapping marketing channels." Entrepreneur Media, Inc. v. Smith, 279 F.3d. 1135, 1151, 61 USPQ2d 1705 (9th Cir. 2002) (emphasis in original). Relying upon prior Ninth Circuit Internet precedents, the Entrepreneur court indicated that "[t]he proper inquiries are whether both parties 'use the Web as a *substantial* marketing and advertising channel, whether the parties' marks 'are utilized in conjunction with web-based products,' and whether the parties' marketing channels overlap in any other way." Id. at 1151 (citations omitted)(emphasis in original).

Federal courts around the country have recognized the importance and commercial value of domain names: "Internet domain names are similar to telephone number mneumonics, but they are of greater importance, since there is no satisfactory Internet equivalent to a telephone company white pages or directory assistance, and domain names can often be guessed. A domain name mirroring a corporate name may be a valuable corporate asset, as it facilitates communication with a customer base." MTV Networks v. Curry, 867 F. Supp. 202, 204 n. 2 (S.D.N.Y. 1994).

B. COPYRIGHT LAW AND THE DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA)

The Ninth Circuit addressed copyright issues of first impression in Kelly v Arriba Soft Corp., 280 F.3d 934 (9th Cir. 2002). The trial court, Judge Taylor of the Central District of California, had granted summary judgment for the defendant, a visual search engine operator, based on a finding of fair use as to various copyrighted images of a photographer who copyrighted his pictures of the American West. The Ninth Circuit set the stage as a case which "involves the application of copyright law to the vast world of the internet and internet search engines." Id. at 937. The Court described defendant's activities as follows: "[Defendant] operates an internet search engine that displays its results in the form of small pictures that displays its results in the form of small pictures rather than the more usual form of text. Arriba obtained its database of pictures by copying images from other web sites. By clicking on one of these small pictures, called 'thumbnails,' the user can then view a large version of that same picture within the context of the Arriba web page." Id. at 938. The Ninth Circuit split the baby, and held that the thumbnail pictures used in the search engine results were a fair use, while the display of the larger versions of those thumbnail images on defendant's web pages was a violation of Kelly's copyright on his images, namely, the exclusive right to publicly display his works.

The defendant's search engine, in other words, instead of producing text results from different web sites containing the queried key words, produced its results in small pictures. Arriba did this by developing a web "crawler" software program, one that searches the Web looking for images to be indexed for its search engine. First, however, the crawler

would download full-sized copies of the images it found, which were then converted by the program into the smaller thumbnail images, at which point the full-size images were deleted from the server. Kelly, supra at 938. Next, when a user of Arriba's search engine would double click on the thumbnail image, they were taken to "the 'Images Attributes' page [which] contained the original full-sized image imported directly from the originating web site, along with text describing the size of the image, a link to the originating web site, the Arriba banner, and Arriba advertising." Id. at 938. This process, importing those images from other web sites, is called "inline linking." "The image imported from another web site is displayed as though it is part of the current web page, surrounded by the current web page's text and advertising. As a result...the user typically would not realize that the image actually resided on another web site." Id. at 938-39. Significantly, the Ninth Circuit analyzed the reproduction of the copyrighted images in the search results separately from the display of those images as a result of both of inline linking and framing.

After finding that the facts fitted a prima facie case of copyright infringement (ownership of the copyright and copying by the defendant), the Ninth Circuit discussed the four factors balanced on a determination of the fair use defense, under 17 U.S.C. § 107, to a copyright claim: 1) Purpose and character of the use; 2) the nature of the copyrighted work; 3) the amount and substantiality of the portion used in relationship to the copyrighted work as a whole; and, 4) the effect of that use upon the potential market for the copyrighted work or its value. Kelly, supra at 940 (citations omitted). One interesting point in its analysis was the finding that defendant's use of the copyrighted images did not harm the value or market for the photographer's works because the defendant's "search

engine would guide users to Kelly's web site rather than away from it...[T]hey would ...have to go to Kelly's web site to see the full-sized image." Id. at 944.

Other major copyright issues relating to use of the Internet were addressed by the California courts when the now famous Napster web site was enjoined from allowing users to download copyrighted music files from its web site in MP3 format, in A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 55 USPQ2d 1780 (N.D. Cal. 2000), on appeal, 239 F.3d 1005 (9th Cir. 2001). As most attorneys know, the aftermath of this case resulted in the demise of Napster. The trial judge, Judge Patel, issued a preliminary injunction— which the Ninth Circuit later temporarily stayed-- in favor of the record and music companies whose songs had been copied, despite the defendant's assertion of the fair use defense under copyright law. Napster provided, free of charge, access to its proprietary software on its Internet web site which allowed sharing of MP3 music files between other users logged onto its system, using a "a peer-to-peer file-sharing system that allows Napster account holders to conduct relatively sophisticated searches for music files on the hard drives of millions of other anonymous users." Id. at 901-02. The trial court also rejected Napster's attempt to rely upon the safe harbor provision of the Digital Millennium Copyright Act, 17 U.S.C. § 512, because Napster either had actual knowledge that its activities were infringing, or was aware of facts or circumstances from which the infringing activity was apparent. Id. at 919.

The Central District of California also grappled with numerous intellectual property issues of the Internet kind, including copyright theories and the safe harbor defense under the DMCA, in Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp.2d 1146 (C.D. Cal.

2002), granting a preliminary injunction on theories of contributory infringement and vicarious infringement, but not for direct infringement, under copyright law. The plaintiff, an adult magazine, filed its suit for copyright infringement, trademark infringement, invasion of right of publicity, and unfair competition, against an internet age verification service called "Adult Check." One noteworthy point was the court's rejection of the defendant's argument that it lacked control over various web sites "because it cannot 'affirmatively work as some sort of Internet 'hall monitor,' policing an unruly class of webmasters and responding instantaneously when any copyright infringement occurs.'" Id. at 1173. The district court described the DCMA law in the following manner:

> "In 1998 Congress passed Title II of the Digital Millennium Copyright Act ("DCMA"), Pub. L. 105-304, Title II, § 202(a), 112 Stat. 2877 (1998)(codified at 17 U.S.C. § 512). The DCMA marked Congress' entry into the online copyright fray. The DCMA created a series of four 'safe harbors' to protect 'providers of online services' from liability, primarily monetary liability, based on claims of copyright infringement attributable to the actions of users. *See* 17 U.S.C. §§ 512(a)-(d), (j)."

Perfect 10, supra at 1174. Some of the issues in this case will be discussed in more detail during the seminar.

A New York federal court, in an action brought by the major motion picture studios under the Digital Millenium Copyright Act, enjoined certain Internet web site owners from posting on their site for downloading by third parties, the decryption software that allowed digitally encrypted movies to be decrypted and downloaded to a DVD, or

from including hyperlinks on their web site to other web sites that made decryption software available. Universal City Studios, Inc. v. Reimerdes, 111 F.Supp. 2d 294, 55 USPQ2d 1873 (S.D.N.Y. 2000).

C. PATENT LAW (COVERED BY NEIL A. SMITH)

D. TRADE SECRET LAW (COVERED PRIMARILY BY NEIL A. SMITH)

One subject matter for multiple trade secrets claims under California law has been the CSS encryption software owned by the DVD Copy Control Association for the protection of movie DVD's, as discussed below in more detail. In DVD Copy Control Association, Inc. v. McLaughlin, 2000 WL 48512 (Cal. Sup. Ct., Santa Clara 2000), the California trial court issued a preliminary injunction to prevent unauthorized posting on defendants' web site of a decryption software called DeCSS that was developed to decode the CSS program, holding that the DeCSS program was a protectable trade secret which appeared to have been improperly reversed engineered. "The Plaintiff has shown that the CSS is a piece of proprietary information which derived its independent economic value from not being generally known to the public and that Plaintiff made reasonable efforts to maintain its secrecy." Id. at *1. . Judge Elfving rejected the defendants' arguments that "a 40 bit encryption system is weak at best," noting that "[u]nder the law, a system to protect secrecy does not become unreasonable simply because a clever thief finds a way to penetrate the security." Id. at *1 (citation omitted). Though the court indicated that the trade secret was "obtained through reverse engineering," it cited the legislative comment to the Uniform Trade Secrets Act indicating that reverse engineering per se is not prohibited:

"'Discovery by 'reverse engineering,' that is, by starting with the known product and working backward to find the method by which it was developed,' is considered proper means. The only way in which the reverse engineering could be considered 'improper means' herein would be if whoever did the reverse engineering was subject to the click license agreement which preconditioned installation of DVD software or hardware, and prohibited reverse engineering." Id. at *2.

Under Cal. Civ. Code § 3426.1, the plaintiff "must also show that the trade secret was misappropriated, or that the trade secret was obtained through *improper means* and that the Defendants *knew or should have known* that the trade secret was obtained through improper means when posted it or its derivative to the internet." McLaughlin, supra at *2 (emphasis in original). The Court found that these elements had been shown, and that a preliminary injunction was necessary (a TRO having already been entered), because "once this information gets into the hands of an innocent party, the Plaintiff loses the ability to enjoin the use of their trade secret." Moreover, "[I]f the Court does not immediately enjoin the posting of this proprietary information, the Plaintiff's right to protect this information as secret will surely be lost, given the current power of the Internet to disseminate information and the Defendants' stated intention to do so." McLaughlin, supra at *3, citing, Religious Tech. Center v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361, 1365-66 (N.D. Cal. 1995). Further, the CSS encryption software licensed to Plaintiff "cannot simply be changed like a secret code used by a military where everyone involved simply changes to new code because millions of people own current DVDs and DVD viewing systems." McLaughlin, supra at *3.

The Court also refused to withhold trade secret protection even though the DeCSS program has already been posted on the Internet without authoritiy, because "[t]o hold otherwise would do nothing less than encourage misappropriaters of trade secrets to post the fruits of their wrongdoing on the Internet as quickly as possible and as widely as possible thereby destroying a trade secret forever. Such a holding would not be prudent in this age of the Internet." McLaughlin, supra at *3.

While the California Supreme Court did not decide the merits of the issue, it dealt with the same DeCSS software several years later in another action by the same plaintiff, the DVD Copy Control Association, on its claims of trade secret misappropriation by a different set of defendants. Pavlovich v. Superior Court, 2002 WL 31641714 (Cal. 2002).

III. DEFAMATION, RIGHT OF PRIVACY LAW AND PRIVACY OF THE INTERNET

A. OVERVIEW OF DEFAMATION LAW

The Internet, like many scientific endeavors, may be used as a tool for good or for evil. As a means of disseminating defamatory material to the largest possible number of third parties with the greatest speed, it is almost a nonpareil, and is exceedingly difficult to control or prevent once it has occurred. It should come as no surprise, therefore, that a rath of cases have confronted claims based upon misuse of the Internet to say bad things about people and businesses.

B. OVERVIEW OF PUBLICITY AND PRIVACY LAW

The Ninth Circuit recently commented on the importance of privacy during electronic communications, and problems with privacy currently on the Internet:

> "In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately. Cellular phones are subject to monitoring, email is easily intercepted, and transactions over the internet are often less than secure. Something as commonplace as furnishing our credit card number, social security number, or bank account puts each of us at risk. Moreover, when we employ electronic methods of communication, we often leave electronic 'fingerprints' behind, fingerprints than can be traced back to us. Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb."

Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132, 1145-46 (9th Cir. 1999).

C. SPECIAL PROBLEMS OF DEFAMATION, RIGHT OF PUBLICITY AND PRIVACY LAW ON THE INTERNET

The Internet developed initially as a means of scholarly exchange of ideas and criticism, and has a special role in the development and free flow of information throughout not only the scientific and educational communities of the world, but also the

masses themselves. There is always a balance between the Internet's fundamental purpose and various proprietary rights of individuals and businesses.

Indeed, those who challenge an Internet web site's owner in court, often seem to find themselves on the receiving end of a lot of negative publicity generated in large part by the offending web site's own content directed at the challenger. Thus, when Playboy sued former Playmate of the Year, Terri Welles, she in turn "included discussions of the suit and criticism of [Playboy] on her website...". This is a fairly common tactic of web site owners who are legally attacked, at least from the experience of this author with his own Internet clients. For example, a law professor at Case Western Reserve Univesity School of Law challenged the government's enforcement of export regulations directed at encryption software, and "his web sites also set out documents involved with this lawsuit. Plaintiff Junger uses his web site to describe the process of this litigation through press releases and filed materials." Junger v. Daley, 3 F. Supp.2d 708, 714 (N.D.Ohio 1998).

Indeed, a part of the settlement of an Internet dispute may and often does include a demand that the web site remove the commentary from its web site, despite obvious First Amendment rights. One might, for example, learn more about a lawsuit or how it was resolved by visiting the parties' web site, and seeing what is not there. On the author's web site, www.levinhawes.com, a number of press releases about large damages being sought in intellectual property law cases, are later either completely removed, or result in confidential settlements where nothing further is said at some point after the suit is filed. There are also many settlements of Internet disputes which are largely driven by a large company's desire to avoid negative Internet publicity.

Encryption software, and the government's attempts to regulate it, has engendered special problems relating to rights of privacy and the First Amendment's protection of free speech as discussed below, and in such cases as Bernstein v. U. S. Dept. of State, 974 F. Supp. 1288 (N.D. Cal. 1997), affirmed, Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132 (9th Cir. 1999). As Judge Fletcher stated about the unique role of encryption software in the area of privacy on the Internet: "The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost [in electronic communications]. Government efforts to control encryption thus may well implicate...the constitutional rights of each of us as potential recipient's of encryption's bounty....[W]e leave for another day the resolution of these difficult issues...". Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132, 1146 (9th Cir. 1999). Similarly, decryption software sometimes pits the interests of individuals in exercising free speech and engaging in scientific research against those of protecting entire industries that rely upon encryption to minimize or eliminate rampant copying of copyrighted materials. See, e.g., Pavlovich v. Superior Court, 2002 WL 31641714 (Cal. 2002)(use of DeCSS decryption software posted on a web site by a Purdue University student supporting open source programming).

IV. PERSONAL JURISDICTION IN THE INTERNET WORLD (COVERED BY NEIL A. SMITH)

One of the most recent pronouncements in California on this topic came from the California Supreme Court in Pavlovich v. Superior Court, 2002 WL 31641714 (Cal. 2002), which held that mere knowledge that the tortious conduct may harm certain industries in California (such as the motion motion, computer or consumer electronics industries), is

insufficient to establish targeting in California, that is, "purposeful availablement" under the effects test, and the mere posting of information on a passive web set accessible to California users is insufficient. The Court appeared to favor the "sliding scale analysis" used in Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997).

Other relevant citations include Jewish Defense Orgnanization, Inc. v. Superior Court, 72 Cal. App. 4th 1045, 85 Cal. Rptr.2d 6111 (Cal. 4th Dist. 1999); Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414 (9th Cir. 1997); GTE New Media Services Inc. v. Ameritech Corp., 21 F.Supp.2d 27 (D.C. Cir. 1998).

V. ETHICAL CONSIDERATION (ALSO COVERED BY NEIL A. SMITH)

A. ATTORNEY-CLIENT INTERACTION ON THE INTERNET

B. CONFLICTS OF INTEREST

C. EMAIL COMMUNICATIONS, CLIENT CONFIDENTIALITY AND PRIVILEGE

VI. ELECTRONIC COMMERCE

A. WHAT IS ELECTRONIC COMMERCE

Electronic commerce currently includes essentially all communications and transactions made using the Interent, whether email communications sent on the Internet, or postings to electronic bulletin boards, Internet auctions of different types, electronic chat rooms, placing email or web site orders for merchandise, and many communications now made by cellular phones, digital or not, and Palm Pilot or other personal assistant devices ("PDA's). Indeed, most of us now only have telephones that must be plugged in to operate at all, coupled with an answering machine containing a computer chip, making our lives totally dependent upon electronic devices, not just the computer. Though, as to computers, it is hard to imagine how many lawyers could function without the ubiquitous computer rather than the erstwhile typewriter or dictating equipment. In commercial transactions, the Internet has many advantages over fax machines and snail mail (i.e., regular first class mail or even overnight mail) and courier services no matter how fast. The Uniform Commercial Code was not really intended to address the issues involved in the electronic commerce that reigns today in the business world. Even the former cocktail napkin deal of former business lore is today replaced laptop computer print outs, or emails sent from a PDA.

Lawyers too are constantly engaged in electronic commerce. Don't most of now communicate with clients by email and over the Internet. With our own colleagues? The Internet is certainly now one of the main methods of attracting new clients, and web sites can capture, or drive away, millions of dollars of business a year. Even the court's dockets

can now normally be accessed via the Internet, such as by using Pacer, and tentative rulings and orders are obtained quicker at the court's web site than by mail. Courts and lawyers use the Internet to do both factual and legal research far more effectively, and certainly more rapidly, than traditional methods from even a few years ago. Even legal research is done through a web site, such as www.westlaw.com, normally now rather than using software on one's computer to gain access over a computer modem to a legal publisher's electronic database.

B. BASIC CONTRACT PROVISIONS (COVERED BY NEIL A. SMITH)

C. DIGITAL SIGNATURES (COVERED BY NEIL A. SMITH)

D. ENCRYPTION AND SECURITY ISSUES

a. Network Security

Network security entails such traditional security as the creation of a firewall to prevent unauthorized electronic access by third parties, to the installation of appropriate virus software to preclude electronic viruses, identify and diagnose them, and quarantine them if they infect a computer or a portion of its data or applications. Law firms, among others, cannot afford to allow someone hack into their computer network and access all of the files contained on the computers within that network. Hence, encryption and other security software designed to prevent such access is critical to network security. In an antitrust action brought by U.S. Department of Justice against several leading educational publishers, the District of Columbia federal court dealt, among other things, with use of the

Internet for the administration of educational testing, and observed that while "the Internet may be used to deliver tests to individual testing centers or to an entire network, the security required for high stakes examinations still requires that they be administered in a secure, proctored environment. Currently, the technology is not available to enable test proctoring via the Internet." U.S. v. Thompson Corp., 2001 WL 761237 (Dist. of Col. 2001).

b. Encryption – How Secret is Secret

Encryption of electronic communications and software and data available on the Internet germinated in the ancient science of cryptography, but poses novel and special issues on the Internet. In one recent case involving an encryption program known as Snuffle, the Ninth Circuit reviewed what cryptography and encryption are all about:

> "Cryptography is the science of secret writing, a science that has roots stretching back hundreds, and perhaps thousands, of years. For much of its years, cryptography has been the jealously guarded province of governments and militaries. In the past twenty years, however, the science has blossomed in the civilian sphere, driven by [in part]...the needs of modern communication and information technologies. It is the cryptographer's primary task to find secure methods to encrypt messages, making them unintelligible to all except the intended recipients."

Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132, 1136-37 (9th Cir. 1999)(citations omitted).

As the Court pointed out, encryption deals not only with safeguarding secrecy: "[E]ncryption can also be employed to ensure data integrity, authenticate users, and facilitate nonrepudiation (e.g., linking a specific message to a specific sender." Id. at 1137 (citations omitted).

It is necessary from many legal perspectives to insure, within reason, that electronic communications on the Internet, such as emails, and data and programs made available on the Internet or on one's own web site, are secure and cannot be accessed by those for whom they are not intended, or by anyone having Internet access. For example, attorney-client communications sent by email obviously require security and secrecy in order to avoid waiver of the privilege, and trade secrets may lose their status due to failure to take reasonable steps to safeguard their secrecy if posted on the Internet or available on the owner's or licensees web sites without adequate safeguards. One Internet issue, therefore, is how secure such communications and data must be in order to maintain their status relative to various secrecy requirements.

There is also tension with the government or military's desire to be able to encrypt certain communications for a variety of reasons, because, "[f]or example, encryption can be used to conceal communications of terrorists, drug smugglers, or others intent on taking hostile action against U.S. facilities, personnel, or security interests." Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132, 1137 (9th Cir. 1999). The Ninth Circuit aptly observed that "as increasingly sophisticated and secure encryption methods are developed [such as the Snuggle program], the government's interest in halting or slowing the proliferation of such methods has grown keen." Id. Naturally, interest in programs to decrypt such encrypted

data has also increased. After September 11, 2001, the government's interest in monitoring communications between terrorists has certainly solidified, while such terrorists would be focused on sending communications that cannot be decrypted by the government or others.

In DVD Copy Control Association, Inc. v. McLaughlin, 2000 WL 48512 (Cal. Sup. Ct., Santa Clara 2000), a California trial court granted a preliminary injunction against posting of the DeCSS decryption program, finding the program it decoded, CSS, constituted a protectable trade secret under California law. Judge Elfving rejected the defendants' arguments that "a 40 bit encryption system is weak at best," noting that "[u]nder the law, a system to protect secrecy does not become unreasonable simply because a clever thief finds a way to penetrate the security." Id. at *1 (citation omitted). Though the court indicated that the trade secret was "obtained through reverse engineering," it cited the legislative comment to the Uniform Trade Secrets Act indicating that reverse engineering per se is not prohibited: "'Discovery by 'reverse engineering,' that is, by starting with the known product and working backward to find the method by which it was developed,' is considered proper means. The only way in which the reverse engineering could be considered 'improper means' herein would be if whoever did the reverse engineering was subject to the click license agreement which preconditioned installation of DVD software or hardware, and prohibited reverse engineering." Id. at *2.

c. Legislative Efforts Concerning Encryption

The federal government has sought to regulate encryption software for a number of reasons, some of which are discussed below, including exportation of such software. Many of the government's concerns focus on the secrecy applications of such software: "The interception and deciphering of foreign communications has long played an important part in our nation's national security efforts." Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132, 1137 (9th Cir. 1999). Thus, the federal government has adopted "specific regulations to control the export of encryption software, expressly including computer source code. Encryption software is treated differently from other software in a number of significant ways. First, the term 'export' is specifically broadened with respect to encryption software to preclude the use of the internet and other global mediums if such publication would allow passive or active access by a foreign national within the United States or anyone outside the United States." Bernstein, supra at 1137 (9th Cir. 1999). These Export Administration Regulations can be in 15 C.F.R. § 730 et seq., and, as indicated above, Internet publications are expressly covered: Export includes "downloading or causing the downloading of , such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S. or making such software available for transfer outside the United States...". 15 C.F.R.§ 734.2(b)(9)(B)(ii). Balanced against the government's need to regulate encryption software for national security and other reasons, are the rights of individuals and businesses to develop such software to protect their communications and express themselves freely without fear of government censure. As an Ohio federal court observed, while upholding the

constitutionality of the regulations as applied to a computer law professor, in general under the EAR, "almost any posting of software on the Internet is an export." Junger v. Daley, 3 F. Supp.2d 708, 713 (N.D.Ohio 1998).

Judge Patel, of the Northern District of California, struggled, in a trilogy of cases which pitted a mathematician student at Berkeley specializing in cryptography against the federal government's legislation aimed at nonmilitary encryption products, with the constitutionality of certain regulations directed at encryption software, culminating in Bernstein v. U. S. Dept. of State, 974 F. Supp. 1288 (N.D. Cal. 1997)(*Bernstein III*), affirmed, Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132 (9th Cir. 1999).

The Court first defined encryption as follows:

> Encryption basically involves running a readable message known as "plaintext" through a computer program that translates the message according to an equation or algorithm into unreadable "ciphertext." Decryption is the translation back to plaintext when the message is received by someone with an appropriate "key." The message is both encrypted and decrypted by compatible keys. The users of cryptography are far-ranging in an electronic age, from protecting personal messages over the Internet and transactions on bank ATM's to ensuring the secrecy of military intelligence.

Bernstein III, supra at 1292 (N.D. Cal. 1997)(footnote omitted).

Plaintiff Bernstein claimed that his First Amendment rights were violated because he was "not free to teach, publish, or discuss with other scientists his theories on cryptography embodied in his Snuffle [encryption] program" due to the regulations of

encryption enacted to enforce the Arms Export Control Act ("AECA"), 22 U.S.C. § 2778 (1990) and the International Traffic in Arms Regulations ("ITAR"), 22 CFR Pts. 120-30 (1994). In earlier decisions involving the same parties, the Court had held that the source code constituted protected speech under the First Amendment, Bernstein v. U. S. Dept. of State, 922 F. Supp. 1426 (N.D.Cal. 1996)(*Bernstein I*), and that the ITAR's licensing requirements for the encryption software was an unlawful prior restraint on free speech. Bernstein v. U.S. Dept. of State, 945 F. Supp. 1279 (N.D.Cal. 1996)(*Bernstein II*). Then, President Clinton transferred jurisdiction over the subject matter from the Department of State to the Department of Comerce. In so doing, the accompanying White House press release emphasized that "export of encryption software, like the export of other encryption products described in this section, must be controlled because of such software's functional capacity, rather than because of any possible informational value of such software...". Bernstein III, supra at 1293-94. The new encryption regulations then enacted were also found by Judge Patel to be "an unconstitutional prior restrain in violation of the First Amendment." Id. at 1308. Despite the finding that the regulations were unconstitutional on their face, the Court opted to implement a narrow injunction, running only to preclude enforcement of the encryption regulations against "plaintiff or against anyone who seeks to use, discuss or publish plaintiff's encryption program." Id. at 1310.

The Ninth Circuit, in affirming Judge Patel's Bernstein III decision, agreed that the regulations in question, certain Export Administration Regulations ("EAR"), constituted a prior restraint on speech that violated the First Amendment, but used "a somewhat narrower rationale than did the district court...". Bernstein v. U.S. Dept. of Justice, 176

F.3d 1132, 1135 (9th Cir. 1999)(*Bernstein IV*). The Court described the encryption program Bernstein developed, Snuffle, as "an encryption method—'a zero-delay private-key stream encryptor based upon a one-way hash function.'" Id. For those who are not mavens at cryptology, the Court elucidated "hash function" as a term that "describes a function that transforms an input into a unique output of fixed (and usually smaller) size that is dependent on the input." Id. at 1136 n. 1. A "one-way hash function" was described as one that was "impossible to derive the input data given only the hash function's output," useful for such purposes as error checking and digital signatures. The "zero-delay" denoted that the Snuffle program "can be used for interactive communications because it encrypts and decrypts on a character-by-character basis—the users need not complete an entire message before encrypting and sending." Id. The Ninth Circuit concurred that "encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes," though it indicated its ruling did not extend to object code. Id. at 1141. Indeed, the Ninth Circuit emphasized, as did Judge Patel previously, the narrowness of its holding: "We do not hold that all software is expressive. Much of it surely is not." Id. at 1145.

Other federal courts have, however, upheld the constitutionality of EAR regulations enforcing export controls over encryption software, and expressly disagreed with the district court's rationale in the Bernstein cases. See Junger v. Daley, 3 F. Supp.2d 708 (N.D.Ohio 1998)(the source code was not expression under the First Amendment, and the regulations did not constitute an unconstitutioinal prior restraint).

Judge Patel also touched upon private industry's attempts to regulate and develop encryption software and specifications in the music industry, in the seminal case of A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 55 USPQ2d 1780 (N.D. Cal. 2000), though the primary issue before her related to the distribution over the Internet of copyrighted music. The Secure Digital Music Initiative ("SDMI"), which she described as "a forum that brings together interested parties to develop technology specifications for protecting the distribution of digital media," was planning to utilize both encryption and watermarking. Judge Patel noted that "[e]ncryption software has limitations.... For example, encrypted CDs will not function in existing CD players because the players will not be able to read them. Thus, consumers will have to purchase new CD players to listen to encrypted CD music. Also, encryption technology will provide only prospective protection because it will not affect existing discs." Napster, supra at 927.

A New York federal court, in an action brought by the major motion picture studios under the Digital Millenium Copyright Act, enjoined certain Internet web site owners from posting on their site for downloading by third parties, the decryption software that allowed digitally encrypted movies to be decrypted and downloaded to a DVD, or from including hyperlinks on their web site to other web sites that made decryption software available. Universal City Studios, Inc. v. Reimerdes, 111 F.Supp. 2d 294, 55 USPQ2d 1873 (S.D.N.Y. 2000). The defendants' decryption program, called DeCSS, where the program being decrypted was called CSS, was described as one that "allows CSS-protected motion pictures to be copied and played on devices that lack the licensed decryption technology." Id. at 303.

The California Supreme Court addressed personal jurisdiction issues for misappropriation of trade secrets involving a web site operator who posted the same DeCSS decryption software on an Indiana web site in Pavlovich v. Superior Court, 2002 WL 31641714 (Cal. 2002), where the defendant's "sole contact with California is LiVid's [www.livid.on.openprojects.net] posting of the DeCSS source code containing DVD CCA's [DVD Copy Control Association, Inc.] proprietary information on an Internet Web site accessible to any person with Internet access." Id. at *7.

The Court first described the development of the encryption software for DVD's (digital versatile discs) as follows: "Before the commercial release of DVD's containing motion pictures, the Content Scrambling System (CSS), a system used to encrypt and protect copyrighted motion pictures on DVD's, was developed. The CSS technology prevents the playing or copying of copyrighted motion pictures on DVD's without the algorithms and keys necessary to decrypt the data stored on the disc." Pavlovich, supra at *1. As to the real party in interest, DVD Copy Control Association, Inc. (DVD CCA), it is "a nonprofit trade association organized under the laws of Delaware with its principal place of business in California. The DVD industry created DVD CCA in December 1998 to control and administer licensing of the CSS technology." Id. The defendant Pavlovich was the project leader, while a student at Purdue University in Indiana, of the LiVid video project which operated a Web site with a single page with links to other sites. Livid's goal was to further the Linux model of software including promotion of open source code. "To reach this goal, the project sought to defeat the CSS technology and enable the decryption and copying of DVD's containing motion pictures. ...Livid posted the [DeCSS] source

code...on its Web site.... DeCSS allows users to circumvent the CSS technology by decrypting data contained in DVD's and enabling the placement of this decrypted data onto computer hard drives or other storage media." Pavlovich, supra at *2.

Unfortunately, the California Supreme Court never reached the merits of the the claims, only holding that California was not an appropriate forum to decide the issues: "DVD CCA has the ability and resources to pursue Pavlovich in another forum such as Indiana or Texas. Our decision today does not foreclose it from doing so. Pavlovich may still face the music—just not in California." Id. at *10. Ironically, as a dissenting judge pointed out, the DVD industry had the nettlesome job of trying to put the DeCSS horse back in the barn after it had already romped around the world via the Internet: "As early as October 25, 1999, Jon Johansen, a resident of Norway, posted on the Internet ...DeCSS... DeCSS was derived by 'willfully hacking and/or improperly reverse engineering [CSS] software'...Thereafter, many other Web sites 'in at least 11 states and 11 countries' either posted the code directly or provided links to the sites where it appeared directly... The Motion Picture Association sent cease and desist notices to some 66 Web sites and Internet service providers...". Pavlovich, supra at *12 (Baxter, J., dissenting). Indeed, it may be argued that once such a decryption becomes widely available on the Internet, it may simply be too late to prevent the damage from occurring. Trying to stop the viral efforts of a wide-spread Internet posting like this one would be akin to cleaning up the proverbial Augean stables.

Various lawsuits have been filed around the country involving this same DeCSS software. However, California courts have also addressed the protectability of other kinds

of encryption software. For example, in RSA Data Secruity, Inc. v. 1-Link, Ltd., 1998 WL 827415 (N.D. Cal. 1998), Judge Smith granted summary judgment to the a company which "develops encryption software tools which secure the electronic transmission of information and licenses its products primarily to original equipment manufacturers (OEM's)." Id. at *1.

d. Encryption and Attorney/Client Privilege

Encryption software has clear implications for attorney-client communications and whether there is a waiver of the attorney-client privilege if such communications are not reasonably secure. In today's electronic world, to preserve the privilege may require some type of encryption software so that third parties may not easily intercept and decipher such communications over the Internet between lawyers and their clients and control groups. Some of these issues are discussed below under the subject matter of attorney-client privilege and email communications.

E. UNIQUE BUSINESS-TO-BUSINESS AND BUSINESS-TO-CONSUMER ISSUES

Any number of business issues relating to the Internet have been litigated in courts throughout the country. See, e.g., BCI Telecom Holding, Inc. v. Jones Intercable, Inc., 3 F. Supp. 2d 1165 (D. Col. 1998)(suit between major shareholders over agreement between affiliates to provide an Internet access service on a cable television system); GTE New Media Services Inc. v. Ameritech Corp., 21 F.Supp.2d 27 (D.C. 1998)(suit by telecommunications company under Sherman and Clayton Acts against various local telephone companies on the basis that they had tried to monopolize the Internet Yellow Pages market); Pavlovich v. Superior Court, 2002 WL 31641714 (Cal. 2002) (misappropriation of trade secrets due to posting of DeCSS decryption software allowing circumvention of CSS encryption software protecting movies on DVD's).