NEW MEDIA THREATS – RESPONDING TO CYBER-ATTACKS

Priscilla L. Dunckel
Baker Botts LLP

and

Michael K. Lindsey
Paul, Hastings, Janofsky & Walker LLP

October 15 – 17, 2008
The Hilton Austin
Austin, TX
Table of Contents

I. INTRODUCTION ....................................................................................................................... 1

II. THE TENSION BETWEEN TRADEMARK RIGHTS AND FREEDOM OF SPEECH ...... 1

A. A Balancing Act ...................................................................................................................... 1

   1. Trademarks ............................................................................................................................ 1

   2. Freedom of Speech ............................................................................................................... 2

   3. Trademark Rights v. Freedom of Speech ............................................................................ 2

B. Third Party Use of Trademarks ............................................................................................. 3

   1. Domain Names Incorporating Franchisor Trademarks .......................................................... 3

   2. Websites Operated by Franchisees ...................................................................................... 3

   3. “Gripe” and “Fan” Sites ........................................................................................................ 5

   4. Domain Names Used for Unrelated Purposes ..................................................................... 6

C. Anticybersquatting Consumer Protection Act ...................................................................... 7

D. Uniform Domain-Name Dispute-Resolution Policy ................................................................. 9

E. Fair Use and Other Legal Uses of Another’s Trademarks .................................................... 11

   1. Classic Fair Use ..................................................................................................................... 11

   2. Nominative and Other Legal Use ....................................................................................... 12

F. Special Trademark Issues ...................................................................................................... 14

   1. Linking .................................................................................................................................. 14

   2. Competitor’s Use of Franchisor-Specific Metatags .............................................................. 15

G. Keyword Advertising - Purchasing Competitor’s Trademarks for “Sponsored Advertising” ...................................................................................................................................... 16

H. Legal Remedies v. Practical Business Realities .................................................................... 17

III. COPYRIGHT ISSUES ........................................................................................................... 19

A. Protection of Franchisor Copyrightable Materials ................................................................. 19

   1. Subject Matter ....................................................................................................................... 19

   2. Ownership ............................................................................................................................ 19
3. Transfer of Ownership ................................................................. 20

B. Special Internet Copyright Problems ........................................ 20
   1. Background Information on Linking .................................. 20
   2. Deep Linking ..................................................................... 21
   3. Framing .............................................................................. 24

C. Digital Millennium Copyright Act ......................................... 27

IV. PROTECTION OF FRANCHISOR CONFIDENTIAL INFORMATION FROM DISCLOSURE .................................................. 29
   A. Trade Secret Protection Generally ................................... 29
   B. Inconsistency Between Internet Publication and Trade Secret Status .......... 30
   C. Potential for Restoring Trade Secret Status for Matter Posted on Internet .......... 31
   D. Potential Data Security and Sarbanes-Oxley §404 Concerns ......... 33

V. POTENTIAL LIABILITIES: FRANCHISOR AND THIRD PARTIES ................................................................. 35
   A. Trade Libel Laws Generally ........................................... 35
   B. State Anti-SLAPP Statutes .............................................. 37

VI. DO REAL WORLD LAWS APPLY IN VIRTUAL WORLDS? ................................................................. 40
   A. When Two Worlds Collide ............................................ 40
   B. Current and Potential Methods of Protection .................... 41

VII. FRANCHISE AND RELATED AGREEMENTS ................................................................. 43
   A. Franchise Agreements ................................................. 43
      1. Trademark license ...................................................... 43
      2. Confidential Information and Trade Secrets .................. 43
      3. Termination ............................................................ 44
      4. Other ........................................................................ 44
   B. Website Development Agreements/Web Master Agreements .......... 44
   C. Independent Contractor Agreements ................................ 45
D. Confidentiality/Non-Disclosure/Employment Agreements for Franchisee Employees.................................................................45

E. Linking Agreements........................................................................45

VIII. CONCLUSION......................................................................................45
NEW MEDIA THREATS – RESPONDING TO CYBER-ATTACKS

I. INTRODUCTION

The world of franchising understandably has some ambivalence about the internet and new media generally. While franchisors certainly understand the broad reach and powerful impact that the internet can have in promoting and extolling their products and services, they have also come to understand that their companies’ critics can just as easily exploit the same technologies. Given the libertarian cultural roots of the internet and the medium’s modest cost of communicating to an enormous audience, the internet has become the modern-day soapbox, with a worldwide reach, for those wishing to air their personal complaints regarding people, companies and even entire franchise systems. Such complaints – frequently posted by disgruntled customers or former employees – may have little basis in reality and may include the complainant’s unauthorized use of the target’s protected trademark or a parody thereof. Franchisees and even franchisee associations have also had unpleasant experiences with cyber-attacks.

The new media can present other, frequently unexpected threats to franchise systems. Such threats can be delivered through an almost dizzying variety of media, ranging from franchisee or third party websites, to chat rooms or blogs, to social networking sites and virtual worlds. The purpose of this paper is to survey some of the more significant of such threats, analyze the existing and developing law in this area, and provide recommendations for how such threats and related risks may be appropriately addressed.

II. THE TENSION BETWEEN TRADEMARK RIGHTS AND FREEDOM OF SPEECH

A. A Balancing Act

1. Trademarks

For a franchise system, trademarks and service marks are what unify the system and communicate to consumers that this franchise business will provide them the same quality of goods or services they have come to rely on from other franchisees from the same franchise system. The trademarks and service marks not only identify the franchise system as the source of the goods or services, but represent the goodwill and reputation of the franchisor and its...
network of franchisees, which result in continued public patronage. Accordingly, one significant benefit of a franchise is that the new business will benefit from “repeat customers” of the franchise system drawn to the business by the familiar trademarks from the first day the business opens its doors.

Trademark owners have a right and an obligation to control the use of their trademarks. Consumers rely on trademarks not only to identify the source of the goods or services but to assure a consistent quality of goods and services offered under the mark. Under the theory of “naked licensing,” a trademark owner may be deemed to have abandoned its trademark rights if it has licensed its trademark without the right to and actual exercise of control over the quality of the goods or services offered under the mark.

2. Freedom of Speech

The First Amendment of the U.S. Constitution guarantees its citizens the right to freedom of speech to express their thoughts and views without restriction by the government. Such rights include the right for individuals to express their opinions about businesses, products and/or services, whether the opinions are positive or negative. In our technology-driven world, free speech is often expressed through such outlets as on-line product reviews; blogs; chat rooms; websites set up for the specific purpose of complaining about a company or product (often referred to as “gripe sites”), and websites set up for the opposite purpose of promoting a favorite business or product (referred to as “fan sites”) in addition to the more traditional outlets such as newspapers, radio, television, and word of mouth. In fact, the internet seems to have given every individual the opportunity to say what they want and be heard, whether they are identified or make their thoughts known anonymously.

3. Trademark Rights v. Freedom of Speech

The rights of U.S. citizens to freely express themselves and the rights of trademark owners to control and protect the use of their trademarks often come into conflict on the internet, as they have to a much lesser degree in other media. Trademark law recognizes various legitimate uses of trademarks by parties other than the trademark owner, including for such purposes as news reporting, comparative advertising, parody, criticism, comment, and other types of “fair use.” Historically, businesses have used the trademarks of their competitors to compare the competitor’s products to their own in television and radio commercials and to tout the alleged superiority of their own product. This comparative advertising is accepted and protected, so long as the comparisons don’t include false or misleading statements. Similarly, investigatory news programs use trademarks in their news reports, while criticizing or complimenting a company’s actions or products. However, in general, traditional media have offered individuals only very limited outlets to air their individual complaints and disputes in television programs, radio “call-in” shows, and letters to the editor for print media.

The internet has exploded as a leveling field for communications from individuals and business entities, and seems to have tipped the scale in favor of individuals. While traditional laws relating to false advertising, libel, slander, defamation, and trademark protection still apply, the new media outlets of blogs, chat rooms, product reviews, gripe and fan sites offer opportunities for comments, opinions, and complaints to be broadcast worldwide immediately upon posting. When these comments, opinions and complaints are directed at businesses and/or their products, they generally include references to and often distortions of trademarks owned by the target company. These comments may last forever in “caches” or disappear just as quickly, leading to difficulty in tracing and identifying their source. Consequently, the new
media threats require thoughtful consideration and analysis of not only the rights of the company or individual being attacked or complimented and how to enforce them, but also the risks, benefits, and costs of taking action to stop such activities.

B. Third Party Use of Trademarks

1. Domain Names Incorporating Franchisor Trademarks

One issue that often troubles trademark owners and franchisors is the incorporation of their registered trademarks into domain names. Some of the domain names are a legitimate use of the trademarks and some are not. Registration of a domain name that incorporates a trademark owned by someone else is not necessarily a violation of any trademark rights per se.

Use of a domain name may qualify as trademark or service mark use, but only if the domain name functions as a source identifier of goods or services (e.g., Amazon.com). Use of a domain name merely as an informational part of the domain name registrant's internet address or as part of the contact information for the domain name registration is not trademark use and thus may not constitute infringement of a third party's trademark, although depending upon the nature of the use, it could constitute trademark dilution. Such use is arguably similar to an address for a home or business, merely directing the person where to go.6

An individual or entity can register a domain name and hold on to it without violating someone’s trademark rights unless the domain name is registered in bad faith or linked to a website that creates a likelihood of confusion with the trademark owner’s marks. Bad faith occurs in the registration if the domain name is registered with the intent to try to sell it to the trademark owner, to block the trademark owner from getting a desired domain name, or another improper intent. However, if a trademark owner approaches the owner of a domain name and the domain name owner agrees to sell the domain name, for whatever price, the sale of the domain name will not, without more, establish the element of bad faith. Likewise, if a trademark owner wants a particular domain name, the mere fact that someone else owns it will also not establish bad faith without other facts showing improper conduct.

2. Websites Operated by Franchisees

A franchisee may register a domain name with the franchisor’s trademarks and set up its own website to promote its franchised business. Such use of the trademark is usually well-intentioned and difficult to stop, as long as it complies with the terms of the license granted in the franchise agreement. A franchisee, who has been authorized to use the trademarks, may register a domain name with the franchisor’s trademark plus additional terms, often geographic. For example, a franchisee may register a domain such as www.TRADEMARKnorthchicago.com for use in promoting its franchise business. Since the franchisee’s business is operated in compliance with the terms of a franchise agreement, its use of the trademarks, even in a domain name, is considered to be controlled by the franchisor. Therefore, unless the franchise agreement specifically restricts use of the trademark in a domain name, such use of the trademark will likely be considered authorized and within the scope of the license, even if the franchise agreement is silent regarding domain names.

---

One problem that can arise from a franchisee registering and using a domain name incorporating the franchisor’s trademark occurs when there are a number of franchisees in the same geographic area, and the associated website directs potential consumers to just one or a group of franchise businesses to the detriment of the others. This situation generally upsets other franchisees in the area, who feel the website is encroaching into their protected territory. Furthermore, the franchisee’s website may show up in search engines and draw consumers to it and away from the franchisor’s official site. In some instances, the franchisee may pay to have its website listed high in the search results or purchase keyword advertising to assure its website comes up when the franchisor’s trademark is searched. (See discussion of keyword advertising in Section II.G. below.)

Other websites may be set up by current franchisees to connect with other franchisees of the franchise system to exchange ideas and/or to complain about the franchisor. Former franchisees or franchisee associations may set up websites or blogs to communicate with each other. For current franchisees, use of a trademark in a domain name for a purpose other than promoting their business would generally be outside the scope of the license granted in their franchise agreement. However, use of a domain name by a former franchisee to complain about the franchisor or franchise products may be protected as free speech.

If a franchisee leaves the franchise system, the domain name goes with the franchisee unless there is an agreement by the franchisee to transfer it to the franchisor. This same domain name can be used to complain about the franchisor or the franchise products. In some instances, such as a bankruptcy, the ex-franchisee may be able to legitimately use the domain name to direct consumers to another business offering competitive products or services.

The Anticybersquatting Consumer Protection Act (“ACPA”) provides a cause of action for a trademark owner against registration of a domain name with its trademark, however, the trademark owner must prove that the registrant has a bad faith intent to profit from the mark.7 (See discussion in Section II.C. below.) Therefore, without a provision in the franchise agreement to the contrary, the franchisee would normally have a legitimate right to register a domain name with the franchisor’s trademark in connection with its business. Following termination of the franchise agreement, unless the franchisor has evidence that the ex-franchisee has a bad faith intent to profit from the trademark, the situation may not meet the required factors for a remedy under the ACPA.

A Uniform Domain-Name Dispute-Resolution Policy (“UDRP”) proceeding (as discussed in Section II.D. below) would also not be available to the franchisor in this situation, again because the domain name would not have been registered in bad faith. While the franchisor would have a right to stop use of the domain name for a commercial purpose, there would be no easy procedure to use to obtain or stop use of the domain name short of litigation. Of course, litigation for trademark infringement is costly, and a recovery of the costs and fees or damages are very difficult to obtain. The success of litigation will depend on the facts of the case, how the domain name is actually used and whether the franchisor can prove there is a likelihood of confusion.

A similar situation is created when a franchisee operates a website for his or her franchised business using a domain name that does not incorporate the franchisor’s trademark. He or she then puts that domain name in all of its advertising, along with the address and

---

telephone number of the particular location, including on advertising materials obtained from the franchisor. The franchisee therefore promotes its own franchise business and its website on everything that is distributed, closely associating them with the franchise system. When the franchise agreement is terminated, there is no legal basis for the franchisor to claim ownership of the domain name that has been so closely associated with the franchise system without a contractual obligation. In this situation, where the domain name does not incorporate the franchisor’s trademarks, there is a higher risk that the franchisor will not be able to ultimately gain control of the domain name than there is if its trademark is incorporated.

A provision in the franchise agreement requiring any domain name used in connection with the franchise business to be transferred to the franchisor upon termination for any reason, as well as the standard provision that the franchisee may not use the franchisor’s trademarks following termination for any purpose, including in a domain name, will help avoid future use of a domain name that has been closely associated with the franchise system after the franchisee has moved on. Since the domain name is recognized by many courts as a property right, the franchisor may also want to take a security interest in the domain name since a bankruptcy court is more likely to enforce a security interest in a domain name than an agreement to transfer.

3. **“Gripe” and “Fan” Sites**

A ‘gripe site’ is a website established to criticize corporations, businesses and products, and can damage a company’s reputation. These can take the form of “xxxsucks.com,” “xxxfraud.com,” “boycottxxx.com,” or “ihatexxx.com.” In fact, gripe sites are so common that there have been suggestions to set up a new top level domain of “.sucks” for domain names to be used for websites complaining about businesses and other issues.

A ‘fan site’ is a website created and maintained by the fans of a company, product or celebrity. Because positive comments from consumers can enhance the goodwill in a mark, action may not be necessary. Still, trademark owners are wary since fan sites may appear to be authorized or suggest uncontrolled use of a mark. Furthermore, often fans set up fan sites with domain names that the trademark owner would like to have for their business. Unless these websites sell advertising or make other commercial use of the domain name, they may also be protected under the tenets of freedom of speech.

Both gripe and fan sites can affect the strength and integrity of a mark and the goodwill of a business. United States courts generally hold that the protection of free speech outweighs the proprietary rights of a single trademark owner, and are unwilling to enjoin such websites. However, courts are willing to enjoin such acts when gripe or fan sites engage in commercial activities. A legitimate gripe site protected as free speech does not attempt to sell any products, but merely displays consumer commentary.

---

8 Many franchise systems create standard advertising and marketing materials that have a blank area for the local franchisee to customize and insert its local information. If the local franchisee maintains a website, the web address is often included with the address and telephone number of the franchise business.

9 See *Bosley Med. Inst. Inc. v. Kremer*, 403 F.3d 672 (9th Cir. 2005); *Taubman Co. v. Webfeats*, 319 F.3d 770, 778 (6th Cir. 2003) (use of the domain name taubmansucks.com “removes any confusion as to source”).

10 See *People for Ethical Treatment of Animals v. Doughney*, 263 F.3d 359 (4th Cir. 2001).
Challenging gripe and fan sites can bring unwanted attention to a franchisor or trademark owner. Each has its own issues. For gripe sites, the disgruntled employee, customer or franchisee will often be very committed to defending against any efforts to stop their use of the site. The more public attention they can attract, the better. Because the right to complain and criticize is protected as the very core of free speech, there are consumer advocacy organizations that are willing to assume the defense of such use of a trademark without charge to the person who has registered the domain name at issue. Furthermore, if the trademark owner takes action against them, this will often confirm to the speaker that their actions are disturbing to the trademark owner and therefore they are getting what they want. Sending a cease and desist letter or escalating the dispute to a UDRP proceeding or litigation may become a public relations nightmare, with letters and court documents posted on the internet on a personal website or one operated by the consumer advocacy organization. Sometimes, this will gain more attention than the original website and complaints.

As far as the fan sites, these can bring their own challenges because the domain name registrant is very loyal to the trademark owner and wants to promote them. However, the fan sites can become problematic to a trademark owner because they put out their own opinion of the business or product which may or may not be consistent with the position of the trademark owner. In some cases, the fan site may make unsupported claims about the business or product that the trademark owner does not agree with or may be legally restricted from making. If the owner(s) of the fan site are associated with the trademark owner, such as a franchisee or employee, their actions may be deemed to be those of the franchise system. In some instances, a UDRP proceeding can be successful in stopping use of a trademark in a domain name for a gripe or fan site, but the actions are determined on a case by case basis depending on the relevant facts regarding the use.

4. Domain Names Used for Unrelated Purposes

Domain names that incorporate registered trademarks are often registered by domain name registrars or others. In many cases, these domain names are maintained on a “link farm” where the owner posts links to websites operated by competitors of the trademark owner and is paid for each “click” to the relevant website. Such link farms are intended to drive and increase traffic to websites willing to pay for the clicks. For example, if the domain name incorporates the trademark of a restaurant, then it will lead to a website that has a list of links to websites for various restaurants. The list may or may not include the trademark owner’s own website. Then, when someone accesses a website through one of the posted links, the domain name owner will receive payment for the link/access.

There are also companies that make a business of registering domain names with variations of well-known trademarks, and may own 500,000-1,000,000 domain names at a time. They may add hyphens, generic terms, or misspell the well-known mark (“typo-squatting”). No business appears to be immune, with domain names registered by third parties incorporating versions of such well-known trademarks as Pier 1, Microsoft, Estee Lauder, Land’s End, Hewlett-Packard, Pottery Barn, General Electric, Google, Wachovia, Exxon-Mobil, Yahoo, and many, many more. Once registered, the domain names are often used for the link farms discussed above. When the domain names are discovered by the trademark owner, these companies often will cooperate to cancel or transfer the domain name in order to avoid a judgment or adverse ruling. Any one individual domain name is not of significant value to this type of company, since they will still have hundreds of thousands of others.
In other situations, domain names are registered and linked to websites that post an “Under Construction” or “Coming Soon” announcement. Or, the domain name may be inactive and when searched, an ERROR will show, stating that the URL is not available. This is especially frustrating to trademark owners who would like to register a domain name, and find it is registered by someone else who is not using it. Without commercial use of the domain name or evidence that it was registered to obtain money from or interfere with the trademark owner, such registration would not meet the standards for a UDRP proceeding, violate the ACPA discussed below or constitute trademark infringement.

C. Anticybersquatting Consumer Protection Act

The ACPA Anticybersquatting Consumer Protection Act (also known as the Truth in Domains Act) provides a cause of action by an owner of a distinctive or famous mark against the registration, trafficking, or use of a domain name that is identical or confusingly similar to that mark, or in the case of a famous mark, is dilutive of that mark, if the registrant has a bad faith intent to profit from the mark.\(^\text{11}\) The ACPA outlines nine factors to be considered in determining whether a person has a bad faith intent to profit from such a trademark\(^\text{12}\), including such factors as:

1. the trademark or other intellectual property rights of the person, if any, in the domain name;

2. the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

3. the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

4. the person’s bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

5. the person’s intent to divert consumers from the mark owner’s online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

6. the person’s offer to transfer, sell or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person’s prior conduct indicating a pattern of such conduct;


7. the person’s provision of material and misleading false contact information when applying for the registration of the domain name, the person’s intentional failure to maintain accurate contact information, or the person’s prior conduct indicating a pattern of such conduct;

8. the person’s registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

9. the extent to which the mark incorporated in the person’s domain name registration is or is not distinctive and famous within the meaning of the Act.

Notwithstanding the foregoing, if a court determines that the person believed and had reasonable grounds to believe that use of the domain name was a fair use or otherwise lawful, then such actions will not constitute bad faith.

Each case brought under the ACPA is decided on its own facts, but the types of actions that have been found to constitute a bad faith intent to profit from a trademark under ACPA are (i) a pattern of registering domain names of other trademark owners, 13 (ii) making false statements when registering the domain name, and attempting to get the trademark owner to pay for the domain name; 14 (iii) registration of a domain name by a former employee with knowledge of the employer’s trademark rights, and then offering to sell the domain name to the trademark owner. 15

Actions where free speech has been found to outweigh the trademark owner’s rights are (i) criticism of the trademark owner with a disclaimer and a link to the trademark owner’s site for internet users who were looking for the trademark owner’s site 16, and (ii) use of a website by a consumer to complain about its business dealings with the trademark owner, with a comment section for other consumers to share feedback about other contractors, and a disclaimer that it was not the site of the trademark owner. 17

Available remedies for violations of the ACPA are (i) a transfer of the domain name to the trademark owner; (ii) cancellation of the domain name registration; (iii) an injunction against registering a domain name with the trademark owner’s mark(s) and/or against use of the trademark owner’s mark(s); (iv) a recovery of actual damages, or (v) statutory damages in an

---

13 Northern Light Technology v. Northern Lights Club, 236 F.3d 57 (1st Cir. 2001).

14 See People for the Ethical Treatment of Animals, 263 F.3d at 369.


16 Lamparello v. Falwell, 420 F.3d 309 (4th Cir. 2005).

amount not less than $1,000, and not more than $100,000 per domain name. In exceptional cases, the trademark owner may recover its attorney’s fees.

D. Uniform Domain-Name Dispute-Resolution Policy

The Internet Corporation for Assigned Names and Numbers ("ICANN") was formed in 1998 as a not-for-profit partnership to coordinate the internet’s naming system throughout the world. ICANN identifies its mission “to coordinate, at the overall level, the global internet’s systems of unique identifiers, and in particular to ensure the stable and secure operation of the internet’s unique identifier systems.” ICANN has established the UDRP (Uniform Domain-Name Dispute-Resolution Policy) as an expedited administrative proceeding that can be used to resolve most types of trademark-based domain name disputes in a period of approximately 2 months. Under the UDRP, a trademark owner can commence an administrative proceeding electronically with an approved dispute resolution service provider (e.g., World Intellectual Property Organization or WIPO) in order to acquire or cancel a domain name, regardless of where the accused domain name registrant is located. A UDRP proceeding is usually decided by a single panelist, however, either the complainant or the respondent may elect to have it decided by a three-person panel. Fees are paid by the complainant unless the respondent elects the three-person panel, in which event the respondent will be responsible for one-half of the fees.

To prevail in a UDRP proceeding, a trademark owner/complainant must prove that:

- the domain name at issue is identical or confusingly similar to a trademark owned by the complainant;
- the domain name registrant has no rights or legitimate interests in the domain name; and
- the domain name was registered and/or used in bad faith.

Generally the first two elements are easy for the complainant to establish. The trademark owner first must establish its own trademark rights by submitting evidence of a trademark registration or common law rights. Once such rights are established, the complainant must then show that the domain name at issue incorporates the complainant’s trademark or a variation or misspelling of the trademark.

There has been some disparity on the issue of whether domain names containing a trademark with the term “sucks” are identical or confusingly similar to the trademark. For

---

20 ICANN Mission (from the bylaws); available at http://www.icann.org/about.
21 Trademark rights in the United States come from use of a trademark, not registration, however federal or state registrations provide additional benefits. Common law rights are established through actual use of a trademark in connection with the sale or goods or services. Such rights are limited geographically to the area in which the mark has been actually used.
example, in *Société Air France v. Virtual Dates, Inc.*, the Panel noted that the domain name airfrancesucks.com consists of the well known trademark AIR FRANCE and the addition of the generic term “sucks.” The Panel found that AIR FRANCE was the dominant portion of the domain name and found it to be confusingly similar. The Panel noted that there is a split among UDRP decisions, with the majority of decisions finding confusing similarity in cases involving a trademark with the term “sucks.” The minority of decisions have found that adding the term sucks is an obvious indication that the domain name is not affiliated with the trademark owner, and therefore not confusingly similar.

The second element, proving that the domain name registrant has no rights or legitimate interests in the domain name, is also fairly straightforward. The complaint must make a reasonable showing that the terms in the domain name at issue are not part of the corporate or business name, the person’s surname, and that there is no other legitimate interest in those terms. The burden on the second element is generally on the respondent to show that it does have legitimate rights or interests in the domain name.

Keep in mind that the respondent may be able to establish a legitimate interest in the domain name if the terms in the domain name (and the complainant’s trademark) are descriptive. In other words, if the complainant claims trademark rights in a descriptive mark, even if there is evidence that the descriptive mark has acquired distinctiveness, the respondent may be able to show a legitimate right to use the descriptive terms to describe its own goods or services, which may or may not be competitive.

The most contested issue in a UDRP proceeding is the third factor, the issue of bad faith. The UDRP sets forth four examples of bad faith, which are not exhaustive:

- Circumstances indicating that the domain name owner has registered the domain name primarily for the purpose of selling or renting the domain name for valuable consideration in excess of out-of-pocket costs;
- Circumstances indicating the domain name owner has registered the domain name in order to prevent the owner of the trademark from registering the domain name, provided respondent has engaged in a pattern of such conduct;
- Circumstances indicating that the domain name owner is a competitor and registered the domain name in an attempt to disrupt the trademark owner’s business;
- Circumstances indicating that the respondent is attempting to attract internet users by creating a likelihood of confusion with the trademark owner’s mark(s).

In most cases, the UDRP procedures work well to resolve disputes involving the registration of domain names that incorporate terms that are identical or similar to a registered or common law trademark owned by another. Such a procedure is low cost in comparison to


23 UDRP Rule 4(b).
litigation, a decision is reached fairly quickly, and the remedy (transfer or cancellation of the domain name) is received without having to wait for action to be taken by the respondent. In any event, in many cases, the mere filing of a UDRP Complaint will act as an incentive for the domain name owner to agree to the transfer without the need for a decision by the arbitrator or panel, however, the dispute resolution service providers have no authority to order a recovery of damages or attorneys fees.

Evidencing the difficulty of proving bad faith, Warner Bros. Entertainment Inc. was unable to prove the requisite bad faith to obtain transfer or cancellation of the daisydukes.com domain name. Warner Bros.' complaint was based upon its common law rights in the DAISY DUKE mark, derived from the TV series The Dukes of Hazzard. Although the registrant was using the daisydukes.com domain name to redirect users to a commercial pornographic site, the Panel agreed with the registrant's arguments that the term “Daisy Dukes” has become generally recognized as a type of clothing worn by attractive woman and was used for respondent's business purpose of directing users to attractive women. Therefore, the Panel found that there was no evidence of bad faith.24

E. Fair Use and Other Legal Uses of Another's Trademarks

“Fair use” is a defense against a claim by a trademark owner of infringement of its trademark rights, whether registered or common law. The defense is that the alleged infringer is using the trademark legally, and therefore such use is not infringing. The fair use defense or legal and legitimate use of the trademark of an unrelated party are all grounded in the rights to free speech, i.e., the right to make truthful statements to communicate information without restriction. Two very different kinds of fair use of a trademark are classic and nominative fair use.

1. Classic Fair Use

Under the common law classic fair use defense codified in the Lanham Act at 15 U.S.C. § 1115(b), “[a] junior user is always entitled to use a descriptive term in good faith in its primarily, descriptive sense, other than as a trademark.”25 To establish a classic fair use defense, a defendant must prove the following three elements: (i) defendant’s use of the term is not as a trademark or service mark; (ii) defendant uses the term “fairly and in good faith;” and (iii) defendant uses the term “only to describe its goods or services.”26 For example, use of “Sweet-tart” to describe juice drinks was upheld under the classic fair use defense, even though the plaintiff owned a TM for SWEE TARTS.27 Likewise, use of “Fish Fry” to describe fish seasoning products was found to be fair use notwithstanding plaintiff’s registration for Fish-Fri for fish seasoning products.28 In a classic fair use situation, the trademark owner will usually


25 Cairns v. Franklin Mint Co., 292 F.3d 1139, 1150 - 51 (9th Cir. 2002) (citing McCarthy on Trademark and Unfair Competition § 1145 (4th ed. 2001)).

26 Id. at 1151.

27 Sunmark, Inc. v. Ocean Spray Cranberries, 64 F.3d 1055 (7th Cir. 1995).

28 Zatarains, Inc. v. Oak Grove Smokehouse, Inc., 698 F.2d 786, 796 (5th Cir. 1983).
have argued that consumers have learned to recognize the descriptive term(s), when used in a trademark sense, to identify the trademark owner as the source of goods or services offered in connection with the mark. A trademark owner who adopts a descriptive term as a trademark does so with the knowledge that it cannot stop use of such a trademark in its classic descriptive sense, i.e., to fairly and in good faith describe a competitor's goods or services, the geographic origin of the goods or services, or as a surname to identify the person running a business, even if competitive. Classic fair use has been held to be legal, even if there is a certain amount of confusion. Therefore, the key element in an analysis of classic fair use is the type of use (descriptive rather than trademark use) and not whether there is confusion.

2. **Nominative and Other Legal Use**

Nominative use is different from classic fair use because it refers to use of the trademark to refer to the actual trademark owner or its goods. In other words, this type of use "names" the owner of the trademark and the source of the goods and is not really a defense, but is used in the analysis of whether use of the trademark is likely to be confusing to consumers to imply an affiliation, endorsement or sponsorship. In *New Kids on the Block v. News America Publishing, Inc.*, the Ninth Circuit identified three questions relevant to the analysis of whether nominative use of a trademark (to identify the trademark owner) is likely to cause confusion and is infringing:

- Is the product or service of the trademark owner one which is readily identifiable without use of the trademark?
- Has the mark been used by the defendant more than is reasonably necessary to identify the product or service?
- Has the defendant done acts that would falsely suggest sponsorship or endorsement by the trademark holder?

Thus, the key element in an analysis of nominative use is whether such use creates a likelihood of confusion in the minds of consumers as to the source or sponsorship of the products or services. If such use creates a likelihood of confusion, then it will constitute infringement of the trademark owner's rights.

In a recent decision, the Southern District of New York held that eBay's use of Tiffany's marks by advertising the availability of Tiffany items on the eBay website, was protected by the doctrine of fair use. In analyzing the fair use factors, the court found that the product in question, Tiffany silver jewelry, was not readily identifiable without the use of the Tiffany trademark. In addition, the court found that eBay demonstrated that it used only so much of the mark as was reasonably necessary to identify the product, noting that use was limited to the

30 971 F.2d 302, 308 (9th Cir. 1992).
TIFFANY name, as opposed to fonts or symbols associated with Tiffany. 33 Finally, the court found that eBay did not do anything that would suggest sponsorship or endorsement of eBay by Tiffany. 34 Because the court found that authentic Tiffany merchandise was sold and that eBay always removed potentially infringing listings when Tiffany notified them of such, no conclusion could be made that eBay’s use of the TIFFANY mark created the impression of sponsorship or endorsement. 35 This was further strengthened by the fact that Tiffany’s “About Me” page on the eBay website contained a disclaimer that Tiffany did not endorse or sanction the sale of products through eBay. 36

Nominative fair use often comes into play in comparative advertising, where one company compares its goods or services to the goods or services of another company. The user identifies its own company with its own trademarks and the competitor’s company or products with that company’s trademarks, and then makes a comparison. This is nominative fair use because the competitor’s mark is being used to identify the competitor’s products. As long as there is no likelihood of confusion as to source, affiliation, endorsement or sponsorship, nominative use of a trademark does not constitute infringement. 37

Another way in which a trademark may be legally used in a nominative way by others unaffiliated with the trademark owner is to communicate truthful facts. For example, a franchisee may include a statement on his resume that he was a franchisee for XX franchisor from X date until X date. Such use of the franchisor’s trademark would communicate to a potential employer the ex-franchisee’s experience in a given field. In addition, such person could also post a blog that identified him or her as an ex-franchisee and give his opinion about the franchise system, its products or services. This nominative use of a trademark would be protected as free speech.

On the other hand, an ex-franchisee would likely not be allowed to put a big sign in the window of his competitive store or a prominent statement on his website for a competing business stating he is a former franchisee of XX franchisor because the purpose for such a sign or statement would be commercial and intended to improperly connect the new business with the franchised business and the associated goodwill. Signage or statements like this would be likely to confuse consumers as to the source or sponsorship of the products or services offered by the new business. Use of the trademark of the franchisor would not be protected as free speech, but would more likely be deemed trademark infringement since the mark would falsely suggest sponsorship or endorsement by the trademark holder, and the trademark would have been used more than is reasonably necessary.

33 Id. at * 28.
34 Id.
35 Id. at * 28-29.
36 Id. at * 29.
37 All factual statements used in comparative advertising must also be truthful and not misleading or it will constitute false advertising in violation of Section 1125 of the Lanham Act.
A service business may legitimately use another company's trademark to truthfully indicate that it services that brand of product. However, such use should not imply sponsorship or authorization by or a connection to the product manufacturer. Use of trademarks in other commercial enterprises such as surveys, news commentary, and similar circumstances that do not imply a sponsorship, association, endorsement or connection with the trademark owner are also legitimate, non-infringing, and protected as free speech. Use of a trademark belonging to another company to criticize the trademark owner or its goods or services is protected as free speech.

It is often an annoyance and, depending on the level of animosity, very frustrating for a trademark owner to see criticism posted on the internet for the whole world to see in a blog, chat room, or even a fully dedicated website. However, generally there is nothing that can be done to stop such exercise of free speech unless there are statements made that can be proven to be factually false, and the person should know they are false. In some such instances, it is helpful to notify the owner of the blog, chat room, website, or other conveyance of the falsity, provide them the accurate information and demand it be changed. If the blog or site owner is a third party, they might be persuaded to remove the offending material in order to avoid liability. However, if the owner of the medium being used to convey the false information is the “aggrieved party,” such a demand may only encourage them to continue. The notice will provide them with the feedback that their postings are working, and may become incentive to increase the postings. Furthermore, if the statements are false, in addition to claims for false advertising under the Lanham Act, if applicable, traditional causes of action for product disparagement, injurious falsehood, slander of goods and other similar actions are also available as would be available for any other type of publication of false information about a business or individual. (See discussion in Section V.A. below on Trade Libel.)

F. **Special Trademark Issues**

1. **Linking**

A ‘link’ is a connector placed on a webpage used to bring internet users from one webpage to another. Links can direct internet users to the homepage of another website, or to an interior page within the linked site (known as a deep link).

Website owners typically encourage others to link to their sites to increase traffic. However, in certain instances, companies have objected to linking on the basis that it suggests sponsorship or a business relationship between the owners of the linked sites. Trademark owners have likewise objected to linking from websites deemed to be objectionable and to offensive domain names redirected to the trademark owner’s website.

---


Deep linking (hyperlinks that bypass the home page and take the user directly to an internal page in that site) may create the impression that two sites are associated with each other. In *Ticketmaster Corp. v. Tickets.Com, Inc.*\(^{41}\) Tickets.com provided deep links to inner Ticketmaster pages to allow users to make ticket purchases, bypassing the Ticketmaster ticket sales site’s home page and advertising. Tickets.com included a statement with the link that it cannot sell the tickets but will refer the buyer to another company’s website that can sell the tickets. The court found that the disclaimer eliminated the possibility of unfair competition because there was no confusion as to the source of the ticket purchase.

2. **Competitor’s Use of Franchisor-Specific Metatags**

A ‘metatag’ is invisible programming code utilized by website developers to provide information for search engines regarding webpage content. This data is used, in part, by search engines to identify and display search results matching a given query. Metatags have been used in an attempt to direct search engine users to a particular site, even if the content of the site does not correspond to the search term or trademark. However, this practice may be on the verge of becoming obsolete as search engines realize that because of manipulation of the metatags by webmasters, use of metatags has become a poor indicator of relevancy in a search request. Therefore, modern search engines primarily use algorithms that rank a website by the number of other sites that link or point to it. Trademark owners frequently protest the use of their marks in metatags where such use leads internet users to another’s website.

Courts differ on whether the mere use of another’s mark in a metatag constitutes infringement. One view taken by some US courts is that use of a mark in a metatag which redirects traffic from the mark owner to a third-party site constitutes infringement even though, once having arrived, the user would know that it was not at the mark owner’s site.\(^{42}\) The Seventh Circuit found infringement for use of a direct competitor’s trademark in a metatag based on the initial interest confusion doctrine.\(^{43}\) Initial interest confusion occurs when a customer is lured to a product by the similarity of the mark, even if the customer realizes the true source of the goods before the sale is consummated. The Seventh Circuit found that the use of the competitor’s trademark in metatags diverted customers to the infringer’s website and likely caused customer confusion.\(^{44}\) In a similar vein, the Eleventh Circuit recently upheld a district court decision finding that use of the plaintiff’s trademarks as metatags constitutes trademark infringement, where the search engine results contained a description of the website that included and highlighted plaintiff’s trademarks.\(^{45}\)

In contrast to prior decisions, the Eastern District of Wisconsin has recently ruled that without some type of direct competition, use of another’s trademark as a metatag will not create

---

\(^{41}\) *Ticketmaster Corp.*, 2000 WL 1887522.

\(^{42}\) *See Brookfield Commc'ns Inc. v. West Coast Entm't Corp.*, 174 F.3d 1036 (9th Cir. 1999); *Playboy Enters. v. Welles*, 279 F.3d 796, 801-04 (9th Cir. 2002) (holding use of plaintiff’s trademarks in defendant’s website metatags to be fair use where defendant had no practical way of describing herself without plaintiff’s trademarked terms; court noted that it might have found infringement if defendant had used plaintiff’s marks so repeatedly that her site appeared above plaintiff’s site in a search for the trademarked terms).

\(^{43}\) *Promatek Indus., Ltd. v. Equitrac Corp.*, 300 F.3d 808 (7th Cir. 2002).

\(^{44}\) *Id.* at 812.

a likelihood of confusion.\(^{46}\) This decision was based on the court’s finding that modern search engines do not use metatags to influence search results. The court further reasoned that even if search engines made use of metatags and consumers were diverted to the website, because consumers were able to purchase plaintiff’s genuine products, there was no competition and no likelihood of confusion.

Where use of metatags creates confusion as to the affiliation of a site, such use will generally be enjoined by the courts. With increased sophistication and use of the internet, it may be increasingly more difficult to prove likelihood of confusion.

G. **Keyword Advertising - Purchasing Competitor’s Trademarks for “Sponsored Advertising”**

Most search engines, including Google and Yahoo!, offer advertisers the ability to purchase search terms (keywords) that trigger links to the websites of paid advertisers on a search results page. The advertisements linked to keywords are typically displayed as 'sponsored links' on the search results page.

The law covering keywords varies between jurisdictions. First, there is a split as to whether the purchase of a competitor’s trademark as a search engine keyword constitutes “use in commerce” of that trademark. For example, a New York district court found that the act of purchasing another’s trademark as a keyword does not constitute trademark use as such use is not visible to the consuming public.\(^{47}\) In contrast, district courts in California, Minnesota and Virginia have found keyword purchases to constitute trademark use.\(^{48}\)

Second, when found to constitute trademark use, the law differs on whether keyword purchases are likely to cause confusion. A California Circuit Court held that the sale of the trademarks PLAYBOY and PLAYMATE to trigger paid advertising constituted use of the marks, and determined that triable issues of fact existed as regards to whether the competitors’ banner advertisements triggered by keywords were likely to cause confusion, but noted that if a banner advertisement either clearly identified its source or overtly compared Playboy’s products to those advertised in the ad, confusion would not likely occur.\(^{49}\)

Facing a similar issue, a Virginia court held that Government Employees Insurance Co (GEICO) had failed to establish a likelihood of confusion stemming merely from Google’s use of GEICO’s trademarks as keywords to trigger paid advertisements. However, it found that GEICO had established a likelihood of confusion “with regard to those sponsored links that use GEICO’s trademarks in their headings or text.”\(^{50}\) Likewise, a Pennsylvania court held that there


\(^{49}\) *Playboy Enter., Inc. v. Netscape Commc’ns Corp.*, 354 F.3d 1020 (9th Cir 2004).

was no likelihood of confusion from the purchase of a keyword through Google’s AdWords program because consumers had to affirmatively enter the website.\textsuperscript{51}

The recent decision of the Southern District of New York found that eBay’s practice of purchasing the keyword TIFFANY as part of sponsored link advertisements on Yahoo! and Google to advertise the availability of TIFFANY merchandise on the eBay website was protected by fair use, and avoided the question of whether purchasing the keyword constitutes “trademark use.”\textsuperscript{52} The Southern District distinguished the case from a decision in 1-800 Contacts, Inc. v. WhenU.com, Inc., where the Court found that use of a trademark to trigger key-

word advertising where the trademark was not viewable by the public does not constitute use under the Lanham Act,\textsuperscript{53} because eBay’s use resulted in a display of the TIFFANY mark that was viewable to the public.\textsuperscript{54} Even if the purchase constituted trademark use, however, the Court found that all elements of the nominative fair use test were met and thus such use was permissible.\textsuperscript{55}

At this point, the law is unsettled on whether the purchase of keyword advertising constitutes “trademark use,” and if it does, whether the facts support a finding of a likelihood of confusion.

H. Legal Remedies v. Practical Business Realities

The internet has opened many new opportunities for competitors and others to use or misuse a company’s trademarks and other intellectual property. In some cases, such use involves individuals who are upset about the trademark owner for some reason, including former employees, former franchisees, and customers. In other situations, individuals love the trademark owner and its products or services, and want to use the internet to promote the business. And finally, individuals or entities that have never had a relationship with the trademark or copyright owner may see opportunities to benefit from use of a well-known trademark. Each of those situations raise different legal issues.

The legal position of the trademark owner, while important, is often not the most relevant factor to consider. In some instances, a cost/benefit analysis will bring the trademark owner to decide to just leave the situation. Is there actual confusion, a strong likelihood of confusion, or will the use of the mark dilute the trademark owner’s rights? In a franchise system, the concern of the franchisees about the protection of the trademark rights is also a factor to consider how important it is to take action. In addition, if the trademark owner is too tolerant of misuses of its trademark, the trademark rights can be quickly eroded by third party use so the mark is weakened and in some cases becomes generic.


\textsuperscript{52} Tiffany (NJ) Inc. & Tiffany & Company v. eBay, Inc., 2008 WL 2755787 * 29-31 (S.D.N.Y. July 14, 2008).

\textsuperscript{53} 1-800 Contacts, Inc. v. WhenU.com, Inc., 414 F.3d 400 (2d Cir. 2005).

\textsuperscript{54} Tiffany (NJ) Inc., 2008 WL 2755787 at *31.

\textsuperscript{55} Id.
If a domain name in use incorporates the franchisor’s or franchisee’s trademark, and the facts show commercial use of the website (sale or promotion of commercial products or services) and bad faith, then a UDRP proceeding can offer a remedy of transfer of the domain name to the trademark owner at a reasonable cost. The filing fees for such a proceeding will run in the $1,000-2,000 range, depending on the number of panelists, and the time and legal costs for an investigation and preparing the complaint can generally be limited to a few thousand dollars. There is no discovery and oral arguments are not allowed. Furthermore, from the investigation and preparation of the complaint to the final decision, a UDRP proceeding can be completed in two or three months. Therefore, the UDRP procedure can offer a cost efficient and quick resolution of this limited type of problem.

On the other hand, if the problem raised is use of a trademark on a website with false statements, criticism of the trademark owner or other use of the trademark, a remedy is much more difficult and in some cases impossible. In those instances a careful analysis of the problem, the damage to the trademark owner, the type of action required to solve the problem, and the cost, must be carefully balanced.

For example, if a domain name has been registered incorporating a trademark, but it links to a webpage saying the website is “Under Construction,” there is no actual damage to the trademark owner at this time other than that it cannot register that domain name. In this case, a UDRP proceeding is probably not a good option because (i) it is difficult to show the domain name owner has no legitimate interest in the domain name, and (ii) if no demand has been made for money and the website is not being used for a competitive purpose, the trademark owner will have a difficult time proving the domain name was registered or used in bad faith. In this type of situation, the best option is most likely to continue to monitor the website to see if the status changes and facts are developed to establish the necessary elements for the UDRP proceeding.

Another example is a gripe site. While these can be annoying to the trademark owner, they generally get little traffic, and when they do, most people are put off by the negativity. If the trademark owner reacts and tries to respond, perhaps posting their own side of the story in a chat room or comment section on the site, this usually just reinforces the website owner’s actions by letting them know their comments are disturbing and getting the reaction they are aiming for from the trademark owner, franchisor or franchisee. In many cases, their actions and comments will then just escalate. In some cases, where false statements are posted that the target can refute by documentary evidence, action may be taken in a court to stop the false statements. However, as everyone knows, litigation is expensive. Furthermore, while the remedy may be achieved to stop the false statements, it cannot stop the “negative opinions” of the website owner and others posting to the site. The lawsuit might generate news stories on the dispute and unwanted publicity. In these cases, the small value of the benefit that might be achieved is generally not worth the expense. It may be better not to react and take a “wait and see” attitude. In many such cases, the website owner will eventually get tired of putting energy into this endeavor and will stop.

If a decision is made to take action, it is also particularly important to consider a back-up plan. For example, if you are considering sending a cease and desist letter, it is important to think about what your next step will be if the offending party ignores the letter or refuses to stop the infringing action. Is the offense egregious enough to justify the expense of litigation, and is there enough evidence to be successful? Or, if there is no response, would a follow up letter stating that you are not aware of any current confusion but will continue to monitor the situation and will take action if actual confusion is discovered in the future suffice? Protecting trademarks
against new media threats is very similar to other threats to trademark rights. The only
differences are that infringement comes in many different forms, is easier to do, and easier to
find, and often harder to stop.

III. COPYRIGHT ISSUES

A. Protection of Franchisor Copyrightable Materials

1. Subject Matter

The Copyright Act provides for copyright protection for “original works of authorship fixed
in any tangible medium of expression, now known or later developed, from which they can be
perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine
or device.”56 Such works include literary works; musical works, including any accompanying
words; dramatic works, including any accompanying music; pantomimes and choreographic
works; pictorial, graphic and sculptural works; motion pictures and other audiovisual works;
sound recordings; and architectural works.57 In a franchisor’s business, copyrighted works may
take various forms, including text and graphics in operations and other manuals, advertising and
marketing materials, packaging designs, original fabric designs used in the décor of the
franchised business, logos and signage designs, advertising jingles, architectural designs of
facilities, etc. A copyright is “created” when the work is “fixed in a copy or phonorecord for the
first time; where a work is prepared over a period of time, the portion of it that has been fixed at
any particular time constitutes the work as of that time, and where the work has been prepared
in different versions, each version constitutes a separate work.58 Such fixation may occur in a
blog, chatroom, website content, on a CD, DVD, and other new media. Registration of
copyrights is not required except to enforce those rights in litigation.

2. Ownership

Copyright vests initially in the author of a copyrighted work.59 The authors of a joint work
are co-owners of copyright in the work.60 However, when the author of the work is an employee
who created it within the scope of his or her employment, then it is considered to be a “work
made for hire” and the author is deemed to be the employer.61 In addition, a work specially
ordered or commissioned is a “work made for hire” if it is for use as a contribution to a collective
work, as part of a motion picture or other audiovisual work, as a translation, as a supplementary
work, as a compilation, as an instructional text, as a test, as answer material for a test, or as an
atlas, but only if the parties expressly agree in a written instrument signed by them that the work

57   Id.
60   17 U.S.C. § 201(a).
61   17 U.S.C. §§101 & 201(b).
shall be considered a work made for hire.” \(^{62}\) The employer or commissioning party for a work made for hire is considered the author and owns all of the rights comprised in the copyright unless there is an express written agreement between them that states otherwise. \(^{63}\)

Works created by franchisees for use in or by their franchise business or the franchise system are thus owned by the franchisee unless there is a specific provision in the franchise agreement transferring those rights. Likewise, works created by a consultant or independent contractor are owned by that consultant or independent contractor. Such works may include drafting a manual, creating a new logo or advertising text, creating a new menu design, writing and/or recording an advertising jingle; creating website content or a logo design and any other copyrightable materials, fixed in any type of media.

3. **Transfer of Ownership**

Under copyright law, any transfer of ownership of copyrights must be in writing signed by the copyright owner. \(^{64}\) Therefore, a franchisor must have a specific term in the franchise agreement or a written agreement with an independent contractor that specifically transfers the ownership rights to such works in order to own the works.

On the other hand, for a franchisee, an automatic assignment of rights to all copyrightable materials and other intellectual property created by it to the franchisor without compensation should be thoughtfully considered. If the franchisee (or its owners) is an innovative person, they may develop new materials and inventions that may greatly improve and be adopted by the franchise system as a whole. While restrictions against using a franchisor’s intellectual property and confidential proprietary information to develop independent intellectual property rights are necessary and reasonable, if a franchisee is creative or innovative and makes contributions to the franchise system as a whole, some compensation may be appropriate. Some franchisors adopt a reward system for compensating franchisees who create works of benefit to the whole system, even while requiring assignment of works created in this way.

B. **Special Internet Copyright Problems**

1. **Background Information on Linking**

As discussed earlier, a “link” is an electronic address embedded in a website that “points” to another part of the website or to a completely different website altogether. The act of linking (also known as hyperlinking) increases the utility of the internet as it allows for users to

\(^{62}\) A “supplementary work” is “a work prepared for publication as a secondary adjunct to a work by another author for the purpose of introducing, concluding, illustrating, explaining, revising, commenting upon, or assisting in the use of the other work, such as forewords, afterwords, pictorial illustrations, maps, charts, tables, editorial notes, musical arrangements, answer materials for tests, bibliographies, appendices, and indexes, and an “instructional text” is a “literary, pictorial, or graphic work prepared for publication and with the purpose of use in systematic instructional activities.” 17 U.S.C. §101.

\(^{63}\) 17 U.S.C. §201(b).

navigate more efficiently through the World Wide Web and find their target page/content. Linking is desirable because of the increased visibility that it gives both the website that contains the link and the website to which the link is directing the user; however, legal issues can arise when a website does not want another website to carry its link. The use of unlawful links can result in violations related to endorsements, compliance, deceptive practices, copyright and patent infringement (direct and indirect), reputation and trademark, and misappropriation relating to the access right to and data retrieved from the linked site. Two of the most controversial legal issues with respect to linking are the acts of “deep linking” and “framing.”

2. Deep Linking

As discussed earlier, deep linking is the practice of linking one website directly to an interior page, a page other than the home or main page, of the linked-to website. Similar to a basic link, a deep link has the benefit of allowing the user to be more efficient by letting the user proceed directly to the desired page/content without additional navigation. However, by helping the user proceed directly to the desired content page in the linked-to website, the website providing the link allows the user to bypass other pages that the linked-to site may want the user to see. Such intervening pages may include pages displaying the linked-to site’s advertisements or containing important information about the linked-to site (e.g., its terms of use or privacy policy). Furthermore, in certain situations as described below, deep linking to content at the linked-to website may result in copyright violations.

The practice of linking has received varied treatment in the courts. For example, in Ticketmaster Corp. v. Tickets.com, a U.S. federal district court considered whether deep linking violated the Copyright Act. In Ticketmaster, defendant Tickets.com’s website allegedly contained deep links to event descriptions on Ticketmaster’s website, bypassing the home page and other pages, and through use of “spiders,” systematically copied and extracted event descriptions reformatted on defendant’s site. Plaintiff Ticketmaster alleged that Tickets.com’s deep links to its website were diluting its value. In a March 27, 2000 minute order, the district court noted that “hyperlinking does not itself involve a violation of the Copyright Act (whatever it might do for other claims) since no copying is involved” and that “deep linking by itself (i.e., without confusion of source) does not necessarily involve unfair competition.” On the other hand, the court noted that the practice could involve a breach of contract, as a violation of the “terms of use” at Ticketmaster’s site.

An aggressive variation of linking was at issue in eBay v. Bidder’s Edge, Inc. There a federal district court found that eBay was likely to prevail on the merits of its trespass claim against Bidder’s Edge due to potential irreparable harm to eBay. eBay sued Bidder’s Edge for infringement of eBay’s intellectual property by way of “crawling” on eBay’s website in

---

66 See id. at § 9.03.
67 Id. at § 9.05.
contravention of eBay’s posted terms of use policy. Bidder’s Edge then used the data collected about eBay items on Bidder’s Edge’s own site. Following the district court’s ruling that such conduct was likely to render Bidder’s Edge liable for trespass, the parties settled the lawsuit by agreeing to a confidential payment by Bidder’s Edge and its promise to cease crawling eBay’s site for information.

a. Recent Developments in the U.S.

In 2007, the court in *SFX Motor Sports, Inc. v. Davis* held that it was illegal for the defendant to provide a deep link to the plaintiff’s copyrightable material on the defendant’s website. In SFX the plaintiff promoted, produced, and provided live audio webcasts of motorcycle races for visitors to its website. The defendant provided links that allowed users visiting the defendant’s website to listen to the audio webcasts provided by the plaintiff. The court determined the audio webcasts were copyrightable material belonging to the plaintiff. Furthermore, the court stated that:

[The unauthorized link to the live webcasts that Davis provides on his website qualifies as a copied display or performance of SFX’s copyrightable material. The court also determines that the link Davis provides on his website is not a ‘fair use’ of copyright material as Davis asserts through his Answer.]

The court granted summary judgment on the plaintiff’s copyright infringement claim based on the defendant’s unauthorized link.

b. Recent Developments Abroad

As in the United States, the treatment of deep linking varies around the world with different countries handing down different judgments based on similar facts. For example, in *The Shetland Times Co., Ltd. v. Wills*, the plaintiff Shetland Times maintained on its website articles that had appeared in the print version of its newspaper, accessible by clicking on a headline on the “front page” of the website. The defendant Shetland News maintained a website containing the Times’ headlines verbatim which, when clicked, linked directly to the full text of the Times’ articles, bypassing the Times’ front page (and the advertisers who appeared on that front page). In the only order issued in the case before it was settled out of court, the

---

70 eBay’s current User Agreement states that the site “contains robot exclusion headers. Much of the information on the Sites is updated on a real-time basis and is proprietary or is licensed to eBay by our users or third parties. You agree that you will not use any robot, spider, scraper or other automated means to access the Sites for any purpose without our express written permission.” http://pages.ebay.com/help/policies/user-agreement.html (visited May 30, 2008).


73 *Id.* at 12.

Court of Sessions ruled for the plaintiffs by enjoining the defendants from deep linking. The court determined that the headlines were copyrightable literary works, rejecting the defendant's argument that the headlines were not the product of sufficient skill or effort to be copyrightable, and that copying of the headline constituted copyright infringement, at least in some instances.

A directly contrary result was rendered by a Dutch court. PCM, the publisher of several Dutch daily national newspapers, sought to prevent the online publication of headlines by Kranten.com. Each headline linked to the text of the related article on the newspapers' websites, bypassing the newspapers' home page. The Rotterdam District Court rejected PCM's copyright claims, noting that the website could rely on the "droit de citation" of the Berne Convention, and observed that PCM had neither implemented technical measures to prevent linking nor sought to mitigate its home page advertising losses by placing ads adjacent to articles on the PCM site.

In the Danish case of Danish Newspaper Publishers' Association v. Newsbooster.com, decided in 2002, the court found that deep links provided by the defendant on its website, which led to newspaper articles at the plaintiff's website, violated the Copyright Act of that country. The defendant would receive fees from members and in exchange those members could, through the use of key-word searches, search for newspaper articles and receive headlines and links that would take the user directly to the article, thereby bypassing the plaintiff's homepage.

However, in, Verlagsgruppe Holtzbrinck v. Paperboy, a case from Germany based on facts similar to those in Newsbooster.com, the court held that the defendant did not commit any violations by deep linking to the plaintiff's website. The defendant provided users the ability to search and bring up links to relevant articles (located on other websites) which allowed the user to access the articles directly. The plaintiff argued that the defendant violated copyright and unfair competition laws by allowing users direct access to articles that the plaintiff published online. The court held that linking to the plaintiff's articles was not a violation of copyright and unfair competition laws when the plaintiff did not take any measures to protect the articles on the internet. According to the court, the links simply made finding the articles easier for the public.

In India in 2005, the high court in Naukri v. Bixee issued a restraining order to prevent Bixee from deep linking to content on Naukri's website. Bixee used web crawlers to collect job posting information from Naukri's website which it then provided to users who performed job searches on Bixee's website. Although the links led to the job posting on Naukri's website, and thus benefited Naukri, Bixee benefited from the increased traffic on its website and, moreover, Bixee encouraged users to upload listings to Bixee's website as opposed to Naukri's website.

---

75 President District Court of Rotterdam, 22 August 2000, Mediaforum 2000, p. 344 (Kranten.com).


The restraining order was based on the potential for decreased advertising revenue because of decreased traffic on Naukri’s website.79

c. Current State of the Law; Link Licenses

The foregoing discussion illustrates that U.S. and foreign law regarding deep linking remains unsettled as it continues to be fact dependent, with no clearly established standards by which deep linking issues are judged. In comparing Ticketmaster with SFX Motor Sports, the determination of legality of the deep linking in those cases appears to have had more to do with what was being deep linked (i.e. copyrightable material vs. material protected by the terms of use of the website) rather than the act of deep linking itself. However, courts have not provided an exhaustive list of what material can or cannot be the subject of a deep link without violating copyright law, breaching a contract, constituting a trespass or otherwise being legally proscribed. Therefore, the safest alternative is for a person/company to deep link to another website only after receiving permission to add the link. Such permission may come in the form of a link agreement or license, a practice that is becoming more common between commercial websites.80 On the other hand, a person/company seeking to protect against deep links should carefully review website terms of use, consider the use of technical measures to thwart deep linking, reflect on whether deep linking could be acceptable under some circumstances and, if so, build those circumstances into a link agreement. Such agreements frequently address such matters as the link location and context, link duration, modifications, restrictions on framing, restrictions on the use of trademarks, names, and logos, compensation and disclaimers.81

3. Framing

Framing (also known as in-line linking) is “the process of allowing a user to view the content of one website (the linked-to site) while it is framed by information from the linking site.”82 Framing therefore in effect pulls text, images or other materials from the linked-to site into the page then being viewed by the user on the linked-from site, typically with a frame or border surrounding the framed material.83 Framing may result in copyright and trademark issues because the framing of another party’s content may constitute a derivative work or may create “the impression that the owner of the linked-to content endorses or voluntarily chooses to associate with the framer.”84


81 Id.

82 NIMMER & TOWLE, supra note 65 § 9.04.


84 NIMMER & TOWLE, supra note 65 § 9.04[1].

24
The first reported case to address the technique known as framing was *Washington Post Co. v. TotalNews, Inc.* In *TotalNews*, defendant TotalNews provided links from its website to more than 1200 news organizations, identified by name. Upon clicking one of the names, the user viewed the remote site, displayed within the frame of TotalNews’ website, thereby permitting messages from TotalNews’ advertisers to remain on the screen. The Washington Post and a number of other news organizations sued TotalNews for copyright infringement and related causes of action. In their complaint, the plaintiffs accused TotalNews of “pirating copyrighted material,” republishing it and profiting from the work of others. The case settled shortly after being filed. As part of the settlement agreement, TotalNews agreed to discontinue framing the seven websites that were at issue in the suit. Thereafter, TotalNews would provide a direct link to the websites without TotalNews, or its advertisers, tagging along to decorate the site.

On the other hand, the United States District Court for the Central District of California opted not to find copyright infringement in *FutureDontics Inc. v. Applied Anagramics Inc.* There the plaintiff, FutureDontics, operated a dental referral business utilizing the anagramatic phone number “1-800-DENTIST,” while the defendant, Applied Anagramics, owned the registered service mark “1-800-DENTIST.” Later, the plaintiff decided to establish an internet website to promote its dental referral service. Its site consisted of a number of web pages containing graphics and text, which were copyrightable material. The plaintiff registered its copyrighted web pages. Thereafter, defendant Applied Anagramics developed its own website. Its website established a link which reproduced FutureDontics’ web pages within a frame that includes its logo and information about Applied Anagramics. The court ruled for the defendant by denying plaintiff’s preliminary injunction motion because the plaintiff had failed to demonstrate that framing of material from its website created a derivative work in violation of its copyrights.

Subsequent to the copyright action, both FutureDontics and Applied Anagramics were back in court on trademark grounds. In this second round of the parties’ dispute, the district court issued a preliminary injunction against FutureDontics, prohibiting promotion of any product “in connection with” the mark Applied Anagramics. The Ninth Circuit Court of Appeals upheld the injunction, noting the threat of irreparable harm to Applied Anagramics and that FutureDontics should be aware it cannot use the plaintiff’s mark to promote any dental products without Applied Anagramics’ prior approval.

Similarly, in *Kelly v. Arriba Soft Corporation*, the court held that the defendant, Arriba Soft, did not violate any copyright laws by allowing users to view thumbnails of pictures that belonged to the plaintiff and were posted on the plaintiff’s website. The court stated that the

---

85 97 Civ. 1190 (S.D.N.Y. 1997).
86 45 U.S.P.Q.2d 2005 (C.D. Cal. 1998), aff’d, 152 F.3d 925 (9th Cir. 1998).
87 *FutureDontics, Inc. v. Applied Anagamrics, Inc.*, 201 F.3d 444 (9th Cir. 1999).
88 *Kelly v. Arriba Soft Corporation*, 336 F.3d 811 (9th Cir. 2003).
89 Thumbnails are “reduced-size versions of pictures, used to make it easier to scan and recognize them, serving the same role for images as a normal text index does for words.” *Thumbnail*, WIKIPEDIA, http://en.wikipedia.org/wiki/Thumbnail.
defendant, a visual search engine, was allowed to post thumbnail pictures because the use fit under the “fair use” exception to copyright infringement. However, in a part of the opinion that was reversed on procedural grounds, the court stated that allowing users to view the full size image through in-lining (framing) would not constitute “fair use.” Although this part of the opinion was reversed on procedural grounds, it seemed to set an important distinction between thumbnail and full size images with regard to framing.

However, no such distinction was drawn in *Perfect 10 v. Amazon.com, Inc.*, where the court held that the defendant, Google Inc., was not liable for copyright infringement for allowing users to search for and view thumbnail and full size pictures that belonged to the plaintiff. The defendant allowed users to search for and view content (text and pictures) located on other websites. In the case of pictures/photos which are retrieved from the search, the user is able to view the images in thumbnail format while still on the defendant’s website and has the option of clicking on the thumbnail for a larger view of the picture, which view is still framed within the defendant’s website. Through this process users were able to search for photographs (copyrighted images of nude models) originally located on the plaintiff’s website, which were published without authorization by third party websites, and to view them on the defendant’s website. *Citing Kelly v. Arriba Soft Corporation,* the court held that allowing users to view the plaintiff’s photos in thumbnail format on the defendant’s website was protected by the “fair use” exception. However, the court went further in stating that the defendant was also not liable for framing full sized photos in addition to the thumbnails. The court’s holding turned on a determination of where the framed photos were actually located. The court stated that:

> Google does not, however, display a copy of full-size infringing photographic images for purposes of the Copyright Act when Google frames in-line linked images that appear on a user’s computer screen. Because Google’s computers do not store the photographic images, Google does not have a copy of the images for purposes of the Copyright Act. In other words, Google does not have any “material objects ... in which a work is fixed ... and from which the work can be perceived, reproduced, or otherwise

---

90 “Notwithstanding the provisions of sections 106 and 106A [17 U.S.C. §§ 106 and 106A], the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include—(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.” 17 U.S.C. § 107 (1997).

91 The Ninth Circuit reversed on procedural grounds as to the issue of full size images. The court stated that, “With limited exceptions that do not apply here, a district court may not grant summary judgment on a claim when the party has not requested it. The parties did not move for summary judgment as to copyright infringement of the full-size images. Further, Arriba had no opportunity to contest the prima facie case for infringement as to the full-size images.” *Kelly* at 822.

92 *Perfect 10 v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007).

93 *Id.* at 1156.
communicated” and thus cannot communicate a copy. 17 U.S.C. § 101.94

C. Digital Millennium Copyright Act

As a franchisor develops a greater presence on the internet, the Digital Millennium Copyright Act95 (“DMCA”) becomes more important. The DMCA implements the World Intellectual Property Copyright Treaty and Performances and Phonograms Treaty (“WIPO treaties”) and explicitly provides limitations on liability for copyright infringement to internet service providers (“ISPs”). An increasing number of franchisors provide their franchisees and others with various internet enabled means of communication, which could permit the franchisors to come within the definition of an ISP. Accordingly, franchisors that provide such resources may be able to assert that the protections afforded by the DMCA to a traditional ISP are available to franchisors as well. The WIPO treaties require ratifying countries to update their laws against piracy of copyrighted materials in accordance with the treaties. Each country also must extend its laws “to the electronic commerce marketplace epitomized by the internet.”

The DMCA defines an ISP 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 as sent or received.” Section 512(a), as amended by the DMCA, states that an ISP is not liable for copyright infringement “by reason of the provider’s transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the... (ISP), or by reason of the intermediate and transient storage of that material” in performing this service. This limitation is conditioned on: (1) the transmission being at the request of a person or entity other than the ISP; (2) selection of the material transmitted by a person or entity other than the ISP; (3) selection of the recipient of the material transmitted by a person or entity other than the ISP; (4) the ISP not maintaining a copy accessible to anyone other than the requesting party; (5) the ISP not maintaining a copy longer than is reasonably required for the transmitting, routing, or provision of connections; and (6) the ISP transmitting material without modification. In addition, to be protected by the limitations on liability provided in the DMCA the ISP must have designated an agent to receive notifications of claimed infringement.

Section 512(a) insulates ISPs from claims of contributory copyright infringement resulting from aiding users in accessing material on the Web. Section 512(b) limits ISPs’ liability regarding system caching, which involves storing a copy of material in the system as a result of a request. Specifically, Section 512(b)(1) provides that an ISP is not liable “for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider.” This language protects ISPs from claims of direct infringement for storing copies, or equivalent reproductions, of the work on the ISP systems at a user’s request. This protection is conditioned on: (1) the material having been made available on the Web by someone other than the ISP; (2) the material being transmitted at the direction of someone other than the ISP; and (3) the storage occurring as part of an automatic process for the purpose of making it available to the users. Furthermore, the ISP must not modify the material, must comply with any requirements imposed by the person making the material available on the Web, must ensure that any access requirements, such as

94 Id. at 1160-1161.
passwords for users, are met, and must disable access expeditiously if notified that the material was made available without authorization of the copyright holder.

In regards to linking, DMCA section 512(d) serves to protect ISPs from copyright liability “by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link.” 96 The liability protection will apply if the ISP:

(1)(A) does not have actual knowledge that the material or activity is infringing; (1)(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (1)(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material; (2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and (3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link. 97

Although the DMCA’s safe harbor is intended to strike a balance between the rights of copyright owners and protecting ISPs from liability when users illegally use the ISP’s technology, some critics believe the measures provided in the DMCA’s safe harbor are ineffective in protecting copyrightable material. In a complaint filed by Viacom International Inc. against YouTube, LLC, although the DMCA’s safe harbor was not specifically mentioned, Viacom claimed that “take down” requirements are ineffective to address illegally uploaded copyrighted content because of the ease with which duplicate copies of the infringing material may be uploaded. In part, the complaint stated that:

Because YouTube directly profits from the availability of popular infringing works on its site, it has decided to shift the burden entirely onto copyright owners to monitor the YouTube site on a daily or hourly basis to detect infringing videos and send notices to YouTube demanding that it “take down” the infringing works. In the meantime, YouTube profits handsomely from the presence of the infringing works on its site. And even after it receives a notice from a copyright owner, in many instances the very

97 Id.
same infringing video remains on YouTube because it was uploaded by at least one other user, or appears on YouTube again within hours of its removal. YouTube has deliberately chosen this approach because it allows YouTube to profit from infringement while leaving copyright owners insufficient means to prevent it.98

In posting to a website materials furnished by third parties, and in providing internet, extranet or similar services to franchisees, franchisors should consider how best to avail themselves of the statutory protection provided by the DMCA.

IV. PROTECTION OF FRANCHISOR CONFIDENTIAL INFORMATION FROM DISCLOSURE

A. Trade Secret Protection Generally

Trade secrets are largely a creature of state law.99 Most states have adopted the Uniform Trade Secrets Act, which provides some uniformity in defining trade secrets. A trade secret “derives independent economic value, actual or potential, from not being generally known to” others and “is the subject of efforts that are reasonable under the circumstances to maintain its secret.”100

Trade secrets have always been carefully protected, but the internet is making it more difficult to protect companies' confidential and highly sensitive information. In the past, a company could brand its name on its product or secure machinery to the floor in order to protect its most valuable assets. Now, valuable assets often consist of intellectual property, such as trade secrets. Besides the inability in many cases of physically securing a trade secret in order to protect it, the advent of the internet has compounded the problem: the internet travels at the speed of light and can disseminate information across the world in an instant.

Although the destruction of a trade secret may be borne out of a malicious act (such as by a disgruntled former employee who deliberately posts company secrets onto his or her personal blog or third party websites), the internet creates opportunities for trade secrets and their flexible softcopies to circulate unintentionally:

- A company may post a trade secret online deliberately, without fully understanding the consequences of its post. For example, a company’s website may contain in-depth information regarding strategic visions for the future of the business or plans for new products.

---


99 Trade secrets are also protected by the federal Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839, which defines trade secrets in a manner consistent with the Uniform Trade Secrets Act discussed in this Section of the paper. The federal Act, among other things, prohibits the misappropriation of trade secrets related to or included in a product that is produced for or placed in interstate or foreign commerce with the knowledge or intent that the misappropriation will injure the owner of the trade secret. Id. at § 1832.

100 Uniform Trade Secrets Act §1 (amended 1985).
• A company may also carelessly post secrets onto its website, such as posting
details about products currently under development.

• Secrets may also leak onto the internet through unexpected channels. For
  example, Jerome Stevens Pharmaceuticals (JSP) is a drug company that
  sought FDA approval for a new thyroid treatment drug. The company
  provided the FDA with various information about the treatment drug, including
  trade secrets, as required by FDA regulations regarding new drug approval;
  the FDA then posted these trade secrets on its website by accident. 101

  Adding insult to injury, remedies available for trade secrets revealed online are not as
  stringent as for those revealed offline. Take, for example, a comparison of the consequences in
  the following cases: 102

  • Jeffrey Wigand, a Brown & Williamson executive, engaged in an interview
    with CBS in which he revealed that the tobacco company knew nicotine was
    addictive. The tobacco company sued Wigand for his disclosure of
    confidential information and, ultimately, Wigand lost his marriage, his family
    and his career as a result of the ordeal.

  • Philip Kaplan, on the other hand, published appalling and chauvinistic instant
    messenger conversation logs, written by the CEO of eFront.com, on Kaplan’s
    website. When Kaplan received warning letters from eFront.com, urging
    Kaplan to remove the logs from his site, he posted the legal e-mail onto his
    site rather than de-posting the eFront material. Kaplan mocked the warning
    letter, describing it as “hilarious.”

B. Inconsistency Between Internet Publication and Trade Secret Status

Why is there such a discrepancy between how trade secret law is treated offline and
online? Since Kaplan in the example above was the second webmaster to post the information
on the internet, he probably fell into the “public knowledge” exception to trade secret law. This
important exception provides that if something is no longer a secret, but rather has become
public, it is no longer legally protected. Therefore, with the advent of the internet, showing that a
trade secret has become public knowledge can be very easy. To receive protection as a trade
secret, information must be kept secret because “matters of public knowledge or of general
knowledge in an industry cannot be appropriated by one as his secret.” 103 Thus, the internet,
with its broad reach and widespread use, has added a twist to conventional trade secret
protection; once a trade secret is posted on the internet, the information is no longer a secret.
While the original poster may be held liable for misappropriation, subsequent posters cannot be
liable for misappropriation of the now “generally known” information.

101 Jerome Stevens Pharmaceuticals v. FDA, 402 F.3d 1249 (DC Cir. 2005)
102 Julie Hilden, Trade Secrets: Not So Secret On The Internet, FINDLAW FOR LEGAL PROFESSIONALS, May 14,
103 RESTATEMENT (FIRST) OF TORTS, Section 757, comment b (1939).
The cases below demonstrate the trade secret internet disclosure problem; they reflect the courts’ attempts to reconcile the inconsistency between internet publication and information’s trade secret status:

- In *Ford Motor Co. v. Lane*\(^{104}\), the defendant (who was not an employee of Ford) posted confidential documents and trade secrets on his website, disclosing photographs of unreleased Ford products, blueprints and other confidential information. The court denied plaintiff Ford’s motion for a preliminary injunction, holding that such an injunction would violate the First Amendment.

- In *Religious Tech. Center v. Lerma*,\(^{105}\) church documents were not considered trade secrets under Virginia law because the documents had been introduced into the public domain through internet publication. The court was not persuaded by evidence that the plaintiff Church of Scientology had taken extraordinary measures to keep the documents a secret.

- In *Religious Tech. Center v. Netcom On-Line Communications Servs., Inc.*,\(^{106}\) the plaintiff Church of Scientology sought an injunction against a disgruntled former member who posted Church writings on the internet. The court examined the Church’s claim that the writings were trade secrets and held that there would be a loss of secrecy and a loss of trade secret rights if unrelated third parties reposted the writings. The court noted that since the writings were posted on the internet, they were available to the general public and there was no trade secret right available to support an injunction.

C. **Potential for Restoring Trade Secret Status for Matter Posted on Internet**

Initially, as evidenced by the cases above, courts held that the unauthorized disclosure of trade secrets on the internet destroyed their secrecy and there was no potential for restoration once the posting had been made.\(^{107}\) *The Religious Tech Center v. Lerma* court noted that the information had been made publicly available (and, thus, destroyed trade secret protection) because it had been posted for ten days during which the information was potentially available to millions of internet users.\(^{108}\)

Subsequent courts, however, have recognized that unauthorized disclosure does not necessarily destroy information’s trade secret status if it is removed promptly and has not been


widely broadcasted. In reference to his decision in Netcom (that a posting on the internet necessarily destroys a secret), Judge Whyte wrote:

The question of when a posting causes the loss of trade secret status requires a review of the circumstances surrounding the posting and consideration of the interests of the trade secret owner, the policies favoring competition, and the interests, including First Amendment rights, of innocent third parties who acquire information off the internet ... The relevant inquiry is whether the documents for which trade secret protection is sought are “generally known” to the relevant people... 

Enforcement issues remain, but courts have recently held that if the leaked trade secret’s owner moves quickly and can show that it took reasonable measures to protect its secrets, the owner may be able to prevent further online dissemination and subsequent destruction of the secret. The following cases exemplify courts’ progression to this more sophisticated evaluation as to whether an unauthorized posting destroys secrecy:

- In DVD Copy Control Ass’n v. Bunner, the plaintiff controlled rights to an encryption program that restricted the playback of encrypted DVDs to DVD players and computers authorized to decode the content. The plaintiff alleged that a Norwegian teen reverse engineered the program and created a program that allowed encrypted DVDs to be played on any DVD player or computer (regardless of authorization). The defendant found and posted that program onto the internet for public use. The court noted that widespread publication of a trade secret over the internet destroys trade secret status, but added that information retains its value if the internet publication is sufficiently obscure so that it does not become generally known to those who would consider it valuable. The court reasoned that a preliminary showing of likelihood of success of an injunction is an adequate argument for an injunction to remove trade secrets from the internet. However, in this case, the court ultimately held that the trade secret had been widely broadcasted and therefore an injunction would not prevent any further harm from occurring to the plaintiff.

- In United States v. Genovese, the defendant was charged with selling Microsoft’s source code on the internet, violating the Economic Espionage Act of 1996 (“EEA”). The court

---

110 DVD Copy Control Ass’n v. Bunner, 75 P.3d 1, 14 (Cal. 2003).
held that, under the EEA, a trade secret does not lose its protection when “temporarily, accidentally, or illicitly released to the public, provided it does not become ‘generally known.’” The court held that since the defendant had sold the source code, versus posting it online, it still retained some value and was not generally known.

Taking lessons from the previous cases, trade secret owners now have the potential to restore trade secret status to information leaked onto the internet. Trade secret owners should work to detect improper posts early on, such as by running occasional searches to see whether sensitive information about their company has been posted. If such information is found, posters should be immediately notified that their posting is unauthorized and urged to take their posting down. Since all is not necessarily lost by an unauthorized posting on the internet (as noted in both Bunner and Genovese), trade secret owners should make efforts to collect evidence that the secret has in fact not been widely viewed.

D. Potential Data Security and Sarbanes-Oxley §404 Concerns

One category of trade secrets that is receiving increasing attention as well as legal protection is the electronic data held by businesses, which may contain confidential information of great importance but may also be accessible via the internet or other electronic media. Weaknesses or outright flaws in corporate computer systems can be exploited by sufficiently sophisticated hackers seeking confidential information, whether motivated by animosity, curiosity, ego or financial benefit. Although it is beyond the scope of this paper to analyze the rapid and significant developments in this area, suffice it to say that concerns about the security of such data have led to a number of federal and state data security laws imposing duties on the holders of such data.

One of the more well known laws is the Sarbanes-Oxley Act of 2002 (“SOX”), which was adopted in response to the wave of massive corporate fraud scandals such as Enron, Worldcom and Tyco. SOX amends federal securities laws by, among other things, regulating financial disclosures by publicly-held corporations. The goal was to increase the flow of timely and accurate information to investors and consumers, thereby rekindling confidence in the marketplace. One of the aspects of the law that has not received much attention is the SOX obligation for company management to assess and report upon the corporation’s data security policy for financial information.


Section 404 of SOX obliquely requires that publicly-held corporations prepare annual reports containing “internal control reports” that (1) state the “responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting” and (2) contain an assessment of the effectiveness of the company’s “internal control structure” and financial reporting procedures. In addition, Section 302 requires that corporate management evaluate the internal controls within 90 days prior to the report and, for use in the report, present their conclusions about the effectiveness of the controls. Initially, the meaning and scope of the required “internal control structure” were unclear. Under rules subsequently implemented by the Securities and Exchange Commission, however, the importance of data security became apparent. The rules expressly define internal control over financial reporting as a process implemented by company management to provide, among other things, “reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the [company’s] assets that could have a material effect on the financial statements.”

Thus, under the banner of ensuring the integrity of corporate financial data, SOX requires corporate management to adopt a data security policy for material corporate assets and to report the policy’s effectiveness in annual public filings. While it remains somewhat unclear what constitutes “adequate” data security procedures in any given case, it is obviously best practice, in general, to err on the side of data protection in designing security controls. This is all the more obvious given the law’s goal of casting a public spotlight on any data policy shortcomings.

Based on the foregoing, franchisors that are publicly-traded corporations subject to SOX should, at the very least, design and implement security controls appropriate to the nature of the data used and stored, ensure awareness of such controls throughout the corporation, regularly audit such security controls, modify the controls as necessary and document the effectiveness of the controls. Requisite security controls include technological elements such as passwords, network firewalls and tracking systems to limit access and record data manipulation, but also physical elements such as using secure locations and placing locks or other anti-theft devices on computer equipment. Furthermore, it is critical that franchisors subject to SOX truthfully report the effectiveness of their policies in their public filings. Misrepresenting or obscuring the facts would expose a company and its management to harsh criminal penalties. Because SOX governs only companies that are publicly-held, many franchisors are not be bound by it. However, not only is data security a desirable end in its own right, other laws, including the rapidly proliferating state data security laws, may reach companies that SOX does not.

---


117 *Id.* § 7241(a)(4)(C), (D).


119 It is a crime to certify a report with knowledge that it does not comport with the requirements of the law; penalties include imprisonment for up to 10 years and/or a fine of up to $1 million. These penalties may be increased to 20 years and $5 million when the certifying officer “willfully” certifies an inaccurate report. 18 U.S.C. § 1350(c).
V. Potential Liabilities: Franchisor and Third Parties

A. Trade Libel Laws Generally

The trade libel tort, also known as product disparagement, injurious falsehood or slander of goods, occurs when there is a publication of a false statement of fact disparaging a product, which in turn causes pecuniary loss to the product’s owner. Additionally, there is a requisite state of mind requirement. Although closely related to a defamation cause of action, the major difference is that a defamation suit is designed to protect the reputation of the individual, while a disparagement action seeks to recover pecuniary damages suffered as a result of the trade libel. Another difference is that injunctive relief can often be had for product disparagement actions to stop economic losses, while in personal defamation actions that type of relief is not often available. However, a libelous statement may occasionally both disparage a plaintiff's goods as well as personally defame the plaintiff.

Because most states use the legal structure of the Restatement (Second) of Torts, the requirements for the tort are similar among the states. First, there must be a publication of the matter. Second, the publication must be false and disparaging of the plaintiff's product. Third, the defendant must have made the statements with knowledge of their falsity, or at a minimum, with reckless disregard to their truth. Fourth, the defendant must have published these statements with a desire to harm the product and the plaintiff’s interest, or to have known that the harm would have inevitably occurred. Last, the plaintiff must show that there were actual pecuniary damages as a result of the alleged product disparagement.

In order to establish a cause of action, the false statements that were made must be factual assertions and not mere opinions of the author. Often, the line between fact and opinion is a fine one. For example, in Brignoli v. Balch Hardy & Scheinman, Inc. the court held that “[t]he statement that defendant's programs were ‘better’ than those of plaintiff . . . fails to support a claim of disparagement.” The court explained that such claims are mere “puffing” and do not warrant a trade libel lawsuit. Although the comparison could have had falsity contained in it, the general nature and context of the statement made it not actionable. Additionally if the claims are subjective ones, and cannot be proven true or false, there lies (no pun intended) no cause of action. In order to recover against an allegedly false advertisement, the plaintiff

121 Id. at 574.
124 Id.
126 Id.
must prove that the “promotions were literally false.”\textsuperscript{128} Although puffery covers exaggerations and overstatements about a particular product or service if expressed in vague or broad terms, the statements are actionable if they are “both specific and measurable by comparative research.”\textsuperscript{129} Additionally, in \textit{Milkovich v. Lorain Journal Co.} the Supreme Court held that an opinion that contained provably false facts was subject to a product disparagement suit.\textsuperscript{130} The Milkovich decision made clear that only one who is expressing an opinion that is subjective, and not open to proof of truth or falsity, could be immune from defamation lawsuits.\textsuperscript{131}

In order to recover in a trade libel suit, the plaintiff must show that he suffered special damages. This is different from defamation suits where the requirement is a showing of a general loss of reputation in the community. For the plaintiff to recover for losses as a result of product disparagement,\textsuperscript{132} courts often require a showing of damages that is highly particularized. This can involve showing what specific customers have refused to deal with the plaintiff and what particular transactions were involved. It is unclear whether courts will allow a general decline in sales as sufficient proof that the product disparagement had an effect on the plaintiff’s level of business. Of the courts that do accept such theories, many require additional findings.

Without proving all elements of the trade libel tort, the plaintiff in the case cannot recover. Thus, the defendant’s ability to show that the statements were not in fact published would exonerate him of the charge. Important to note is that the publication of the statement has to be to someone other than the plaintiff himself.\textsuperscript{133} As discussed above, there has to be a false statement of fact. If the defendant can show that the statements were opinions rather than facts, the plaintiff is barred from recovery. Additionally, a plaintiff’s inability to show falsity exonerates the defendant.\textsuperscript{134} Although there are slight variations from jurisdiction to jurisdiction, the plaintiff is also required to show a level of malice involved in the defendant’s publication of the libelous material. Some courts accept a showing that the statements were made knowingly or recklessly as sufficient to demonstrate this element.\textsuperscript{135} The last defense available is that the plaintiff has not met his burden in showing that there were special damages that are calculable, apparent and a direct result of the published libelous statements.\textsuperscript{136}

\textsuperscript{128} \textit{Id.}
\textsuperscript{129} \textit{Castrol, Inc. v. Pennzoil Co.}, 987 F.2d 939, 946 (3d Cir. 1993).
\textsuperscript{130} 497 U.S. 1, 19 (1990).
\textsuperscript{131} \textit{Id.} at 12.
\textsuperscript{132} ROBERT D. SACK, SACK ON DEFAMATION § 13.1.4.6 (3rd ed. 2007).
\textsuperscript{133} \textit{Id.} at §13.1.4.1.
\textsuperscript{134} \textit{Brinson v. Carter}, 113 S.E. 820, 821 (Ga. Ct. App. 1922).
\textsuperscript{136} \textit{Hurlbut v. Gulf Atlantic Life Ins. Co.}, 749 S.W.2d 762, 768 (Tex. 1987).
Absolute privileges apply to trade libel claims in the same way that they apply to defamation actions. When the privilege is absolute, “[i]t is not conditioned upon the honest and reasonable belief that the defamatory matter is true or upon the absence of ill will on the part of the actor.” However, traditionally absolute privilege attaches mainly to statements made in connection with a legislative or judicial proceeding. Qualified privileges are also available to the defendant in trade libel lawsuits.137 Invoking qualified privilege in a trade libel claim can raise problems because a plaintiff must show malice on the part of the defendant to overcome the qualified privilege.138 However, malice is an element that the plaintiff must establish to have a trade libel cause of action in most jurisdictions.

For trade libel suits there are two additional privileges that a defendant can invoke. First, there is a “privilege of a rival claimant to disparage another’s title,” and secondly, there is a “privilege of a competitor to make an unduly favorable comparison of his or her own product with that of another.”139 The first privilege allows a rival claimant to disparage another’s interest in land as long as the assertion is in good faith, even if factually false. The second privilege allows a competitor to assert his own product’s superiority, even without a good faith belief that it in fact is superior, because of “the common sense knowledge that purchasers will take such comparisons cum grano salis.”140

B. State Anti-SLAPP Statutes

A SLAPP (strategic lawsuit against public participation) is the name given to actions filed against a person or persons seeking to discourage their exercise of the right to free speech and the right to petition the government. In order to counteract and discourage SLAPP lawsuits, which are filed primarily by land developers and corporations, twenty-five US states and foreign countries have passed anti-SLAPP legislation. In SLAPP actions the plaintiff usually sues for defamation or interference with business relationships. Because the plaintiff’s claimed damages are often in the millions of dollars, “the threat of liability may be enough to scare opponents into silence.”141

The preamble to California’s anti-SLAPP statute explains the reason why California and many other states have taken action to curb malicious litigation and frivolous lawsuits. It states that the “Legislature finds and declares that there has been a disturbing increase in lawsuits brought primarily to chill the valid exercise of the constitutional rights of freedom of speech and petition for the redress of grievances. . . . [I]t is in the public interest to encourage continued participation in matters of public significance, and that this participation should not be chilled through abuse of the judicial process.”142

138 SACK, supra note 132, § 13.1.5.2
139 Id. at § 13.1.5.3.
141 DANIEL R. MANDELKER, LAND USE LAW § 8.46 (5th ed. 2007).
142 CAL. CODE CIV. PROC. § 425.16(a).
Once Section 425.16 is invoked by a defendant, the burden falls on the plaintiff to show that there is a probability that he will be able to prevail on his claim of action.\textsuperscript{143} If the defendant prevails on his motion to strike the complaint, he becomes entitled to recovery of his attorney’s fees and costs.\textsuperscript{144} The defendant’s ability to fully recover his attorney’s fees and costs has served as one of the major deterrents to filing frivolous SLAPP lawsuits.

Additionally, legislation exists that allows defendants who were victims of SLAPP lawsuits to bring counterclaims, called “SLAPPbacks”, against plaintiffs in the suit. The defendant’s counterclaims are often grounded on “theories such as malicious prosecution, abuse of process, or a violation of constitutional rights.”\textsuperscript{145} In \textit{Leonardini v. Shell Oil Co.}, the court stated that “[i]n a malicious prosecution action the legal aspect of probable cause requires a determination whether the prior claim for relief was legally tenable.”\textsuperscript{146} If the prior claim is determined to not be legally tenable, the defendant can file a SLAPPback. However, if the defendant’s actions were not in complete good faith or if the defendant acted with actual malice, a SLAPPback counterclaim may be precluded.\textsuperscript{147}

Some states with anti-SLAPP statutes do not have a motion to strike provision, but rather make an immunity defense available to the defendant. Only if the defendant had a reckless disregard for the truth or knowingly communicated false information would immunity be jeopardized.\textsuperscript{148}

With the implementation of anti-SLAPP statutes by the majority of states, it has become an important consideration for franchisors seeking to silence critics by filing a lawsuit for trade libel or some other cause of action. Additionally, many of the anti-SLAPP statutes contain language that signals that courts should construe the terms of the laws broadly in order to protect the freedom of speech and the right to petition.\textsuperscript{149}

Many of the anti-SLAPP statutes provide protection for a wide array of speech. California’s Section 425.16(e) states that the statute was created to protect:

\begin{enumerate}
\item any written or oral statement or writing made before a legislative, executive, or judicial proceeding, or any other official proceeding authorized by law;
\item any written or oral statement made in connection with an issue under consideration or review by a legislative, executive or
\end{enumerate}

\textsuperscript{143} \textit{Id.} at § 425.15(b)(1).

\textsuperscript{144} \textit{Id.} at § 425.15(c).

\textsuperscript{145} \textit{MANDELKER, supra} note 129, § 8.46.


\textsuperscript{147} \textit{MANDELKER, supra} note 129, § 8.46.

\textsuperscript{148} \textit{Id.} at § 8.47.

\textsuperscript{149} For example, California’s Section 425.16(a), after emphasizing the importance of “participation in matters of public significance,” states that “[t]o this end, this section shall be construed broadly.” \textit{CAL. CODE CIV. PROC.} § 425.16(a).
judicial body, or any other official proceeding authorized by law; (3) any written or oral statement or writing made in a place open to the public or a public forum in connection with an issue of public interest; (4) or any other conduct in furtherance of the exercise of the constitutional right of petition or the constitutional right of free speech in connection with a public issue or an issue of public interest.150

Because Section 425.16(e)(3) and similar statutes expand anti-SLAPP defenses to written or oral expression made in a public forum or that deal with an issue of public interest, filers of SLAPP suits must be aware of the broad protections such statutes provide. Additionally, the legislative intent to broadly construe the statute has given courts leeway to expand anti-SLAPP protections to higher levels.151

The medium in which such written or oral expressions are communicated is irrelevant. For example, in Barrett v. Rosenthal, the California Supreme Court held that websites accessible to the public are public forums in the context of anti-SLAPP legislation.152 The expansion of the definition to include internet websites that are available to the general public has provided protection to those that comment, discuss or criticize topics of public interest online. The ruling also expanded protection to internet users who republish defamatory content on the internet as long as they do not conspire to do so with the original publisher of the defamatory statement.153 Additionally, it provided immunity from civil liability to internet service providers for reposting third-party content online.

Those seeking to discourage criticism through litigation must also be wary of the somewhat expansive interpretation courts have assigned to the requirement that the statements concern an issue of public interest. In Wilbanks v. Wolk, the court held that if the statement “contribute[s] to the public debate,” then the public interest requirement has been met.154 Although Wilbanks requires some showing that the publication will in fact contribute to public discussion of the issue, often matters of public concern and controversy will automatically warrant such a finding.155 Important to note is that the issue does not have to be of any public significance at all, as long as it is under consideration by a legally authorized official proceeding.156

150 CAL. CODE CIV. PROC. § 425.16(e).
151 CAL. CODE CIV. PROC. § 425.16(e).
152 40 Cal. 4th 33, 41 (Cal. 2006).
153 Id. at 63 (Moreno, J., concurring).
Sometimes the publisher of the allegedly defamatory comments is unknown. One’s right to remain anonymous is protected by several Supreme Court decisions. In *McIntyre v. Ohio Elections Comm’n*, the court held that “an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.” Additionally, in *Reno v. ACLU* the court held that speech on the internet is subject to the same protections as are given to other media sources. A few states such as California have also held that, under appropriate circumstances, a plaintiff may not obtain the identities of anonymous publishers through discovery procedures.

The repercussions to those found guilty of violating anti-SLAPP statutes can be severe. Often, the attorney fees incurred by the defendants in litigating the SLAPP suit are high. If defendants succeed in their anti-SLAPP motion to strike, the plaintiffs bringing the suit are responsible for the costs. Additionally, *Ketchum v. Moses* holds that “an award of fees may include not only the fees incurred with respect to the underlying claim, but also the fees incurred in enforcing the right to mandatory fees under Code of Civil Procedure Section 425.16.” Punitive damages can also be awarded by the court in anti-SLAPP violation cases.

**VI. DO REAL WORLD LAWS APPLY IN VIRTUAL WORLDS?**

**A. When Two Worlds Collide**

As if franchisors did not have enough concerns about attacks in the real world, they now must be concerned about attacks on their companies, their products or their intellectual property in virtual worlds, computer-simulated environments in which users can interact with others via avatars. Avatars are typically depicted as three-dimensional representations, which are customizable by the user. Most virtual worlds exist in real time and simulate many characteristics of the real world.

Most of the more popular virtual worlds, such as Blizzard Entertainment’s *World of Warcraft* are viewed as traditional “games” in which users have few rights; users typically fight monsters, increase their points and collect items. In contrast, in Linden Lab’s *Second Life*, users interact with each other as if they were in the real world: users hold jobs, buy and sell real estate, sell items that they create (receiving currency that is readily convertible to real-world money), shop in virtual stores, get married to other users, and even open virtual law firms.

As a result, virtual worlds are no longer the exclusive realm of teenage boys or tech geeks. In fact, the average age of virtual world users is 32 and there is a 1:1 male to female ratio. Virtual worlds have therefore become an ideal place for companies to market their goods to an older and wealthier demographic. Companies such as Toyota, Nissan, Mercedes-Benz,

160 24 Cal. 4th 1122, 1141 (Cal. 2001).
BMW, Dell, Cisco and Intel have all expanded into virtual worlds by opening their own stores and making use of the environment for advertising purposes.\(^{162}\)

*Second Life* has also built up its user base with a unique selling point – that users own the content they create within the game. The problem, though, is that the owners of virtual world intellectual property may not own the same intellectual property in the real world. For example, in *Second Life*, it is estimated that at least 4 million profitable transactions each year are infringing on real world trademarks.\(^{163}\) As of May 2007, over 40 stores in *Second Life* sold infringing Rolex and Chanel watches and more than 50 stores sold infringing sunglasses from Gucci, Prada, Oakley and Rayban. Stores were also selling a number of infringing products from Nike, Apple, Abercrombie & Fitch, Louis Vuitton, and Timberland.\(^{164}\)

### B. Current and Potential Methods of Protection

Most virtual worlds currently rely on in-game protection typically provided by the developers of the virtual worlds.\(^{165}\) These solutions are based on contracts and terms of use to which users must agree before registering accounts in the virtual worlds. For example, providers may close the accounts of deviant users or may ban certain types of activity such as gambling.\(^{166}\)

Virtual world intellectual property protection frequently stems from users individually reporting violations to the providers. This type of system can work, but tends to be slow and inefficient because it is done on a case-by-case basis. eBay’s Verified Rights Owner (VeRO) Program\(^{167}\) is similar, as it relies on individual user reports of improper listings. eBay’s system has decreased the incidence of copyright infringement, but is still criticized for its lack of effectiveness.\(^{168}\)

Even finding infringements in most virtual worlds is difficult because the content of virtual worlds is not searchable through traditional search engines such as Google. In addition to the difficulties in finding and reporting violations, the terms of use that define the protections available to rights owners often narrow the scope of such rights. Even *Second Life*, which

---


\(^{168}\) VeRO for Dummies – Copyright Rules on eBay, EBAY REVIEWS & GUIDES, May 5, 2008, [http://reviews.ebay.com/VerO-for-Dummies-Copyright-Rules-on-Ebay_W0QugidZ10000000001769094](http://reviews.ebay.com/VerO-for-Dummies-Copyright-Rules-on-Ebay_W0QugidZ10000000001769094).
claims that users maintain property rights over their in-game property, limits the property as a “limited license right.” Another clause in the Second Life terms of use states that although users own the intellectual property rights in their creations, the developer owns all the data stored on its servers, including without limitation any data representing or embodying any or all user content.  

Assuming that infringements can be found, the application of real world intellectual property protections can be challenging. The notice and takedown feature of the Digital Millennium Copyright Act is of course available to address copyright issues in virtual worlds, but as previously noted, this remedy is slow and inefficient. A much larger problem exists with virtual world trademark infringement.

Trademark holders must typically report each unique instance of infringement, which is time-consuming and may end up being pointless; once one infringer is reported and removed, two new infringers may pop up. Despite this, trademark holders should still monitor virtual worlds and assert their rights because the law requires trademark holders to actively enforce their trademarks in the event of infringement; a failure to enforce trademarks may result in the loss of registration for the marks. The dilution of a trademark in one or more virtual worlds may also make it difficult for companies to argue that any single infringer should be enjoined. Furthermore, companies that do not participate in virtual worlds today must still maintain their trademarks in these worlds if they decide to participate in them in the future.

Some trademark owners have taken creative approaches to stop trademark infringement. Herman Miller, Inc., the manufacturer of the popular Aeron office chair, responded to infringers selling counterfeit products in Second Life by creating its own genuine in-game products and offering people who had bought counterfeit products a free trade for a genuine chair in the company’s “Get Real” campaign. The exposure that infringing products create for the brand owner may actually serve as free advertising and act as something positive. Because of this, trademark owners actually choose to work together with virtual world infringers to promote their products.

One notable case provides some guidance for trademark protection in virtual worlds. In July 2007, Eros LLC, a popular seller of adult-themed virtual objects for use within Second Life, brought an action against other sellers who had been using Eros’ trademarks in their products. Although the plaintiff was initially unable to obtain the identity of the defendant

---


users, the plaintiff was eventually able to obtain the defendants’ information through subpoenas. In March 2008, the court ultimately enjoined the defendants from copying, distributing, and selling any products bearing Eros’ trademarks and ordered the defendants to disclose all names and email addresses of persons who had access to the account. While this case involved virtual world infringement of a virtual world trademark, there have been no cases yet that address virtual world infringement of real world trademarks. With the amount of infringement in virtual worlds such as *Second Life*, it seems likely that the courts will soon be asked to address this question.

VII. FRANCHISE AND RELATED AGREEMENTS

As discussed above, some of the threats from new media can be resolved or limited by well-written terms set forth in relevant franchise agreements, employment agreements, confidentiality/non-disclosure agreements for franchisee employees, and agreements with vendors or others authorized to link to the franchisor’s website(s). The following checklists summarize some of the provisions that should be considered.

A. Franchise Agreements.

1. Trademark license.
   a. Provision to license or restrict use of trademarks in domain names.
   b. Provision that a grant of a security interest in all domain names used or associated with such business is a condition precedent to authorization to use a website other than the official website for the franchise system in connection with the local franchised business.
   c. Specific provisions for what can and cannot be posted on a website for the local franchise business, including use of trademarks, franchise advertising and marketing materials, and other copyrighted materials.
   d. Consider that any links to or from the franchisee’s website operated in connection with the franchise business be approved by the franchisor.

2. Confidential Information and Trade Secrets
   a. Specific prohibition on posting of confidential information or trade secrets on the internet, during or following term of the franchise agreement, as part of obligation not to disclose such information.
   b. Expand prohibition to address any other form of electronic communication of confidential information or trade secrets.

---

3. **Termination**

   a. Transfer of domain names used in connection with the franchise business to franchisor upon termination, whether or not such domain names incorporate the trademarks of the franchisor.

   b. Prohibition on use of metatags with franchisor’s trademarks following termination. (In circuits where metatags are deemed not to be “trademark use” or no likelihood of confusion, may need to limit time of prohibition to term of non-compete agreement.)

   c. Prohibition on purchase of keyword advertising with franchisor’s trademarks following termination.

   d. Requirement that franchisee delete all electronic documents and information relating to the franchisor, the franchise system, or the franchised business upon termination (with return of confidential information).

4. **Other**

   a. Prohibition on keyword advertising using any franchisor trademark, product name or variation.

   b. Prohibition on posting third party content to any franchisor-sponsored website or any website incorporating or displaying any franchisor trademark unless the franchisee has properly acquired rights to the content.

   c. Prohibition on posting any defamatory, libelous, fraudulent or deceptive content on any such website.

   d. Consider possible need to adjust restriction on area or manner of authorized franchisee sales in light of virtual world issues.

B. **Website Development Agreements/Web Master Agreements**

   1. Assignment of all intellectual property created in connection with the services provided thereunder, including all content, and the associated copyrights. (“Copyrights” should be expressly mentioned in the assignment language.)

   2. Perpetual license for any existing technology of the web developer or web master used in connection with the website, including the right to modify and update such technology and to authorize others to do so.

   3. Requirement that all third party software used to operate the website must be disclosed and licensed to the franchisor.

   4. Requirement that all copyrighted materials posted on or used in connection with the website must be original, owned by the franchisor, web developer or webmaster, or properly licensed unless otherwise agreed by the franchisor.
C. Independent Contractor Agreements.

1. Assignment of all intellectual property created in connection with the services provided thereunder, including all content, and the associated copyrights. (“Copyrights” should be expressly mentioned in the assignment language.)

2. Requirement that confidential documents and information in the Independent Contractor’s possession in electronic form relating to the franchisor, any franchisee or the franchise system be deleted upon expiration or termination of the Agreement.

D. Confidentiality/Non-Disclosure/Employment Agreements for Franchisee Employees

1. Specific prohibition that no documents belonging to the franchisee, franchisor or the franchised business can be posted on the internet or discussed in any blog, chatroom or other medium without the prior written consent of the franchisor.

2. Assignment of all intellectual property rights created or developed by the franchisee’s employee based on any intellectual property owned by franchisor or franchisee, or any knowledge provided or received relating to the franchise system or the local franchise business.

3. Requirement that confidential documents and information in the franchisee’s employee’s possession in electronic form relating to the franchisor, the franchisee, the franchise system, or the franchise business be deleted upon expiration or termination of employment.

E. Linking Agreements

1. Reserve the right for the franchisor to require any link to be removed at any time for any reason.

2. Requirement not to frame franchisor’s website within the linked website and/or to deep link into the franchisor’s website.

VIII. CONCLUSION

The electronic media developed and deployed over the past 15 years have irrevocably changed the style and nature of communications for business and consumers, making the world ever smaller. While this sort of change has produced significant benefits for the world of franchising, including facilitating communications between franchisors and franchisees, and between franchise systems and their customers, it has also created new varieties of threat, as surveyed in this paper, which simply cannot be ignored. These threats confront not only those franchise systems aggressively pursuing an e-strategy; they can impact all members of the franchising community. Although this paper has surveyed some of the most significant new media threats affecting franchising, franchise participants should remain alert to ongoing technical, legal and policy developments, and be sensitive to the potential for abuse arising from any such development.
PRISCILLA L. DUNCKEL

Priscilla Dunckel is a partner in the Dallas office of Baker Botts L.L.P, an international law firm with approximately 800 attorneys. Ms Dunckel manages the trademark department for the Dallas office, concentrating her practice on the protection, enforcement, and licensing of trademarks and copyrights; unfair competition; trade secrets; technology transfers and licensing (domestic and international); publishing; internet issues, cybersquatting, domain name acquisitions; media and entertainment; and specialized legal issues and transactions relating to anticounterfeiting programs, opposition and cancellation proceedings, intellectual property acquisitions and transfers, and related litigation. She also handles matters centering on advertising and computer game development. Priscilla has spoken extensively on intellectual property issues, including on IP issues specifically relevant to franchising. She has been active in the Dallas Bar Association, and served as Chairman of the Dallas Bar Association Sports & Entertainment Section for two terms. Currently, Ms. Dunckel is First Vice Chair of the Franchise & Distribution Law Section of the DBA. Ms. Dunckel received her B.A. degree from Michigan State University, and her J.D. degree *cum laude* from Southern Methodist University. Ms. Dunckel began her professional career as a teacher. She later held a management position in a franchise company and owned two small businesses.
Michael K. Lindsey is a partner in the Los Angeles office of Paul, Hastings, Janofsky & Walker LLP. He is a corporate and transactional lawyer, with a practice concentration in the areas of franchise, distribution and intellectual property law. Mr. Lindsey’s practice includes the acquisition, development, protection and licensing of various forms of intellectual property; antitrust preventive counseling; merger analysis and structuring; franchise disclosure, registration and relationship matters; and advice concerning the sale, distribution and marketing of products and services through manufacturing, joint venture, distribution, dealership and agency relationships. He has spoken and written extensively in these fields. He served as co-editor-in-chief of *International Franchise Sales Laws* (ABA 2006) and the treatise *State Antitrust Law and Statutes* (ABA 2d ed. 1999). He is also a co-author of *Antitrust Handbook for Franchise and Distribution Practitioners* (ABA 2008), *The Intellectual Property Handbook: A Practical Guide for Franchise, Business and IP Counsel* (ABA 2005), *Annual Franchise and Distribution Law Developments 2003* (ABA 2003) and *International Sales Transaction Checklist* (IBA 2003). Mr. Lindsey has been active for a number of years in various Bar organizations, having served as chair of the Franchise Law Committee of the California State Bar Business Law Section and of the Franchise and Dealership Committee of the ABA Antitrust Law Section. He currently serves as Director of the International Franchise and Distribution Division of the ABA Forum on Franchising, Chair of the Computer Industry & Internet Committee of the ABA Section of Antitrust Law, and a member of the Executive Committee of the Antitrust and Trade Regulation Section of the Los Angeles County Bar Association. He received his B.S. degree, *summa cum laude*, from Texas A&M University and his J.D. degree from Stanford Law School. Mr. Lindsey has been named a Southern California Super Lawyer by *Los Angeles Magazine*, and is listed in *The Best Lawyers in America*, *Guide to the World’s Leading Competition and Antitrust Lawyers* and in *Who’s Who Legal*, *The International Who’s Who of Business Lawyers*. 