

**RECENT DEVELOPMENTS:
INTELLECTUAL PROPERTY LAW AND THE INTERNET**

by: Andrew R. Basile, Jr.¹
Cooley Godward LLP

I. INTRODUCTION

A. SCOPE AND PURPOSE OF THIS DOCUMENT

This paper reviews developments in U.S. intellectual property law during the period June 1999 through June 2000 as they relate to the Internet and electronic commerce. For each substantive area, a “background” section is provided reviewing major developments prior to June 1999.

B. HISTORY OF THE INTERNET

In the 1960s, the U.S. Department of Defense began funding research into packet-switching technology and communications networks. This research led to the *ARPANET*. *ARPANET* later evolved into what is now known as the *Internet*.

The Internet is a network of disparate components -- or hosts -- which are not under central control. Communications between hosts are made possible by each host's voluntary adherence to a set of shared protocols known as TCP/IP.

The infrastructure of this remarkable network began to take shape in the 1960s with the work of the late Dr. Jon Postel, then a graduate student at UCLA. Postel handled the administrative details of the old *ARPANET*, maintaining a list of host names and addresses and also tracking comments prepared by other researchers. Postel's collection of comments came to define in part the technical parameters of the Internet and to this day are known as Requests for Comments (*RFCs*).

Postel's role grew throughout the 1970s. He became a government contractor and, as his network management responsibilities expanded, he delegated some tasks to other contractors. The function handled by Postel and other contractors was known as the Internet Assigned Numbers Authority (*IANA*).

Despite its name, *IANA* was more of an “initiative” or a “program” rather than a *de jure* institution or authority. In a sense, *IANA* existed merely as a label for the coordinated efforts of Postel, government agencies, academia and other groups. It operated on an *ad hoc* basis, albeit with the aura of government authority brought to bear by grants and contracts from the Department of Defense and, later, the National Science Foundation. *IANA* drew its legitimacy not from any

¹ Copyright © 1999, 2000 Andrew R. Basile, Jr. All rights reserved. The author gratefully acknowledges the assistance of Helena Ku in preparing this document.

government edict but from the personal leadership of insiders like Postel and from the mere fact that “it” collected, controlled and disseminated the databases of addresses and technical parameters that defined the Internet.

This loose management structure was appropriate and sufficient when the Internet was used by a limited number of academics and government agencies. It was, however, ill-equipped to handle the complex issues that arose in the 1990s, when commercial and consumer use of the Internet increased dramatically. From trademark disputes, to controversies over obscenity, to concerns of business as to the security and reliability of the Internet, these complex issues have proved especially difficult to resolve in the absence of private or public authority to govern the Internet.

C. The World Wide Web and Electronic Commerce

The World Wide Web is a common name for a subset of Internet-based resources that are available under the hypertext transfer protocol (*http*). Files communicated under this protocol are formatted using hypertext mark-up language (*html*), which allows the files to be displayed with an easy-to-use, graphic user interface. Files formatted with *html* can have interactive functionalities (such as online form entry) and can be interfaced with other software systems to allow Internet users access to general business systems (*e.g.*, order entry and fulfillment systems).

The World Wide Web provides a cheaper, faster and more productive means to communicate and access information, and in so doing promises to eliminate costly traditional offline processes and to generally facilitate commerce. Some ways in which the Web impacts commerce are:

- **paper** (not needed when goods and documents are distributed online)
- **communication** (one email replaces multiple phone calls)
- **convergence** (eliminates disparate analog communications channels)
- **distribution** (content can be moved electronically)
- **travel** (video conferencing takes place of personal visit)
- **physical plant** (online services do not require retail storefront)
- **call centers** (Web automates transactions traditionally handled by telephone)
- **intermediaries** (no need for agents when buyers find sellers online)
- **mail and delivery** (parties can use email as an alternative to paper mail)
- **research** (keyword search replaces trip to library)
- **data entry and processing** (no manual handling once user enters data)
- **competition** (buyers have better information about price and other market conditions)
- **contracting** (parties digitally sign documents over the Internet)
- **payment processing** (bill presentment and payment are automated)

- **customized marketing** (sellers use information about the customer to tailor pitch)
- **global reach** (seamless access to worldwide markets)

The Internet wrings cost out of the economy while enhancing personal and commercial productivity and promoting value-adding exchange. The bottom line: consumers and business can accomplish more tasks faster and using fewer resources. It is a boon to buyers and consumers, but will usher in an era of ever-fiercer competition for providers of goods and services. The Internet also threatens certain vested interest both economically (*e.g.*, by eliminating some types of business and occupations) and politically (*e.g.*, by allowing easier access to legislative process).

The impact of the Internet is and will continue to be enormous. Some estimates are that Internet-related activities contributed over US\$300 billion to the U.S. GDP in 1998, creating over 1.2 million jobs. That is an exponential increase from 1994, when the sector was estimated to be only US\$5 billion. Sales of goods and services over online channels are already estimated, on a conservative basis, to exceed an annual rate of US\$100 billion.

D. LEGAL IMPLICATIONS

The legal issues raised by the Internet and electronic commerce fall into several broad categories:

- intellectual property (the subject of this paper)
- online contracting (*e.g.*, digital signatures)
- privacy (who should have access to personal information and for what purposes?)
- regulation of online content and conduct (*e.g.*, gambling, spam and pornography)
- jurisdiction (*e.g.*, where can one be sued? which country's law applies?)
- security (*e.g.*, encryption, espionage, intrusion, viruses and tampering)
- financial transactions (*e.g.*, online payment and securities trading)

E. ADDITIONAL RESOURCES

Internet Governance

Internet Corporation for Assigned Names and Numbers www.icann.org/

Internet Assigned Numbers Authority www.iana.com/

Internet Engineering Task Force <http://www.ietf.cnri.reston.va.us/home.html>

Internet Society www.isoc.org/

Network Solutions, Inc. www.networksolutions.com/

U.S. Department of Commerce www.ntia.doc.gov

Electronic Commerce

Current Events www.news.com

Statistics www.nua.ie/surveys/

II. TRADEMARKS

A. OVERVIEW

The period 1999 through 2000 marked significant progress in the development of the law protecting trademarks online. ICANN established control over the domain name system and imposed a new uniform global dispute resolution policy, including mandatory arbitration, that supplanted the controversial Network Solutions policy. Congress enacted an anti-cybersquatting statute and provided *in rem* jurisdiction for certain domain name cases.

B. BACKGROUND

1. The Domain Name System

Every computer connected to the Internet is assigned a numeric address, which the other computers on the network use to route messages to that computer. A typical numeric Internet address is *200.98.102.23*. These addresses are difficult for humans to remember, so in the 1980s, a group of engineers working under government contracts developed the Domain Name System (*DNS*), under which an alpha-numeric address is assigned to each numeric addresses. These alphanumeric addresses are called *domain names*. Examples of domain names include *whitehouse.gov* and *microsoft.com*.

The DNS is constructed as a hierarchy, having top-level domains (*TLDs*) such as *.com* and second-level domains such as *microsoft* within each of the TLDs. TLDs fall into two categories: country-specific and generic. Country-specific TLDs are denoted by two-character country codes such as *.uk* for “United Kingdom” and are generally assigned to persons and businesses residing in the specified country. Generic TLDs (*gTLDs*) are not limited to a specific country, but rather are based on the type of entity using the domain name. For example, the *.com* gTLD is intended for use by commercial enterprises, the *.org* gTLD is intended for non-profit organizations, and the *.edu* gTLD is intended for educational institutions. Second-level domains under each TLD are assigned to users upon request on a first-come, first-served basis.

To avoid assigning the same domain name to multiple users, the DNS provides for a single, authoritative directory (or *register*) of domain names. Copies of this directory are distributed over the Internet via 13 *root servers* located throughout the world. The primary root server is

designated as the “A” server. Changes to the A server are automatically replicated to the other 12 servers. When a user enters a particular domain name, its host computer resolves that domain name into a numeric IP address – that is, looks up the domain name in one of the 13 root servers. An organization that maintains the authoritative directory is a *registry*. An organization that processes additions, changes and deletions to the directory is a *registrar*.

The DNS has been fostered and financed in large part by the U.S. Government through grants and procurement contracts. In 1991, the National Science Foundation (*NSF*) took over administration of these grants with respect to non-military portions of the Internet. *NSF* contracted out administration of the DNS to a private company, Network Solutions, Inc. Under this arrangement, Network Solutions has had sole physical control over the “A” root server and, as a consequence, the registry for *.com* and the other gTLDs. Network Solutions was also the sole *registrar* for the gTLDs. That is, Network Solutions had a monopoly on the registrar services of adding, changing and deleting second-level domain names in *.com* and the other gTLDs.

Initially, Network Solutions operated in relative obscurity, performing an important but uncontroversial administrative function. Few people gave much thought to domain names. They were like telephone numbers – so long as each one was unique, they allowed the Internet to function. Apart from that, domain names had little significance and were often chosen by technical personnel who paid little or no attention to marketing considerations. For example, a typical domain name ten years ago might have been *mainserver2.utext.comsi.edu*. Commensurate with the seeming immateriality of domain names, Network Solutions adopted a policy of registering them on request on a first-come, first-served basis, without regard to trademark considerations.

The significance of domain names increased dramatically with the advent of the World Wide Web as an advertising channel and marketplace. Because consumers use domain names to locate Web resources, companies doing business online require domain names that are easy to remember and that relate to their products, trade names and trademarks. For example, a florist would find the domain name *flowers.com* very valuable. Likewise, owners of famous trademarks such as *Microsoft* want to use those trademarks as domain names (*e.g., microsoft.com*).

Competition to register the most desirable domain names was particularly acute because of the convention (more custom than legal rule) that parties doing business on the Internet register their domain names only under the *.com* gTLD (as opposed to, for example, a country-specific designation such as *.us*). This arbitrary constraint has meant that a particular word or trademark (such as *golf*) is available for use by only one user as a

commercial domain name. This limitation, in turn, has sparked disputes over domain names between companies with legitimate claims to, or desires for, the same name.

A scarcity of domain names also led to the practice of *domain name hijacking*. Domain name hijackers (or *cybersquatters*) were individuals who registered famous trademarks as domain names (e.g., *mcdonalds.com*), often with the goal of reselling the domain name to the owner of the trademark. In essence, the domain name hijackers exploited trademark owners' delay in registering their trademarks as domain names. Many companies -- including McDonald's Corporation -- were embarrassed and angered to discover that their trademarks were being used without permission as domain names. Trademark owners began suing domain name hijackers for trademark infringement and dilution, resulting in numerous reported decisions. See, e.g., *MTV Networks v. Curry*, 867 F. Supp. 202 (S.D.N.Y. 1994).

Network Solutions quickly found itself embroiled in disputes between trademark owners and domain name users. In an effort to stave off litigation, it adopted a Domain Name Dispute Policy in 1995 for handling trademark disputes. Under this policy, the owner of a trademark registration in the U.S. or abroad could file an objection with Network Solutions if another party was using the trademark as a domain name. The domain name user was then required to show within 30 days that it also had a trademark registration (in any country) identical to the contested domain name, and to post a bond (payable to Network Solutions) sufficient to cover any damages sought by the complaining party.

If the domain name user could not post bond and produce a trademark registration, then the domain name was suspended (or placed into a "hold" status) until the dispute was resolved by court order. Unfortunately, the 1995 policy statement did little to prevent trademark disputes. In fact, because the policy was skewed in favor of trademark registrants, it opened the door to a new type of dispute -- reverse domain name hijacking -- whereby a party with a trademark registration was able to cause Network Solutions to place a domain name into a hold status, even if the use of the domain name was completely lawful. In a number of these cases, domain name holders sued Network Solutions to prevent it from placing their domain names into hold status. See, e.g., *Roadrunner Computer Sys., Inc. v. Network Solutions, Inc.* Case No. 96-413-A (E.D. Va. amended complaint filed Apr. 1, 1996).

In 1996, Network Solutions amended its Domain Name Dispute Policy in an attempt to further insulate itself from litigation. Central to the 1996 amendments was a new procedure governing treatment of domain names that were the subject of litigation. Under this procedure Network Solutions would not place a domain name on hold if either the domain

name holder or the trademark owner filed a lawsuit. Instead, Network Solutions would “deposit control of the domain name into the registry of the court.” The policy was revised in 1998 to specify, among other matters, that once litigation was initiated by either party, that Network Solutions would freeze the status quo. That is, a domain name on hold at the time litigation was filed would remain on hold, while a domain not on hold at the time litigation was filed would remain active.

By 1996, there was widespread dissatisfaction among trademark owners and Internet users with regard to the DNS generally and in particular with Network Solutions’ policy and its *de facto* monopoly as both registry of gTLDs and registrar for adding new second-level domain names to the gTLDs. This dissatisfaction spawned an “AlterNIC” movement to create new gTLDs (such as *.web*) outside of the auspices of Network Solutions. The new movement was seen as a breakdown in the Internet’s fragile chain of command, raising fears that the Internet was falling out of control: a gentleman’s agreement among an extraordinarily large number of users and institutions, with no mechanism for establishing and enforcing legal and other policies.²

In response to these concerns, members of the Internet community created the International Ad Hoc Committee (IAHC) in May 1996 to address domain name trademark issues. Although the IAHC was endorsed by IANA and the Internet Society -- two groups then recognized as leaders in the Internet community -- IAHC was, as its name suggested, a self-appointed group with no real legal authority.

IAHC issued a draft plan in December 1996 to revamp the DNS. IAHC proposed to create seven new gTLDs to be operated by a consortium of private domain registrars called the Council of Registrars. Policies were to be set by a separate body, the Policy Oversight Committee. Although IAHC’s proposals were essentially sound, IAHC became embroiled in controversy and was never able to forge sufficient consensus among the interested parties to implement its plans. IAHC was no longer active by 1997.

² During 1998 and 1999, NSI staved off a number of legal challenges to its practices and position as the sole registrar of gTLDs, including: *Beverly v. Network Solutions, Inc.*, 49 U.S.P.Q.2d 1567 (N.D. Cal. 1998) (holding that plaintiff could not establish civil conspiracy in violation of the Sherman Act because Network Solutions, in placing plaintiff’s domain name on hold, had not entered into any agreement for an unlawful purpose); *pgMedia v. Network Solutions, Inc.*, 51 F. Supp. 2d 389 (S.D.N.Y. 1999) (holding that Network Solutions was immune under the Federal Instrumentality Immunity Doctrine, which provides that companies contracted by the Government are entitled to the same antitrust immunity as the Government itself and rejecting argument that top-level domain names are entitled to First Amendment protection); and *Thomas v. Network Solutions, Inc.*, 176 F.3d 500, (D.C. Cir. 1999) *cert. denied*, 120 S.Ct. 934 (2000) (upholding as constitutional fees collected by Network Solutions for payment to the National Science Foundation where fee had been ratified by Congressional action).

After the collapse of IAHC, the U.S. Government, under the auspices of the NSF, fostered the creation in 1998 of a non-for-profit corporation known as the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN was intended -- and in large part has succeeded -- in taking control of the Internet domain name and numbering systems. As described below, ICANN has adopted a new domain name dispute resolution policy and sanctioned competing private companies to perform the domain name registration services previously handled exclusively by NSI.

2. Cases Before June 1999

Disputes between trademark owners and domain name users have festered since the inception of the World Wide Web. In general terms, these disputes involved either claims by trademark owners of cybersquatting or claims by domain name holders of reverse domain name hijacking.

By 1998, a new kind of online trademark dispute had emerged involving *metatags*. Metatags are html fields that are not displayed to end users but are detected and indexed by search engines. As a result, customers seeking the proprietor of a trademark on the Web could be led by a search engine to the third-party Web site. For example, in *Brookfield Communications, Inc. v. West Coast Entertainment Corporation*, 174 F.3d 1036 (9th Cir. 1999), defendant, a competitor of plaintiff, placed plaintiff's trademark in defendant's Web site as a metatag. In finding infringement, the Ninth Circuit relied on an *initial interest confusion* theory. According to the court, customers searching for the trademarked product would abandon their efforts after they stumbled upon the defendant's competing site. The use of another's trademark in a metatag was tantamount to the defendant posting a competitor's trademark outside of a retail store. While customers in that case may resolve the confusion prior to purchase, the confusing use of the mark has the effect of bringing the customer into the infringer's store in the first place.

Trademark owners also faced a new type of hijacking threat which involved the use as domain names of common misspellings of famous trademarks (*e.g. mcrosoft.com*). Owners of these domain names hoped to capture traffic when users intending to access a trademark owner's site made typographical errors in entering trademark as a domain name. In *Paine Weber, Inc. v. Fortuny*, Case No. 99-0456-A, 1999 U.S. Dist. LEXIS 6552 (E.D. Va. Apr. 2, 1999), the district court granted a preliminary injunction against the operator of the domain name *wwwpaineweber.com*. The domain name differed from plaintiff's domain, *www.paineweber.com* only in that it omitted the "." after the designation "www." Paine Weber had alleged that users would inadvertently reach the defendant's site if they omitted the "period" following the letters "www."

The court found a likelihood of irreparable harm to Paine Weber in view of pornographic content automatically linked to defendant's Web site.

In many of these disputes, the Federal Trademark Dilution Act, 15 U.S.C. §1124(c), proved to be a powerful weapon for trademark owners in protecting marks in cyberspace. See, e.g., *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998). The anti-dilution statute had its limits, however. The law was ineffective in squelching so-called *suck sites*. Suck sites are sites that have as their domain name a famous trademark concatenated with the word "sucks." Examples include, *microsoftsucks.org* and *nikesucks.com*. The purpose of a suck site is to criticize the company that owns the famous mark. In *Bally Total Fitness Holding Corp. v. Faber*, 29 F.2d 1161 (C.D. Cal. 1998), the court held that use of trademark owner's logo in juxtaposition with the word "sucks" did not constitute infringing or diluting use of the mark, but was rather constitutionally-protected consumer commentary.

C. ANTICYBERSQUATTING CONSUMER PROTECTION ACT

1. Overview

The rules of the domain name game changed dramatically when the Anticybersquatting Consumer Protection Act, Pub.L. 106-113, 113 Stat. 150 (1999), was enacted on November 29, 1999 (ACPA). Heralded as a victory for trademark owners, the ACPA created a new cause of action, codified at §43(d) of the Lanham Act, for "bad faith" use of marks as domain names. The ACPA also established *in rem* jurisdiction in certain cybersquatting actions, extended its remedies to unauthorized use of personal names, set limitations on liability for domain name registries, and provided limited relief for domain name owners who are victims of reverse domain name hijacking.

2. New Action for Cybersquatting

The principal provision of the ACPA is §43(d)(1)(A), which provides a cause of action to the owner of a mark against a person who: (i) has a *bad faith* intent to profit from that mark, and (ii) registers, traffics in, or uses a domain name that is *identical or confusingly similar* to the mark (if the mark is distinctive) or *dilutive* of the mark (if the mark is famous).

The statute sets forth nine illustrative factors for determining whether a defendant has the requisite bad faith intent:

1. trademark rights of defendant in the domain name;
2. whether the domain name consists of defendant's legal name;

3. defendant's prior use of the domain name in connection with bona fide offering of goods or services;
4. defendant's bona fide noncommercial or fair use of the mark (*e.g.*, parody);
5. intent of defendant to divert consumers from mark owner's site, either for commercial gain or to disparage or tarnish the mark, by creating a likelihood of confusion;
6. defendant's offer to sell the domain name to the mark owner without having used or intended to use the domain name in the bona fide offering of goods and services;
7. defendant's provision of material false contact information to the registrar, or intentional failure to maintain accurate contact information;
8. defendant's registration of multiple domain names of others; and
9. the extent to which a mark is or is not famous under §43(c)(1).

The statute specifies that bad faith intent does not exist when the defendant "believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful."

Notably, the new §43(d) applies to marks that are distinctive or famous at the time the domain name is registered. As explained in the case summaries below, at least one court has applied the act retroactively in the sense that domain names adopted before the enactment of the ACPA are still subject to §43(d) with respect to distinctive and famous marks existing when the domain name was adopted.

Several aspects of this new cause of action distinguish it from other trademark rights. First, there is no requirement that the defendant's domain name be used in connection with goods or services. Mere registration of the domain name is sufficient to give rise to a cause of action. Second, a claim may arise "without regard to the goods and services of the parties." In effect, the act bestows a dilution-type right on marks that are distinctive (but not famous) with respect to "bad faith" adoptions of those marks by parties even for use in unrelated businesses. Third, some of the enumerated factors for establishing bad faith may be proved by showing defendant's prior conduct with respect to domain names other than the name at issue.

Remedies available include injunctions, damages and statutory damages of between \$1,000 and \$100,000. There are no criminal penalties.

3. ***In Rem* Jurisdiction**

The ACPA provides *in rem* jurisdiction against a domain name in the judicial district where the domain name registrar or registry is located if two conditions are met: (i) the domain name violates any right of the owner of a registered U.S. trademark or a mark projected under §43(a) or §43(c); and (ii) the mark owner either is unable to obtain personal jurisdiction over the domain name owner *or* through due diligence is not able to find the domain name owner by sending notice to the owner's address of record and publishing notice of the action as directed by the court.

The remedies available in an *in rem* action are limited to court orders for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark. It is not necessary to name the domain name registrar or registry in the lawsuit. Plaintiffs need only serve notice of the complaint to the registrar (or registry) by mailing, faxing or delivering a file-stamped copy of the complaint to the registrar. The registrar is then required to expeditiously deposit documents with the court that are sufficient to establish the court's control and authority regarding the disposition of the registration and use of the domain name. The registrar must not transfer, suspend or otherwise modify the domain name during the pendency of the action.

D. RECENT CASES

1. Federal Trademark Dilution Act

Avery Dennison Corp. v. Sumpton, 189 F.3d 868 (9th Cir. 1999). Plaintiff Avery Dennison sued defendant Sumpton for registering the domain names *avery.com* and *dennison.com*. Both AVERY and DENNISON were registered trademarks of the plaintiff and had been used since the 1930s. Defendant was in the business of selling surnames as domain names for email use. The lower court held that the marks were famous and granted summary judgment under the FTDA in favor of plaintiff. The Ninth Circuit reversed, holding that the distinctiveness of plaintiff's trademarks alone does not prove fame for purposes of the FTDA. Here, widespread use of the marks AVERY and DENNISON by other parties makes it unlikely that either can be considered a famous mark under the FTDA. The court also held that defendants did not use "trademarks *qua* trademarks as required by the caselaw to establish commercial use" under the FTDA. Rather, defendants used words that happened to be trademarks for the non-trademark value (*i.e.*, value as surnames).

Hasbro, Inc. v. Clue Computing, Inc., 66 F. Supp. 2d 117 (Mass. 1999). Hasbro sued Clue Computing over Clue Computing's use of the domain name *clue.com*. Hasbro alleged that the domain name infringed and

diluted Hasbro's mark CLUE for games. The district court granted summary judgment in favor of the defendant. With respect to the trademark claims, the court found that there was no likelihood of confusion because Hasbro's goods and the defendant's services were unrelated. With respect to the FTDA claims, the court first considered whether the FTDA could be applied retroactively to defendants who had adopted marks prior to the effective date of the Act. Noting a split among the authorities, the court followed the Eighth Circuit's decision in *Viacom Inc. v. Ingram Enterprises, Inc.*, 141 F.3d 886 (8th Cir. 1998), applying the FTDA retroactively. The court then held that the mark CLUE was not "famous" under the FTDA criteria because it was a common term used by different parties as a trademark. The court also held that even if the mark were famous, there had been no dilution. Rejecting Hasbro's argument that registration of a famous mark as a domain name is *per se* dilution, the court held that holders of a famous mark are not automatically entitled under the FTDA to use that mark as their domain name. Rather, the mark owner must show tarnishment or blurring. The court concluded, that as a matter of law, Hasbro could show neither tarnishment or blurring.

2. Cybersquatting

Cello Holdings v. Lawrence-Dahl Co., 89 F. Supp. 2d 464 (S.D.N.Y. 2000). Defendant registered the Internet domain name *cello.com* and tried to sell it to plaintiff, owner of the registered mark CELLO for audio equipment. Plaintiff sued under FTDA and ACPA. The court denied cross motions for summary judgement, finding that genuine issues of fact existed as to whether the mark CELLO was famous and distinctive for purposes of finding dilution or bad faith registration.

Morrison & Foerster v. Wick, 94 F. Supp. 2d 1125 (Colo. 2000). Defendant had registered the domain name *www.morrisonfoerster.com* and other similar names. Despite defendant's argument that the domain names were chosen with the intent of creating parody sites, the court held that the registration of several domain names that were either identical or deceptively similar to plaintiff's trademark was a bad faith use in violation of the ACPA. The court found that while bona fide parodic content could be protected, the mere incorporation of the trademark as the domain name did not constitute a protectable, communicative message. It simply caused confusion.

Spear, Leeds, & Kellogg v. Rosado, No. 99-11417, 2000 U.S. Dist. LEXIS 3732 (S.D.N.Y. 2000). Plaintiff, a securities brokerage, owned the registered mark REDI and the common law mark REDIBOOK. Defendant registered the domain *redibook* in the *.com* and other gTLDs. Held: plaintiff entitled to relief under both §43(a) of the Lanham Act and under the ACPA.

Sporty's Farm v. Sportsman's Market, Inc., 202 F.3d 489 (2d Cir. 2000). Second Circuit held that an appellate court can directly apply the ACPA without remand to affirm a federal trademark dilution judgment entered before the ACPA was passed. In this case, defendant's bad faith under the ACPA was established because it planned to compete with plaintiff. The court found the defendant's explanation for adopting the *sporty* domain name (based on a dog named Spotty) to be "more amusing than credible." The court declined to award damages since the defendant adopted the domain name before passage of the ACPA.

Volkswagen AG v. Virtual Works, Inc., 54 U.S.P.Q.2d 1126 (E.D. Va. 2000). Defendant's registration of the domain name *vw.net* constituted trademark infringement, dilution and cyberspiracy with respect to plaintiff's mark VW. Relying on the fact that defendant had never used the initials "VW" as a legal name and that defendant had offered to sell the domain to plaintiff, the court found that defendant had attempted to profit from the trafficking of plaintiff's trademark as a domain name. The court also stated that "[t]he holder of a domain name should give up that domain name when it is 'an intuitive domain name' that belongs to another." The court concluded that "VW" was the "intuitive domain name" of Volkswagen. The court placed no stock in the fact that the parties offered different products since both used the Internet as a facility to provide goods and services. With regard to Volkswagen's dilution claim, the court held that "Internet cyberspiracy constitutes *per se* trademark dilution" and that "VW being associated with Virtual Works instead of Volkswagen constitutes trademark dilution."

3. Other

BigStar Entertainment, Inc. v. Next Big Star, Inc., 54 U.S.P.Q.2d 1685 (S.D.N.Y. 2000). Bigstar.com was a Web site for a retailer of videotapes and supplier of celebrity information. Nextbigstar.com sponsored online talent competitions. Bigstar.com sued Nextbigstar.com for trademark infringement, asserting the initial interest confusion theory articulated in *Brookfield*. The court denied preliminary injunction, distinguishing *Brookfield* on several points, including the fact that defendant had not used the mark in metatags to divert to its site the initial interests of potential buyers; the marks were not virtually identical; and the parties were not in direct competition with one another nor were their marks and businesses sufficiently closely related.

Interstellar Starship Ser., Ltd. v. Epix, Inc., 184 F.3d 1107 (9th Cir. 2000). Defendant Epix manufactures video image hardware and software and is the owner of a registered incontestable trademark for EPIX. ISS operated a Web site at the domain name *epix.com* for an unrelated business, the exact nature of which is not explained in the opinion. When Epix sought to have NSI cancel ISS's *epix.com* registration, ISS sued Epix for

declaratory judgment of ISS's right to maintain the *epix.com* domain name. The district court granted summary judgment to ISS. On appeal, the Ninth Circuit reversed and remanded, holding that determination of trademark infringement would require a full factual assessment under the Ninth Circuit's *Sleekcraft* factors for determining likelihood of confusion. In particular, the court noted that under the initial interest theory of *Brookfield*, similarity of products and services can be a compelling factor because customers, once drawn to the Web site, might purchase there even if never confused about the trademark owner's lack of connection to the Web site.

Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980 (9th Cir. 1999). Held: Network Solutions as a matter of law is not liable for contributory trademark infringement based on registration by a third party of Lockheed's trademark SKUNK WORKS as a domain name.

The Network Network v. CBS, Inc., 54 U.S.P.Q.2d 1150 (C.D. Cal. 2000). CBS, owner of the famous mark TNN for a television network, sued the operator of *tnn.com*, a Web site devoted to computer training. The court refused to apply initial interest confusion theory because domain name owner and trademark owner were in different businesses, even though the trademark TNN was famous. Citing *Brookfield* and *Interstellar Starship Services*, the court observed that the finding of initial interests confusion is predicated on having at least a "tangential relationship" between the goods offered by the parties. In this case, the domain name owner had also been using TNN as a common law trademark (albeit not on the Internet) prior to the adoption of the mark TNN by CBS.

OBH, Inc. v. Spotlight Magazine, Inc., 86 F. Supp. 2d 176 (W.D.N.Y. 2000). The district court granted owners of the mark THE BUFFALO NEWS a preliminary injunction against the owner of the domain name *thebuffalonews.com*. Although the Web site was alleged to be a parody of THE BUFFALO NEWS, the court found that its use of plaintiff's mark constituted a trademark infringement. The infringing site also met the "use in commerce" requirement under the Lanham Act because it contained a hyperlink that connected it to defendant's commercial apartment finder Web site. The court also found that defendant's use of the mark created initial interest confusion.

Playboy Enter., Inc. v. Calvin Designer Label, 985 F. Supp. 1218 (N.D. Cal. 1997). The district court held that use of the plaintiff's mark in a metatag constituted a trademark infringement and granted summary judgment in favor of the trademark owner. The court also granted summary judgment on the plaintiff's trademark dilution claim.

Playboy Enter., Inc. v. Welles, 78 F. Supp. 2d 1066 (S.D. Cal. 1999). Playboy, owner of PLAYMATE trademark, sued its former model Welles

for trademark infringement based on her operation of a Web site with the heading “Terry Welles—Playmate of the Year 1981.” Each page of the Web site used a “PMOY ‘81” as a repeating watermark in the background. The Web site also included disclaimers reading as follows: “This site is neither endorsed, nor sponsored by, nor affiliated with Playboy Enterprises.” The marks PLAYBOY and PLAYMATE were also used as metatags. The court found that the defendant’s use was a nominative, fair use to describe her goods and services, and was not an infringement. The court stated that “There is no other way that Ms. Welles can identify or describe herself and her services without venturing into absurd descriptive phrases.” The court distinguished *Brookfield* because the use of the mark in this case, even as a metatag, was a descriptive fair use.

4. **Jurisdiction/International**

Caesars World, Inc. v. Caesars-Palace.com, 54 U.S.P.Q.2d 1121 (E.D. Va. 2000). The court found that *in rem* jurisdiction under the ACPA over defendants who are not subject to the personal jurisdiction of the court does not violate the Due Process Clause of the Constitution. The court rejected the defendants’ argument that *in rem* jurisdiction is constitutional only where the “res” provides minimum contacts sufficient for *in personam* jurisdiction under *Shaffer v. Heitner*, 433 U.S. 186 (1977). The court read *Shaffer* as requiring minimum contacts to support personal jurisdiction only in those *in rem* proceedings where the underlying cause of action is unrelated to the property which is located in the forum state. Here, the property was not only related to the cause of action, but also composed its entire subject matter. Thus, minimum contacts sufficient for *in personam* jurisdiction were unnecessary.

Jeri-Jo Knitwear, Inc. v. Club Italia, Inc., 94 F. Supp. 2d 457 (S.D.N.Y. 2000). Defendant, an Italian company, did not violate a court order permanently enjoining use of plaintiff’s trademark ENERGIE in the U.S. when defendant created a Web site in Italy with the address *energie.it*. The court held that, although defendant’s actions could be viewed as advertising in the U.S. in violation of the injunction, defendant’s conduct was not willful and therefore not subject to a contempt citation. Defendants held legitimate rights to the trademark outside the U.S. and there was no way to conclusively block U.S. consumers from defendants’ Web sites. The court did, however, require that defendant take down links to *energie.it* on defendant’s other Web sites registered in the .com and .net TLDs.

Lucent Technologies, Inc. v. LucentSucks.com, 95 F. Supp. 2d 528 (E.D. Va. May 3, 2000). Lucent filed an *in rem* action against the domain name *lucentSucks.com* pursuant to the ACPA. The owner of the domain name moved to dismiss on the grounds that Lucent waited only 8 days to file the

suit after sending the domain name owner the notice required under the ACPA's *in rem* provisions. The court dismissed the action, holding that 8 days is insufficient notice. Although the ACPA does not specify a notice period, the court held that eight days was insufficient. Citing Rule 12 of the F.R.C.P. by analogy, the court suggested that 20 days might be sufficient notice under the ACPA. Once the defendant is located (as in this case), *in rem* jurisdiction is not appropriate except as a last resort when *in personam* jurisdiction is unavailable. The court wrote "Congress did not intend to provide an easy way for trademark owners to proceed *in rem* after jumping through a few *pro forma* hoops."

Network Solutions, Inc. v. Umbro Int'l, Inc., 529 S.E. 2d 80 (Va. Sup. Ct. 2000). Virginia Supreme Court held that domain name registrations cannot be garnished under Virginia's creditors' remedies law. In this case, plaintiff, a vendor of camping gear, sued a Canadian domain name hijacker in South Carolina for trademark infringement and dilution. After a default judgment, the South Carolina court awarded plaintiff \$25,000. To satisfy this judgment, plaintiff then filed a garnishment proceeding in Virginia against the Canadian defendant's domain name registered with Network Solutions. The lower court held that the defendant's Internet domain names registered with Virginia-based Network Solutions are property subject to garnishment under Virginia statute; however the Virginia Supreme Court reversed, holding that the contract between NSI and a domain name owner is not a "liability" subject to garnishment.

Porsche Cars N. America, Inc. v. allporsche.com, No. 99-1804, 2000 U.S. App. LEXIS 12843 (4th Cir. 2000). Porsche had originally filed this lawsuit in the Eastern District of Virginia as an *in rem* action against 100-plus domain names registered by Virginia-based Network Solutions, alleging that each of the domain names diluted its famous PORSCHE or BOXSTER trademarks. The district court held that *in rem* actions were not permitted under the FTDA, citing due process concerns. In light of the adoption of the ACPA, the Fourth Circuit remanded with instructions to consider whether the ACPA would permit an *in rem* action under the FTDA.

E. ICANN

1. Prior History

Although the U.S. Government does not control the Internet in the same sense that it controls the army or other public functions, it has exerted great influence through the grants and procurement contracts that have been awarded to IANA and the other entities that define the Internet's *de facto* governance structure. After the collapse of the IAHC initiative, the Clinton Administration directed the Secretary of Commerce on July 1,

1997 to revamp the Government's role in the Internet and to foster private, competitive administration of the DNS.

Six months later, in early 1998, the Department of Commerce issued its Proposal to Improve the Technical Management of Internet Names and This so-called *Green Paper* proposed the creation of a new, not-for-profit corporation to manage the DNS. Once the new corporation was in operation, the U.S. Government would relinquish its role as the ultimate overseer of Internet names, numbers and other technical parameters. Internet users generally cheered the Green Paper proposals in principle, but opinions differed greatly on exactly how the proposed not-for-profit corporation should be managed.

In its final policy statement, published on June 5, 1998, the Commerce Department reiterated its vision of a new, not-for-profit corporation formed by "private sector Internet stakeholders" to administer the Internet name and address system. This entity was slated to take over duties then handled by the government through its subcontractors, IANA and Network Solutions.

The Government also announced its intention to invite the World Intellectual Property Organization (*WIPO*) to convene an international process to develop a set of recommendations for trademark/domain name dispute resolution. (WIPO obliged the Government. Its recommendations were published on April 30, 1999 at: <http://wipo2.wipo.int/process/eng/processhome.html>.)

On September 17, 1998, IANA and Network Solutions reached an agreement as to the new entity's by-laws, articles and purpose. Under the agreement, the new entity – now called the Internet Corporation For Assigned Names And Numbers" (*ICANN*) -- would:

- coordinate the assignment of Internet technical parameters to foster universal connectivity
- oversee the Internet Protocol address space
- oversee and coordinate the domain name system, including the development of policies with respect to gTLDs

Despite the agreement, it was apparent that the newly-formed ICANN was months away from becoming operational. NSF was forced to extend Network Solutions' contract until September 30, 2000, which was to have been the new target date for transferring management of the DNS to ICANN. In the meantime, the Department of Commerce and the infant ICANN entered into a Memorandum of Understanding dated November 25, 1998, pursuant to which ICANN was to work with the Department of Commerce to develop a plan for competitive domain name registration services and possibly expanding the number of gTLDs.

On February 8, 1999, ICANN released for public comment proposed guidelines for gTLD registration businesses. The guidelines set forth requirements for prospective registrars who would be authorized to issue domain names in the *.com*, *.net*, and *.org* TLDs. Registrars would be required to pay ICANN a tax of \$1.00 per year for each domain name registered.

On April 21, 1999 ICANN selected the first five competitive registrars, including America Online and the Internet Council of Registrars. The five companies were slated to use a “shared registry technology,” with Network Solutions retaining control over the registry on an interim basis.

By June 1999, however, it had become clear that Network Solutions had little interest in cooperating with ICANN or in giving competitors access to the lucrative *.com* database. As discussions between ICANN, Network Solutions and NSF dragged on, public criticism of all three parties grew louder. A Congressional investigation was launched in July 1999. By that time ICANN was out of money and some commentators were predicting its demise.

On September 28, 1999, Network Solutions and ICANN reached a compromise agreement, in which Network Solutions recognized (and helped fund) ICANN and ICANN allowed Network Solutions to retain substantial controls over the *.com*, *.net* and *.org* registries for at least four years. Competitive registrars will pay Network Solutions a wholesale price for each domain name. The agreement contained incentives for Network Solutions to eventually split its registry and registrar businesses into two unrelated entities. In the meantime, it is expected that Network Solutions will remain the dominant player in domain name registration.

2. Uniform Domain Name Dispute Policy

On October 24, 1999, ICANN (now funded and recognized by Network Solutions) promulgated its Uniform Dispute Resolution Policy (*UDRP*). The policy is available at <http://www.icann.org/udrp/udrp.htm>.

This policy has been adopted by all accredited domain-name registrars (including Network Solutions) for domain names ending in *.com*, *.net* and *.org*.

The UDRP has three principal features. First, it requires persons applying to register a domain name to represent and warrant that: (1) the statements made by the applicant in the registration agreement are complete and accurate; (2) to the applicant’s knowledge, the registration of the domain name will not violate the rights of any third party; (3) the applicant is not registering the domain name for an unlawful purposes; and (4) the

applicant will not knowingly use the domain name in violation of any applicable laws.

Second, the UDRP dispenses with Network Solutions' controversial practice of placing contested domain names on "hold" status. Instead, the registrar will remove domain names in three circumstances: (1) when authorized by the domain name owner; (2) on the order of a court; or (3) upon the decision of an arbitration panel pursuant to a proceeding authorized by the UDRP (as explained in the following paragraph).

Third, the UDRP provides for mandatory arbitration in domain name disputes when the following criteria are met: (1) the domain name is identical or confusingly similar to a trademark; (2) the domain name owner has no rights or legitimate interest in respect of the domain name; and (3) the domain name was registered in "bad faith."

The policy specifies four factors which are evidence of bad faith:

- registration of a domain name for the purpose of selling it back to a trademark owner;
- registration of a domain name to prevent the owner of a trademark from using the mark as a domain name, provided that the domain name owner has engaged in a pattern of such conduct;
- registration of a domain name primarily for the purpose of disrupting a trademark owner's business; and
- use of the domain to intentionally draw traffic for commercial gain to the registrant's Web site by creating a likelihood of confusion with a trademark.

The policy further specifies three factors that demonstrate a domain name owner's legitimate interests in a domain name:

- before notice of the dispute, the owner used or prepared to use the domain name in connection with the bona fide offering of goods or services;
- the domain name owner has been commonly known by the domain name, even if it has no trademark rights in the name; and
- the domain name owner is making legitimate noncommercial or fair use of the domain name without intent for commercial gain to misleadingly divert consumer or to tarnish the trademark or service mark at issue.

To date, ICANN has approved four arbitration bodies to handle disputes under the uniform policy:

- CPR Institute for Dispute Resolution
- Disputes.org/eResolution Consortium
- The National Arbitration Forum
- World Intellectual Property Organization

F. PATENT AND TRADEMARK OFFICE ACTIVITY

On September 29, 1999, the U.S. Patent and Trademark Office issued Examination Guide 2-99 with respect to “Marks Composed, In Whole Or In Part, Of Domain Names.” The Guide states that neither the beginning of the URL (*e.g.*, <http://www>) nor the TLD (*e.g.*, [.com](http://www.com)), has any source-indicating significance. The Guide also address of number of other issues, including use and specimens. It is available at <http://www.uspto.gov/web/offices/tac/notices/guide299.htm>.

III. PATENTS

A. OVERVIEW

The Internet has led to new ways of doing business in an online environment. These so-called online business models are of great importance to the development of electronic commerce and are therefore of substantial economic value. Companies have begun to protect these models using patents.

Traditionally, patent law would not have been a viable way to protect online business models. For many years, neither computer software nor methods of doing business were thought to be patentable subject matter. Methods of doing business that were implemented with software, therefore, would have historically stood little chance of being patentable.

The patent law, however, has evolved. The emergence of online business models has coincided with the steady judicial expansion of patentable subject matter (or, more precisely, the steady erosion of the judicially-created “abstract ideas” exclusion to patentable subject matter). These developments have made it possible to patent online business models.

The Patent Office granted over twenty thousand patents for software-related inventions in 1998, which represents a forty percent increase over the prior year. Likewise, the growth of Internet-related patents has matched the expansion of the Internet, with almost sixteen hundred patents issued in 1998, up from only nine patents granted in 1991. The Patent Office expects to grant over three hundred patents for business models by the year 2000.

B. BACKGROUND

Subject matter eligible for patent protection is specified in 35 U.S.C. §101, which provides that anyone who invents a “new and useful process, machine, manufacture or composition of matter . . .” may obtain a patent. Legislative history indicates that Congress intended statutory subject matter under §101 to “include anything under the sun that is made by man.” *Diamond v. Chakrabarty*, 447 U.S. 303, 309 (1980). However, discoveries of the laws of nature, physical phenomenon, or abstract ideas by themselves cannot be patented. *Id.* If there is anything patentable from these discoveries, it is the application of the law, phenomenon or idea to some new and useful end. *Funk Bros. Seed Co. v. Kato Co.*, 333 U.S. 127 (1948).

Because computer programs are inherently algorithmic, it was thought for many years that they could not be protected as patentable subject matter. During the 1970s, the Supreme Court twice considered the patentability of software-related patent applications and both times decided that the claimed inventions were unpatentable. *Gottschalk v. Benson*, 409 U.S. 63 (1972) (method for converting numbers from BCD format to binary format held not patentable); and *Parker v. Flook*, 437 U.S. 584 (1978) (method for updating alarm limits held not patentable).

The tide began to turn in 1981 with *Diamond v. Diehr*, 450 U.S. 175 (1981). That case involved a method for operating a rubber molding press. In accordance with the claimed method, a computer program used a formula to determine how long the rubber should be allowed to cure. The court held that the method was patentable because it was primarily directed to a physical process, namely curing rubber, to which the mathematical formula was applied.

The inventions in *Benson*, *Flook* and *Diehr* all involved mathematical algorithms, but not to the same degree. The court found the claims in *Diehr* to be primarily directed to a physical process, namely curing rubber, in which the mathematical formula was applied. In contrast, the Court found that the claimed methods in *Benson* and *Flook* were nothing more than the algorithms, albeit performed by computers.

In an attempt to capture the sometimes elusive distinction between patentable invention and unpatentable abstraction, the courts and PTO applied a two-step test known as the Freeman-Walter-Abele test. The first step of this test was to determine whether the claim recites a mathematical algorithm. If an algorithm is found, the second step was to determine whether the algorithm is applied to physical elements or process steps. If so, then the claim is directed to statutory subject matter. *In re Abele*, 214 U.S.P.Q. 682 (C.C.P.A. 1982).

In *In re Alappat*, 33 F.3d 1526 (Fed.Cir. 1994), the Federal Circuit went a step further, holding that an apparatus claim drawn to a programmed general purpose computer could be patentable. The application in *Alappat* was directed to a

software technique for creating a smooth waveform display in a digital oscilloscope. The PTO patent examiner had rejected the claim under §101 as being directed to nonstatutory subject matter. The applicant appealed to the Federal Circuit. The court first held that the claim was directed to an apparatus, and was therefore on its face patentable subject matter under §101.

The court then considered whether the claim fell into the judicially created “mathematical algorithm” exception to §101. It explained that the “algorithms” are only excluded from patentable subject matter to the extent that they represent nothing more than abstract ideas. The dispositive inquiry under §101 is not simply whether the claim contains unpatentable mathematical subject matter. Rather, the proper inquiry is to determine “whether the claimed subject matter as a whole is a disembodied mathematical concept, whether categorized as a mathematical formula, mathematical equation, mathematical algorithm, or the like, which in essence represents nothing more than a law of nature, natural phenomenon, or abstract idea.” In *Alappat*’s invention, the court held, the claimed invention as a whole is directed to a combination of interrelated elements which combine to form a machine to produce a useful, concrete, and tangible result, namely converting discrete waveform. data samples into pixel illumination intensity data to be displayed on a display means.

Finally, the court addressed a separate argument raised by the PTO, namely that the claim at issue was unpatentable because it read on a general purpose computer programmed to perform the functions recited in the means elements. In rejecting the PTO’s argument, the court stated that a claim is not automatically unpatentable under §101 just because it could read on a general purpose computer programmed to carry out the invention. Such programming creates a new machine, because a general purpose computer in effect becomes a special purpose computer once it is programmed to perform particular functions.

The Federal Circuit continued down the path marked by *Alappat* with decisions that not only buttressed the patentability of software but laid to rest the long-standing rule against patenting methods of doing business.

The most significant of these cases was *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*, 149 F.3d 1368 (Fed.Cir. 1998). There, the claimed invention involved a data processing implementation of a “hub and spoke” investment system whereby mutual funds (spokes) pool their assets in an investment portfolio (hub) organized as a partnership. This investment configuration provides the administrator of a mutual fund with the advantageous combination of economies of scale in administering investments coupled with the tax advantages of a partnership.

The defendant, State Street, attempted to negotiate with plaintiff Signature for a license to use the patented data processing system. When negotiations broke down, State Street brought a declaratory judgment action asserting that Signature’s patent was invalid. Initially, the lower court ruled in favor of State

Street, holding that Signature was not entitled to a patent because it had improperly claimed an algorithm. On appeal, the Federal Circuit reversed.

The Federal Circuit addressed three major issues. First, it held that the claim at issue, which recited a “system” having means plus function elements, was directed to a machine, “namely a data processing system.” As such, the claim recited proper statutory subject matter under §101.

Second, the court held that the claimed subject matter did not fall into the judicially-created “mathematical algorithm” exception. The court began its analysis by pointing out that the judicially created categories of unpatentable subject matter consist of laws of nature, natural phenomena and abstract ideas. Mathematical algorithms are not a fourth class of unpatentable subject matter, but rather are unpatentable only to the extent that they constitute merely abstract ideas.

Tracking its reasoning in *Alappat*, the court explained that the difference between patentable and unpatentable algorithms is that unpatentable algorithms are merely disembodied concepts or truths that are not useful, while a patentable algorithm “must be applied in a ‘useful’ way” to achieve a concrete and tangible result. 149 F.3d at 1373.

It will be recalled that the useful result in *Alappat* was the smoothing of waveforms on an oscilloscope. As concrete tangible results go, that may seem a bit abstract. However, the court in *State Street* went even one step beyond, holding that:

[T]he transformation of data, representing discrete dollar amounts, by a machine through a series of mathematical calculations into a final share price, constitutes a practical application of a mathematical algorithm, formula or calculation because it produces ‘a useful, concrete and tangible result’ -- a final share price momentarily fixed for recording and reporting purposes and even accepted and relied upon by regulatory authorities in subsequent trades. 149 F.3d at 1373.

To the extent that the lower court had reached a different result applying the Freeman-Walter-Abel test, the court remarked that the test “has little, if any applicability to determining the presence of statutory subject matter” in light of *Diehr* and *Chakrabarty*.

Thus, the court extended *Alappat* to some extent by holding that mere numbers such as price, profit, percentage, cost or loss may be sufficiently useful, concrete and tangible results to find that a claim is directed to patentable subject matter.

Third, the court held that the venerable business method exception was no longer a basis for invalidating a patent under §101. As the court stated, “We take this opportunity to lay this ill-conceived exception to rest.” The court held, “Whether the claims are directed to subject matter within §101 should not turn on whether the claimed subject matter does ‘business’ instead of something else.” *Id.* at 1377.

The result in *State Street* was extended in *AT&T Corp. v. Excel Communications Inc.*, 172 F.3d 1352 (Fed.Cir. 1999). There, the Federal Circuit held that process patent claims containing mathematical algorithms are patentable subject matter when they “apply” the algorithm to produce a useful, concrete, tangible result. The court clarified that the subject matter determination does not necessarily require a showing of “physical transformation” or physical limitations for process claims. The notion of “physical transformation” is merely one example of how a mathematical algorithm may bring about a useful application.

The Patent and Trademark Office on October 21, 1998 released additional training materials for application of its 1996 Examination Guidelines for computer-related inventions. The added training materials cover patent applications in the areas of business, artificial intelligence, and mathematical processing. They provide examples of computer-related inventions that illustrate proper application of the 1996 guidelines.

The Examination Guidelines and Training Materials are available at:
<http://www.uspto.gov/web/offices/pac/compexam/comguide.htm>

C. RECENT DEVELOPMENTS

Amazon.com, Inc. v. Barnesandnoble.com, Inc., 73 F. Supp. 2d 1228 (W.D. Wash. 1999). Court granted Amazon.com’s motion for preliminary injunction against infringement of Amazon.com’s “one-click” ordering patent. Given the strong showing of patent validity and infringement, Amazon.com is entitled to a presumption of irreparable harm, the court wrote. Other factors also supported a finding of irreparable harm, including the fact that the patented technology was intended to distinguish Amazon.com from competitors in an upcoming holiday season. A delay of twenty-two days from issuance of patent to filing of lawsuit did not preclude preliminary relief.

CoolSavings.com, Inc. v. IQ Commerce Corp., 53 F. Supp. 2d 1000 (N.D. Ill. 1999). Illinois court determined that it had specific jurisdiction over a California Web site operator whose Web site allegedly generated coupons in violation of plaintiff’s patent rights. The California defendant argued that it lacked minimum contacts with Illinois because Illinois residents constituted less than two percent of its Web site activity. The court rejected this argument, noting that even a single act can support specific jurisdiction. While an interactive Web site can be the basis for jurisdiction, this is an unusual case because the use of the interactive technology itself allegedly infringed the plaintiff’s patent. The court concluded

that a case where the contact itself is the wrong is a stronger case for jurisdiction than one in which the contact merely relates to the wrong.

Calls for Reform. In March 2000, Amazon chief executive Jeff Bezos publicly called for patent reform, including limiting the term of business method and software patents to between three and five years. Bezos also called for a public comment period before a patent is issued. Later that same month, the PTO announced that it will add a second layer of review for patent applications in Class 705, which includes business method patents.

IV. COPYRIGHT

A. OVERVIEW

Copyright law gives authors the right to control the reproduction and distribution of their works. Most of the content and software accessible over the Internet (such as via a Web site, for example) is copyrightable subject matter. Because of the nature in which this information is manipulated online, its use and access involves copying, and, therefore, raises complex issues under the copyright law. Moreover, the Internet by its very nature greatly facilitates the reproduction and distribution of copyrighted works, thus offering copyright owners both an *opportunity* for low cost global distribution and a *threat* that their works will be illegally copied *en mass*.

The year 2000 saw a dramatic escalation in the conflict between copyright owners (principally record companies) and providers of new media technology (such as MP3 and Napster). The past 12 months also brought a number of decisions applying the Digital Millennium Copyright Act.

B. BACKGROUND

U.S. copyright law, codified at 17 U.S.C. 101 et seq., protects “original works of authorship” that are “fixed in a tangible medium of expression” such as paper or a computer’s memory. Protected works of authorship include text, graphics and clip art, software, audiovisual works, music compositions and lyrics, and sound recordings. The owner of a copyright has the legal right to prevent others from copying, distributing, adapting, publicly displaying, publicly performing and, in some cases, transmitting, the copyrighted work.

Before the advent of digital technology, these legal rights were effectively buttressed by the practical fact that copying and distribution, whether or not lawful, always entailed some degree of cost and logistical difficulty. For example, an infringer in 1970 who sought to reproduce a copyrighted book would have expended substantial resources on ink, paper and shipping. Not only would such an operation be costly, but it would also be relatively conspicuous and therefore subject to detection by the copyright owner and subsequent enforcement action. These costs, coupled with the threat of liability under the copyright law,

proved an effective deterrent to infringement, allowing entire industries to flourish under the protection of copyright. In a similar fashion, the limitations of analog recording technology restrained serial copying of music (*i.e.*, where an unauthorized copy is used to make another unauthorized copy). For example, a teenager in 1977 could create a reasonably clear copy of a record album on a cassette tape; however, future copies derived from that taped copy would be of markedly poorer quality.

With digital technology generally, and the Internet in particular, the physical and logistical factors that traditionally restrained copyright infringement are greatly diminished. Indeed, the Internet is a copy and distribution machine of immense power. Once a work is posted on the Internet, it may be serially copied a thousand times over, with each copy a perfect reproduction of the last. Those copies can be distributed throughout the world by millions of users, each acting independently with little or no cost and no credible threat of civil or criminal liability. In short, the Internet is a copyright holder's worst nightmare.

Predictably, industries that depend on copyright protection have sought to vigorously enforce copyrights in the face of online infringement. Because infringers are often individuals who may either be hard to locate or judgment proof, copyright owners have also resorted to suing infringers' service providers. *See, e.g., Religious Tech. Ctr. v. Netcom On-Line Comm. Serv., Inc.*, 923 F. Supp. 1231 (N.D. Cal. 1995); *Sega Enter. Ltd. v. MAPHIA* 948 F. Supp. 923 (N.D. Cal. 1996); *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993); *Playboy Enterprises, Inc. v. Webbworld, Inc.*, 991 F. Supp. 543 (N.D. Tex. 1997) *aff'd*. 168 F.3d 486 (5th Cir. 1999).

At the behest of copyright owners, Congress has also acted to strengthen rights and remedies in an online context. Specifically, Congress enacted the Home Audio Recording Act of 1992 requiring certain classes of digital audio recording devices to include a Serial Copyright Management System.

In 1995, Congress enacted the Digital Performance Right in Sound Recordings Act, amending §106 of the copyright statute to provide a limited performance right for sound recordings by means of a digital audio transmission.

In 1997, Congress enacted the No Electronic Theft Act, amending §506 of the Copyright Act to criminalize certain willful infringements, even in cases where the infringer was not acting for purposes of financial gain. The Act was intended to overrule the decision in *United States v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994), in which an MIT graduate student was charged with wire fraud for running an illegal online software exchange. The court in *LaMacchia* had dismissed the charges, holding that the wire fraud statute under which LaMacchia had been charged was not violated because LaMacchia had not operated the exchange for monetary gain, an element required to establish criminal copyright infringement. Through mid-2000, the Justice Department has only prosecuted two people under the NET legislation.

C. DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998

1. Overview

The Digital Millennium Copyright Act (DMCA), Pub. L. 105-304, 112 Stat. 2860 (1998) was signed into law by President Clinton on October 28, 1998. The act is available at: <http://thomas.loc.gov>. An excellent summary is available from the Copyright Office at: <http://lcweb.loc.gov/copyright/legislation/dmca.pdf>.

The DMCA is divided into five titles:

- Title 1, the “WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998,” implements two WIPO treaties.
- Title II, the “Online Copyright Infringement Liability Limitation Act,” creates limitations on the liability of online service providers for copyright infringement when engaging in certain types of activities.
- Title III, the “Computer Maintenance Competition Assurance Act,” creates an exemption for making a copy of a computer program by activating a computer for purposes of maintenance or repair.
- Title IV contains six miscellaneous provisions, relating to the functions of the Copyright Office, distance education, the exceptions in the Copyright Act for libraries and for making ephemeral recordings, “webcasting” of sound recordings on the Internet, and the applicability of collective bargaining agreement obligations in the case of transfers of rights in motion pictures.
- Title V, the “Vessel Hull Design Protection Act,” creates a new form of protection for the design of vessel hulls.

2. Implementation of WIPO Treaties

Title I implements the WIPO treaties by making technical amendments to U.S. law and by adding a new Chapter 12 to the Copyright Act addressing copyright protection and management systems.

New §1201 prohibits users from circumventing a “technological measure that effectively controls access to a work protected under this title.” The prohibition does not take affect until two years after the enactment of the Act (October 28, 2000). There are three-year exemptions that may be granted by the Copyright Office to persons who are users of certain works

who are likely to be adversely affected by the prohibition in their ability to make noninfringing uses of the particular type of work (such as for news reporting).

Section 1201 also prevents the sale of devices that circumvent technological measures that control access to a work or that protect the rights of a copyright owner. Prohibited devices include devices that:

- are primarily designed or produced to circumvent;
- have only a limited commercially significant purpose or use other than to circumvent; or
- are marketed for use in circumventing.

Section 1201 divides technological measures into two categories: measures that prevent unauthorized access to a copyrighted work and measures that prevent unauthorized copying of a copyrighted work. Making or selling devices or services that are used to circumvent either category of technological measures are prohibited as is the act of circumventing access control devices. However, the act of circumventing copy control devices is not prohibited. This distinction was intended to preserve the public's ability to make fair use of copyrighted works.

Query: how users will circumvent copy control devices without commercially available circumvention products?

Section 1201(c) contains two general savings clauses. First, §1201(c)(1) states that nothing in §1201 affects rights, remedies, limitations or defenses to copyright infringement, including fair use. Second, §1201(c)(2) states that nothing in §1201 enlarges or diminishes vicarious or contributory copyright infringement.

Section 1201(d) exempts nonprofit library, archive and educational institutions from the prohibition on the act of circumventing access control measures for the sole purpose of determining whether they want to obtain authorized access.

Section 1201(e) exempts law enforcement, intelligence and other government activities carried out for lawfully authorized investigative, protective, intelligence or information security activities. The term "information security" include activities carried out to identify and address vulnerabilities of a government computer system.

Section 1201(f) exempts access to a computer program by a person who has obtained a lawful right to use a copy of the program for the sole purpose of identifying and analyzing those elements of the program that

are necessary to achieve interoperability of an independently created computer program, but only to the extent that such acts do not otherwise constitute copyright infringement.

Section 1201(g) exempts certain types of encryption research.

Section 1201(h) allows a court applying the prohibitions against circumventing access controls to consider the necessity for its incorporation in technology that prevents access of minors to material on the Internet.

Section 1201(i) permits circumvention when the technological measure or the work it protects is capable of collecting or disseminating personally identifying information about the online activities of a natural person.

Section 1201(j) permits circumvention of access control (and the development of means for such circumvention) for the purpose of testing the security of a computer with the authorization of its owner or operator.

New §1202 addresses copyright management information. Section 1202(a) prohibits any person from knowingly and with the intent to infringe, providing false copyright management information, or distributing or importing for distribution false copyright management information.

Section 1202(b) bars: (1) the intentional removal or alteration of copyright management information, (2) the distribution or importation for distribution of copyright management information knowing same to have been removed or altered, or (3) the distribution, importation for distribution, or public performance of works knowing that the copyright management information has been removed or altered.

The term “copyright information management” is defined as the title, copyright notice, name of the author, terms and conditions for use of the work, and other specified information. An exemption is provided for law enforcement, intelligence and other government activities.

Section 1203 specifies civil remedies. These include injunctions, impoundment, damages, costs, attorneys’ fees at the courts discretion, and certain other remedial measures. Damages are either actual damages and the violator’s profits, or statutory damages. Damages may be trebled in cases where the defendant has violated §1201 or §1201 in the three year period following a judgment against the defendant for a previous violation.

Section 1204 specifies criminal penalties. Under that section, any person who violates §1201 or §1202 “willfully and for purposes of commercial

advantage or private financial gain is subject to a fine of up to \$500,000 or five years in prison for the first offense and a fine of up to \$1,000,000 or ten years in prison for any subsequent offense.

3. Online Copyright Infringement Liability Limitation

Title II of the DMCA adds a new §512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. The limitations are based on the following four categories of conduct by a service provider:

- Transitory communications
- System caching
- Storage of information on systems or networks at direction of users
- Information location tools.

The failure of a service provider to qualify for any of the limitations in §512 does not necessarily make it liable for copyright infringement. The copyright owner must still demonstrate that the provider has infringed, and the provider may still avail itself of any of the defenses, such as fair use, that are available to copyright defendants generally.

Limitation for Transitory Communications. Section 512(a) limits the liability of service providers when the provider merely acts as a data conduit, transmitting digital information from one point on a network to another at someone else's request. This limitation covers acts of transmission, routing, or providing connections for the information, as well as the intermediate and transient copies that are made automatically in the operation of a network. Additional requirements are that:

- transmission must be initiated by a person other than the provider; transmission, routing, provision of connections, or copying must be carried out by an automatic technical process without selection of material by the service provider;
- provider must not determine the recipients of the material;
- any intermediate copies must not ordinarily be accessible to anyone other than anticipated recipients, and must not be retained for longer than reasonably necessary; and
- material must be transmitted with no modification to its content.

Limitation for System Caching. Section 512(b) limits the liability of service providers for online caching. The limitation applies only to intermediate and temporary storage, when carried out through an automatic technical process for the purpose of making the material

available to subscribers who subsequently request it. It is subject to the following conditions:

- content of the cached material must not be modified;
- provider must comply with rules about “refreshing” material when specified in accordance with a generally accepted industry standard data communication protocol;
- provider must not interfere with certain technology that returns “hit” information;
- provider must limit users’ access to the material in accordance with conditions on access imposed by the person who posted the material; and
- material that was posted without the copyright owner’s authorization must be removed or blocked promptly once the service provider has been notified that it has been removed, blocked, or ordered to be removed or blocked, at the originating site.

Limitation for User’s Information. Section 512(c) limits the liability of service providers for infringing material placed by users on their systems. To take advantage of this limitation, the provider must:

- not have the knowledge of the infringing activity;
- not receive a financial benefit directly attributable to the infringing activity if the provider has the right and ability to control the infringing activity;
- must expeditiously take down or block access to the material upon proper notice of infringement; and
- must have filed with the Copyright Office a designation of an agent to receive notifications of claimed infringement.

The form for designating an agent with the Copyright Office is available at <http://www.loc.gov/copyright/onlinesp>. A list of agents registered with the Copyright Office is at <http://www.loc.gov/copyright/onlinesp/list>.

Limitation for Linking. Section 512(d) limits liability for the acts of referring or hypertext linking users to a site that contains infringing material. To take advantage of this limitation, a provider must:

- not have knowledge that the material is infringing;

- not receive a financial benefit directly attributable to the activity if the provider has the right and ability to control the infringing activity; and
- expeditiously take down or block access to the material upon receiving proper notification of claimed infringement.

Section 512(f) provides liability from damages (including attorneys' fees) based on certain misrepresentations about the status of allegedly infringing material.

Section 512(g) shields a provider from liability for taking down material claimed to be infringing, provided that the service provider follows certain notification procedures.

Section 512(h) establishes a procedure by which a copyright owner can obtain a subpoena from a federal court ordering a service provider to disclose the identity of a subscriber who is allegedly engaging in infringing activities.

Section 512(i) sets forth two additional conditions that a service provider must meet to be eligible for the limitations: (1) it must adopt and reasonably implement a policy of terminating in appropriate circumstances the accounts of subscribers who are repeat infringers; and (2) it must accommodate and not interfere with "standard technical measures."

Section 512(k) defines "service providers" entitled to the limitations of the section. For purposes of the first limitation, relating to transitory communications, "service provider" is defined in §512(k)(1)(A) as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."

For purposes of the other limitations, "service provider" is defined in §512(k)(1)(B) as "a provider of online services or network access, or the operator of facilities therefor."

4. Computer Maintenance or Repair

Title III expands the existing exemption relating to computer programs in §117 of the Copyright Act, which allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer.

5. Miscellaneous Provisions

Distance Education. Title IV, among other matters, directs the Copyright Office to report on how to promote distance education through digital technologies. The Copyright Office issued its report in May 1999. It can be found at <http://www.loc.gov/copyright/disted/>.

In sum, the report recommends several amendments to §110(2) of the Copyright Act, which exempts certain performances and displays in connection with instructional activities. The recommendations were:

- permit digital transmissions over computer networks;
- eliminate the physical classroom requirement in §110(2);
- add language that focuses more clearly on the concept of mediated instruction;
- add safeguards to minimize the greater risks of uncontrolled copying and distribution posed by digital transmission;
- retain the current “nonprofit” requirement for educational institutions;
- add a new provision to the Copyright Act to allow digital distance education to take place asynchronously; and
- expand the categories of works exempted from the performance right beyond the current coverage of nondramatic literary or musical works, adding other types of works but allowing performances of only reasonable and limited portions.

Webcasting. The Digital Performance Right in Sound Recordings Act of 1995 (DPRA) created a limited public performance right in sound recordings. The right only covers public performances by means of digital transmission. Three categories of digital transmissions were addressed at that time: broadcast transmissions, which were exempted from the performance right; subscription transmissions, which were generally subject to a statutory license; and on-demand transmissions, which were subject to the full exclusive right.

Transmissions of sound recordings over the Internet using streaming audio technologies (or *Webcasting*) has become a widespread practice since the enactment of DPRA. This activity does not fit squarely within any of the three categories that were addressed in the DPRA. Section 405 of the DMCA amends the DPRA, expanding the statutory license for subscription transmissions to include webcasting as a new category of

“eligible nonsubscription transmissions” and providing a new statutory license for making ephemeral recordings.

D. LEGISLATION

Statutory Damages. The Digital Theft Deterrence and Copyright Damages Improvements Acts of 1999 amended §504(c) of the Copyright Act to increase statutory damages by fifty percent.

Databases. Legislation is still pending to provide *sui generis* protection for databases. The movement to protect databases has been sparked by the Supreme Court’s decision in *Feist Publications v. Rural Telephone Ser. Co.*, 499 U.S. 340 (1991). That case held that compilations of facts that did not constitute creative original expression under the copyright law were not eligible for protection, regardless of the effort that may have been expended in their compilation. Thus, the Court struck down the “sweat of the brow” theory as a basis for protecting factual compilations. Since *Feist*, database publishers have faced the troubling prospect that their compilations may not be legally protected.

In 1997, the European Union adapted its Database Directive (implemented to date in Belgium, Denmark, German, Spain, Austria and Finland) providing *sui generis* protection to databases where the creator has made a substantial investment in obtaining, verifying or presenting the contents of the database.

On January 19, 1999, a bill, the Collections of Information Antipiracy Act (H.R. 354), was introduced into the House of Representatives that would provide special protection to databases. H.R. 354 would prevent the extraction or use in commerce of all or a substantial part (measured either quantitatively or qualitatively) of a collection of information gathered, organized or maintained by another person through the investment of substantial monetary or other resources so as to cause harm to the actual or potential market of that other person. The term of protection would be 15 years. Remedies include damages and injunctions. Criminal penalties are proposed for willful violations.

A competing bill, the Consumer and Investor Access to Information Act of 1999 (H.R. 1858) would provide the Federal Trade Commission (but not private parties) with enforcement authority to prevent theft of databases or misappropriation and resale of real-time stock quotes.

E. CASES

1. Music

Recording Indus. Assn. of America v. Diamond Multimedia Sys. Inc., 180 F.3d 1072 (9th Cir. 1999). Affirmed dismissal of a suit by the Recording Industry Association of America against makers of Rio, a portable music player designed to play MP3-formatted audio recordings. RIAA had sued

Diamond, contending that its Rio player was a “digital audio recording device” as that term is defined in the Audio Home Recording Act of 1992 (AHRA), and has such, that the Rio player must include a Serial Copyright Management System. After analyzing the statute, the court concluded that neither computers, their hard drives, nor the Rio player met the AHRA’s definition of digital audio recording device. In reaching this result, the court relied on the fact that the Rio player did not have the capability of making serial copies. From the court’s perspective, “the Rio’s operation is entirely consistent with the AHRA’s main purpose -- the facilitation of personal use.” The court explained that the Rio “merely makes copies in order to render portable, or ‘space- shift’ those files that already reside on the user’s hard drive. The court drew an analogy to the “time-shifting” concept articulated by the Supreme Court in its *Sony v. Universal City* opinion holding that consumer VCR taping of TV shows was fair use.

A & M Records, Inc. v. Napster, Inc., 54 U.S.P.Q.2d 1746 (N.D. Cal. 2000). Defendant, Napster, provides software and services that allow users to exchange sound recordings in digital MP3 format. The software works by allowing users to post, onto Napster’s server, listings of files that the user is willing to share with other users. Other users may then locate such listings using Napster’s searchable directory. When the desired listing is found, users may access each other’s files over the Internet directly without using Napster’s facilities. Plaintiffs, a group of record companies, sued Napster for contributory and vicarious copyright infringement and related state law claims.

Napster moved for summary judgment arguing that it was protected from liability under the Safe Harbor provision of the DMCA, 17 U.S.C. §512(a). The court denied Napster’s motion, holding that the protections of §512(a) were only available to a service provider “transmitting, routing or providing connections for, material through a system or network controlled or operated by or for the service provider.” Napster did not act as a service provider for purposes of §512(a) because it did not transmit infringing material through its system. Rather, that material was passed directly from one user to the next. The court observed that the legislative history of §512 demonstrates that “Congress intended the §512(a) safe harbor apply only to activities in which the service provider plays the roll of conduit for the communications of others.”

The court also held that even if Napster was a service provider for purposes of §512(a), Napster did not qualify for the safe harbor because it had failed to institute an adequate compliance policy as required by §512(i) to terminate access to its system by users who are “repeat infringers.” Napster’s policy merely blocked infringers’ passwords as opposed to the infringers’ underlying Internet protocol addresses. Because users could easily circumvent this policy by establishing new accounts

under different names, the court found that a genuine material issue of fact existed as to whether Napster had complied with §512(i).

UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000). Plaintiff record company sued defendant MP3 for its “my.MP3.com” service. That service allowed owners of music CDs to store, customize and listen to those recordings via the Internet. To achieve this, MP3 purchased and copied onto its Internet server several thousand popular CDs. Prior to making the service available to an end user, MP3 required the end user to establish that he or she already owned the particular CD by placing a copy of the commercial CD into the end user’s CD-ROM drive for a few moments. Once ownership of the CD was established, MP3 would allow the end users to access MP3’s copy via the Internet at any time and from any place.

Plaintiff record company moved for summary judgment on infringement, and MP3 asserted the affirmative defense of fair use. MP3’s argument was that it merely provided a transformative “space shift” by which subscribers who owned CDs would enjoy those sound recordings without lugging around the physical disk.

Observing that “the complex marvels of cyberspatial communications may create difficult legal issues; but not in this case,” the court granted the record company’s motion on infringement. The court rejected MP3’s fair use argument concluding that the “space shift” was not a transformative fair use but simply another way of saying that the unauthorized copies are being retransmitted in a different medium.

2. Databases

Information Handling Ser., Inc. v. LRP Publications, Inc., 54 U.S.P.Q.2d 1571 (E.D. Pa. 2000). Plaintiff published a computerized database of non-copyrightable U.S. Government statutes and provisions. Defendant, a competitor, copied the database. Plaintiff sued on state law claims of unfair competition and misappropriation. Defendant removed the lawsuit to the federal court on the basis of a federal question (copyright infringement). Denying plaintiff’s motion to remand it back to the state court, the federal district court held that a federal copyright law totally preempts state law misappropriation claims for unauthorized copying with respect to copyrightable as well as uncopyrightable elements. The court noted but did not decide the additional issue as to whether state law claims involving breach of plaintiff’s form license agreement were also pre-empted. The court wrote that it is “questionable whether such licenses, which are not the product of any bargaining, should be permitted effectively to expand copyright protection to information that is not copyrightable in the first instance.”

Tasini v. New York Times Co., 206 F.3d 161 (2nd Cir. 1999). Plaintiffs were a group of freelance writers who wrote articles for publication in defendants' periodicals. They sued when defendants republished the articles in the LEXIS-NEXIS electronic database. The district court granted a motion for summary judgment in favor of defendants. The court reasoned that the plaintiffs' articles were contributions to defendants' collective works. Defendants, as publishers of "collective works," had a privilege under §201(c) of the Copyright Act to distribute the articles in electronic format as a revision of the original collective work. The Second Circuit reversed holding that an electronic database was more than a mere revision of the original collective work and therefore exceeded the scope of defendants' privilege under §201(c).

3. **Linking**

Ticketmaster Corp. v. Tickets.com, 54 U.S.P.Q. 2d 1344 (C.D. Cal. 2000). Plaintiff *Ticketmaster* sued competitor *Tickets.com*, for deep linking (the practice of linking to sub-pages on *Ticketmaster's* Web site). The court held that it was not copyright infringement for the defendant to take basic facts (such as event, time, place and price) from plaintiff's publicly available web pages and use those facts so long as plaintiff's expression and method of presentation was not copied. The court also held that hyperlinking does not by itself involve a violation of the Copyright Act since no copying by *Tickets.com* is involved. It is, the court reasoned, "analogous to using a library's card index to get reference to particular items. . . ."

The court also dismissed *Ticketmaster's* breach of contract claim holding that a mere posting of "terms and conditions" on *Ticketmaster's* home page was not effective to create a legally binding contract. However, were the contract enforceable, the court held that it would not be pre-empted with respect to matters apart from copying, such as prohibitions not to deep link. The court distinguished the present case from cases where online contracts had been held enforceable by requiring users to click on an "agreed" icon. Absent the defendant's actual knowledge of the terms and conditions prohibiting linking, the motion to dismiss should be granted with leave to amend in case there are facts showing the defendant's knowledge of the contractual terms prohibiting deep linking and an implied agreement to them.

Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc., 75 F. Supp. 2d 1290 (D. Utah 1999). The district court granted a preliminary injunction in favor of a copyright owner against a defendant who had posted on its Web site links to other Web sites which contained infringing copies of the plaintiff's book. The court held that users who browsed third party Web sites were infringing the plaintiff's copyright and that the defendant, by

linking to those third party Web sites and actively encouraging end users to access infringing materials, had contributed to such infringement.

4. Digital Millennium Copyright Act

Universal City Studios, Inc. v. Reimerdes, 98 F. Supp. 2d 449 (S.D.N.Y. 2000). Plaintiffs were eight major motion picture studios who distributed movies in DVD format. DVD disks are subject to an industry-wide copy protection scheme known as the Content Scramble Systems (or CSS), an encryption-based security and authentication system that requires the use of appropriately configured hardware such as a DVD player to decrypt, unscramble and play back motion pictures on DVDs. Defendants developed and distributed a computer program that would enable users to circumvent the CSS copy protection scheme and hence make and distribute digital copies of DVD movies. Plaintiffs sued under §1201(a)(2) of the DCMA which prohibits unauthorized offering of products to circumvent technological measures that effectively control access to copyrighted works. Defendants argued that their conduct fell within one of the DCMA safe harbor provisions and, further, was protected by the First Amendment. The court disagreed. With respect to the safe harbor provisions of §512(c), the court held that §512(c) only protected defendants from liability for copyright infringement. Claims under §1201(a)(2) were directed to unlawful circumvention products, not copyright infringement. Therefore, the court concluded, §512(c) did not apply. The court applied a similar analysis to defendant's fair use argument, holding that the fair use defense of §107 did not apply to anti-circumvention claims under §1201(a)(2). The court also rejected defendant's First Amendment arguments.

Kelly v. Arriba Soft Corp., 77 F. Supp. 2d 1116 (C.D. Cal. 1999). Defendant operated a visual search engine which generated images of Web sites in lieu of descriptive text. The images were reduced "thumbnail pictures" of the sites. By clicking on a desired thumbnail, a user could view the address of the Web site where the image originated. Defendant's search engine maintained an index database of approximately 2,000,000 thumbnail images, including 35 images belonging to plaintiff, a photographer. Plaintiff sued after defendant refused to remove his images, claiming copyright infringement and violation of §1202 of the DCMA, governing the integrity of copyright management information.

Granting defendant's motion to dismiss, the court held that the use of the thumbnail images was a fair use under §107 of the Copyright Act. As to §1202 of the DCMA, the court held that plaintiff must show that defendant knew or should have known that its failure to provide copyright management information would lead to infringement of plaintiff's copyright. Here, a user who clicked on the thumbnail image would be given the name of the Web site from which the image was obtained and

where associated copyright management information would be available. Users were also informed that copyright limitations may apply to images retrieved by the defendant's search engine. Based on this, the court concluded that the defendant did not have reasonable grounds to know that it would cause its users to infringe the plaintiff's copyrights.

RealNetworks, Inc. v. Streambox, Inc., No. C99-2070, 2000 U.S. Dist. LEXIS 1889 (W.D. Wa. 2000). The court granted a preliminary injunction against defendant prohibiting distribution of programs that circumvented the copy protection features included in the plaintiff's RealAudio player in violation of §1201 of the DCMA. The court declined to grant a preliminary injunction against defendant's programs that merely converted audio and video files from RealMedia to other formats. These programs, the court reasoned, could be used for legitimate purposes. RealNetwork had not presented any evidence that the RealMedia format by itself was a "technological measure" under the DMCA to prevent violations of copyrights.

Telecomm Technical Services, Inc. v. Siemens Rolm Communications, Inc., 51 U.S.P.Q.2d 1798 (N.D. Ga. 1999). Court held that new §117(c) of Copyright Act applied retroactively to copying occurring prior to the adoption of the DMCA.

5. Other

Los Angeles Times v. Free Republic Electronic Orchard, 54 U.S.P.Q.2d 1453 (C.D. Cal. 2000). Plaintiff newspaper publishers sued defendant, an operator of a bulletin board Web site which allowed its members to post news articles, in their entirety, to which the members would add remarks or commentary. Defendant moved for summary judgment, arguing that the posting of news articles under their Web site is protected under the Fair Use Doctrine. The court held otherwise, stating that the balance of the four factors codified at 17 U.S.C. §107 militates against a finding of fair use. The court reasoned that the postings involved no transformative uses, but rather were mere copies. Although the primary purpose of the postings was to facilitate discussion, criticism, and comment, the ends could have been obtained without copying the articles (such as, for example, by hypertext linking to the original publishers' Web sites).

Sony Computer Entertainment, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000). Defendant sold a software program called "Virtual Game Station," which allowed users to emulate on a regular computer the functioning of the plaintiff's game console so that users who purchased the Virtual Game Station software can play plaintiff's games on their computers. The Virtual Game Station did not contain any of plaintiff's copyrighted material. However, in the process of creating the Virtual Game Station, the defendant copied the plaintiff's copyrighted BIOS

during a reverse engineering of plaintiff's product. The district court granted plaintiff's motion for preliminary injunction. On appeal, the Ninth Circuit reversed, holding that the intermediate copies of plaintiff's BIOS software made during the course of reverse engineering were protected fair use, because they were necessary to permit the defendant to make its non-infringing product function with the plaintiff's games.

Sun Microsystems, Inc. v. Microsoft Corp., 188 F.3d 1115 (9th Cir. 1999). In 1996, Sun licensed Microsoft to use the Java programming language. The license included a clause requiring Microsoft to develop enhancements to Java that would be fully compatible with certain Sun standards. Microsoft developed enhancements that were incompatible with Sun standards, and Sun sued under the license claiming that Microsoft's unauthorized enhancements exceeded the scope of the license and infringed Sun's copyright. The district court found that Sun was likely to succeed on the merits and granted a preliminary injunction against Microsoft. On appeal, the Ninth Circuit vacated the preliminary injunction holding that, although Sun was likely to win on the merits, the cause of action was one for breach of contract, not copyright infringement. Federal copyright law presumes irreparable harm for the infringement of a copyright, this is not the case with breach of contract. When a copyright owner sues on a negotiated copyright license, the presumption of irreparable harm applies only if the copyright holder establishes that the disputed terms are limitations on the scope of the license, rather than independent contractual covenants. In other words, before Sun can gain the benefit of a copyright infringement claim, it must definitely establish that its violated rights deal with copyright, not contract.

Tiffany Design, Inc. v. Reno Tahoe Specialty Inc., 55 F. Supp. 2d 113 (D. Nev. 1999). Defendant scanned plaintiff's photographs of the Las Vegas strip into a computer and then used selected portions of the scanned images to develop competing works. Granting a partial summary judgment in favor of plaintiff, the court held that scanning photographs into a computer, even for a brief time, constitutes infringement. However, the court found that a genuine issue of material fact existed as to whether incorporation of scanned images (in this case, pictures of individual buildings) into defendant's final work constituted infringement. The issue, the court said, was whether the modifications of the inserted images by defendant were significant enough to strip from the images the lighting, perspective, shading and other elements of plaintiff's protected expression.

F. JURISDICTION/INTERNATIONAL

The World Trade Organization (*WTO*) circulated a final ruling on May 5, 2000 upholding its preliminary findings that §110(5) of the U.S. Copyright Act, as amended by the 1998 Fairness and Music Licensing Act, violated Article 9.1 of *WTO's TRIPS*. Section 110(5)(b) of the Copyright Act exempts small

establishments from paying licensing fees to play non-dramatic musical works over radios or TVs. Small establishments are defined in the statute as restaurants, bars, and grills smaller than 3750 square feet or retail establishments smaller than 2000 square feet. The decision had been sought by The Irish Rights Music Organization. The WTO did, however, conclude that the “home-style” provisions under §110(5)(a) are compatible with TRIPS. Section 110(5)(a) allows public performance of a musical work on a “single receiving apparatus of the kind commonly used in private homes.” This exemption, as amended by the 1998 Fairness and Music Licensing Act, only applies to dramatic musical works such as operas and musicals on small scale equipment.

NOTES

1.