1 System Internet Communications

By Keith Klein and Matthew Fojut

I. INTRODUCTION[1]

The marketing of products and services started with the shingle outside a proprietor's store and expanded dramatically over the past century. Franchising proved a significant contributor to that expansion, making it possible for branded products and services—originally only available in a limited geographic region—to be recognized and available to everyone everywhere.

The rise of the Internet has further transformed the scope of marketing, creating new mediums for communication on an immediate and global scale. This transformation has created new opportunities for businesses and, of course, new issues for lawyers. For franchising, with its history of relegating global marketing to the franchisor and local marketing to independently owned franchisees, this new, easily accessible, and pervasive medium has proven problematic.

Imagine, for example, that a New York City franchisee offers a discount to the first fifty customers who respond to a Twitter post. With thirty franchised locations in Manhattan, consumers may be unable to determine which locations are extending the offer. This may result in confused consumers responding to "tweets" at nonparticipating locations and, equally troubling, frustrated franchisees embroiled in disputes with neighboring franchisees after being forced to honor another's social media promotions. Requiring franchisees to identify the participating locations on social media posts sounds like an easy solution, but it may

1. Bryan Cave associate Andrew Chereck and Bryan Cave law clerk Alex Boone contributed to this chapter.

not be feasible on sites such as Twitter, where precious few characters (limit of 140) are permitted.

As counsel to businesses that seek to embrace the Internet, practitioners are expected to understand Internet marketing, identify potential legal pitfalls, establish a legal framework to pursue Internet-based endeavors safely and effectively, and respond to issues as they arise. This chapter seeks to familiarize counsel with the dynamics of online marketing, both to consumers and prospective franchisees, on general communications, and offer some practical and legal solutions for franchise systems. Additional information concerning the structure and operation of national marketing funds, and local advertising and cooperative advertising can be found in Chapter 7 of this publication. Because Internet marketing continues to develop, practitioners are encouraged to stay current on legal developments and confirm the state of the law before providing counsel on material issues.[2]

II. AVAILABLE FORMS OF INTERNET MARKETING

The prevailing forms of communication on the Internet are generally categorized into three formats. The original format, known as Web 1.0, consists of one-way broadcasting in which only the business (or Web site owner) publishes information and no meaningful way exists for the user to respond in the same medium.[3] This is most closely analogous to television and radio advertising. Web 1.0 enables a Web site publisher to control its messages carefully, vetting content before publication and modifying content at its discretion. Because of this extensive control over content, Web 1.0 communication has been widely embraced and now, barely fifteen years since its introduction, it is deemed an almost mandatory component of marketing in the modern-day business environment.

The second form of communication, known as Web 2.0, encompasses previously unavailable forms of mass communication, whereby a conversation between the author of the content and others is broadcast worldwide in microseconds in a medium that enables others to comment or participate equally as immediately.[4]

---

2. Marketing on the Internet is a deceptively complex venture rife with sophisticated legal issues involving a number of disciplines. While this chapter seeks to guide practitioners through some relatively basic and common issues experienced by the franchise community, it is not intended to provide a comprehensive discussion of all of the legal issues. The discussions herein, however, should provide a context for the state of the law on most issues franchisors and franchisees are likely to encounter.

3. *See* Jonathan Strickland, *Is There a Web 1.0?*, HOWSTUFFWORKS, http://computer.howstuffworks.com/web-10.htm (defining Web 1.0 based on the definition of Web 2.0 coined by Dale Dougherty of O'Reilly Media, Inc.).

4. *See* Tim O'Reilly, *What is Web 2.0?*, O'REILLY, (Sept. 2005), http:www.oreillynet.com/

At present, the most widely recognized Web 2.0 format is *social commerce*, a broad term that refers to user-generated advertorial content on e-commerce sites that allow consumers to advise one another about and help each other locate goods and services for purchase.[5] This includes all Web sites containing customer ratings and reviews, shopping tools, forums and communities, social media applications, and social advertising. With the recent exponential growth of these Web sites, Web 2.0 is a major focus of online marketers today, but many businesses have not embraced Web 2.0 as fully and quickly as they embraced Web 1.0. Some of those who have entered the world of Web 2.0 have experienced great success, while others have experienced potentially devastating consequences, thus many businesses have simply remained on the sideline waiting for the practical and legal landscape to become more clearly defined.

Even as Web 2.0 continues to evolve and gain traction, technological developments have brought the Internet to the cusp of the third form of communication, Web 3.0. This term, reportedly coined by *New York Times* writer John Markoff, refers to an "intelligent web" that converts the Internet into a personalized catalog "with the machines doing the thinking" instead of an aggregation of billions of documents that can be vetted through Boolean and other rudimentary electronic searches.[6] As of the date of publication, Web 3.0 has not developed in a manner that permits a meaningful discussion about its impact on franchising or its legal ramifications, but it will no doubt present further unique complexities for franchise systems.

III. DEVELOPING AN ONLINE PRESENCE

The first steps in establishing a presence in the traditional marketplace are staking out real estate and developing a brand. The Internet marketplace is no different, though practically speaking, these first steps are easier and cheaper to accomplish. As the Internet business environment continues to grow, however, the relative ease and low barrier to entry have created congestion and given rise to issues not experienced in the traditional marketplace.

The first critical issue unique to the online environment is the particular scarcity of Internet real estate–domain names. Under trademark law, a fast casual dining

---

pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

5. *See* Paul Marsden, *Simple Definition of Social Commerce*, #DiT (Nov. 17, 2009), http://socialcommercetoday.com/social-commerce-definition-word-cloud-definitive-definition-list/ (last updated Jan. 2011).

6. John Markoff, *Entrepreneurs See a Web Guided by Common Sense*, N.Y. TIMES, Nov. 12, 2006, at www.nytimes.com/2006/11/12/business/12web.html.

brand and a day spa brand could co-exist in the marketplace with the same trade name without issue. On the Internet, however, room exists for only one business to have the name associated with [brand].com, which therefore generates significant demand for that particular online real estate. One relatively high-profile and early example of this problem was a dispute over the domain name www.candyland.com between an adult entertainment provider (which had registered the name first) and Hasbro, a well-known board game manufacturer.[7] Further complicating things is the fact that other businesses, whether for legitimate or nefarious purposes, may seek to obtain a domain name that is, for example, one typographical error away from being an identical domain name. As a widely discussed case in point, Zero Micro Software obtained a registration for micros0ft.com (with a zero in place of the second "o"), leading Microsoft to send a cease and desist letter, which ultimately led to Zero Micro Software's discontinued use of the domain name.[8]

Clearly, the apparently limitless resources of the Internet quickly narrow under the demands for unique domains, and the same issue has quickly developed in the realm of social media sub-domains, which will be addressed later in the chapter. While every business seeking an online presence faces the real estate scarcity issue, the situation is significantly more complex in the world of franchising. Until recently, Internet marketing was largely reserved for the franchisor to focus on building overall brand recognition. With the evolution of Web 2.0, however, franchisees have expressed frustration about their inability to tap the Internet's ability to enhance regional marketing as well. With franchisee pressure increasing, how can a system maintain control over domain names and social media sub-domains (particularly those containing its trademark) and at the same time enable franchisees to embrace the Internet and social media?[9] To address those questions, it is first necessary to understand the process for the registration of domain names and social media sub-domains.

---

7. *See* Hasbro, Inc. v. Internet Entertainment Group, Ltd., C96-0130WD (W.D. Wash., Feb. 9, 1996). IEG ultimately surrendered the domain name and a preliminary injunction was entered.

8. Neal J. Friedman & Kevin Siebert, *The Name Is Not Always the Same*, 20 SEATTLE U. L. REV. 631, 663 n.112 (1997).

9. In one instance, a Taco Bell franchisee registered the domain name www.mylocaltacobell.com for its locations in Illinois and other parts of the Midwest. While that Web site provides information regarding locations in parts of the Midwest, it certainly does not provide local information for locations in Arizona or Oregon, for example. Panera Bread, on the other hand, appears to have taken steps to address this issue. Franchisees register domain names containing the geographic region where stores are located, for instance http://www.paneraiowa.com; http://www.panera-kansas.com; and http://www.panera-colorado.com.

A. OBTAINING DOMAIN NAMES

Until recently, securing domain name rights only involved two primary steps: (1) obtaining trademark rights and (2) registering the desired brand with a Top Level Domain (TLD), e.g., .com, .net, or .org, by purchasing it from either a domain registrar or a private party. Ongoing developments with TLDs and the proliferation of social media sites now necessitate a more strategic and forward-thinking approach to this process.

1. SECURING TRADEMARK RIGHTS

Almost inherently implied in an online brand presence is the existence of a trademark or trade name. The process of registering a trademark is not addressed in this chapter, but a brief discussion of related issues is appropriate. Some of the most frequent and potentially costly missteps in registering a domain name occur when the registrant fails to undertake an adequate trademark search and further fails to register the domain name with the United States Patent and Trademark Office (USPTO) without the TLD. For purposes of a good faith search before submitting an application, a search engine query of the desired domain name is a decent first step; however, a full trademark search should be conducted before investing substantial capital to purchase the domain name and brand the underlying Web site.[10]

The proliferation of branded Web sites since the late 1990s has placed quite a strain on the federal trademark framework.[11] It stands to reason that the USPTO examiners (and possibly judges and juries) may take into account the dearth of available trademarks and favor new brand entrants to stimulate new business ventures—potentially having the effect of shrinking the existing protections of current trademark owners. There seems to be good news and bad news for brand owners from such a phenomenon. While it may become easier to secure domain and related trademark rights as a new brand entrant, new brand threats will undoubtedly emerge in the future. It is already challenging to (1) conceive of a powerful and relevant brand, (2) register a domain name related to the brand, and (3) get comfort that the brand does not infringe upon another's trademark. As the Internet continues to expand, it will narrow the breadth of protection afforded to trademark owners.

---

10. The most commonly used vendor for trademark searches is Thomson Compumark. *See* THOMSONCOMPUMARK, http://www.Compumark.thomson.com (last visited December 8, 2013).

11. The USPTO reported the largest number of total active trademark registrations in its history as of Fiscal Year 2012: 1,838,007. *See Active Registrations*, TRADEMARKSTATISTICS.COM, http://www.trademarkstatistics.com/ (last visited December 8, 2013).

2. DOMAIN NAME REGISTRATION

Formed in 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) is a not-for-profit, public-benefit corporation responsible for coordinating and ensuring the overall stability of the global Internet's systems of unique identifiers: domain names, Internet protocol numbers and autonomous system numbers.[12] The technical management and operation of the Internet is not particularly relevant to franchise law practitioners, but as briefly described now, monitoring ICANN's management is becoming increasingly important.

In the 1990s, the domain name registration process was rather simple—go to www.networksolutions.com or another of the then relatively few registrars, enter the desired name and limited additional information, pay a registration fee, and enter the date for the expiration of the registration. Today, however, even the relatively mundane task of registering a domain name involves strategic and budgetary considerations.

First, almost everyone seeks a .com, .net, or .org domain name. Unless the desired name consists of a "fanciful" trademark,[13] it is now rare to find domain names available for registration or for purchase from third parties at a low purchase price. Strategies to obtain the desired domain can vary. If assigned the task of registration, some basic issues should be considered.

1. Investigate Registration Options. Merely inquiring at an Internet registrar regarding availability of a proposed domain name may alert others of interest and thus enhance the potential value of the name. Therefore, when conducting an inquiry, be prepared to execute immediately if the name is available, otherwise the name may be registered shortly thereafter by others. In all likelihood, the domain name being sought will already be registered and either actively used for a primary purpose Web site or parked by the registrant for an alternative purpose. In either event, be sure to review the registration information carefully as the name may be scheduled to become available soon or, at a minimum, the expiration date may provide insight regarding the current registration's length of use and how the registrant obtained ownership of the domain name.
2. Evaluate the Current Use of the Domain Name. Pre-existing use of the domain

12. *See* Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers, Nov. 25, 1998 *available at* http://www.icann.org/en/general/icann-mou-25nov98.htm.

13. A fanciful mark is a name that is made up to identify the trademark owner's product like EXXON for oil products and KODAK for photography products. *See* J. Thomas McCarthy, TRADEMARKS AND UNFAIR COMPETITION, §§ 11:2, 11:3, 11:4A (2d ed. 1984) (McCarthy, Trademarks).

name as a primary purpose Web site typically bodes poorly for an easy or inexpensive acquisition, unless it is being overtly used by a competitor or other party for an improper purpose, a process often referred to as cybersquatting (see Section III.A.3 below). Most cases of cybersquatting are readily apparent, but a more discreet form of cybersquatting occurs when domain name registrars and private parties "park" domains and place search engine links on the parked Web pages, thereby deriving revenue from unsuspecting traffic searching for branded Web sites.[14] While this practice is generally legal, it may cross the line when implemented as a way of driving traffic to a competitor's Web sites.

3. Develop an Acquisition Strategy. Efforts to purchase an existing domain name through a negotiated business transaction require a comprehensive understanding of the marketplace, an investigation of the registrant's intended purpose, and some luck. Basic steps should include the analysis of a legal right to acquire the name, the expression of interest conveyed from a generic e-mail account, and the use of a simple but comprehensive domain name assignment agreement. Sending an expression of interest from a law firm e-mail account and using complex assignment agreements can imply an enhanced value to the name. If current use of the domain name involves cybersquatting, evaluate the likelihood of success through available legal recourse and the associated costs.

A second strategic step when registering domain names involves investigating other available potentially useful domain names. This may seem intuitive, but consider other TLDs as well. As the Internet further expands, this may become critical. For example, ICANN has already started accepting applications for new TLDs to provide more innovation, choice, and competition on the Internet. Additional TLDs may be in the works as ICANN continues to solicit input about opening TLDs to any string from three to sixty-three characters in length, which may be supported by a number of other scripts (e.g., Chinese, Arabic, etc.). Groups representing cities such as New York (i.e., .nyc), charities (i.e., .green), and generic terms (i.e., .franchise, .hotel, .autos, etc.) have previously expressed interest in proposing new TLDs. Even multi-national companies have expressed interest in their own TLD, i.e., .deloitte.[15] Keeping current with the proposed TLDs and

14. The term "domain parking" is "the registration of an Internet domain name without using it for services such as e-mail or a Web site i.e., without placing any content on domain." *See Domain Parking*, Wikipedia, http://en.wikipedia.org/wiki/Domain_parking.

15. ICANN limited the first batch of applications to 500 and has scheduled future windows for additional applicants. ICANN began delegating the first new TLDs in October 2013 and the first English language TLDs in November 2013. Some new TLDs include

possibly proposing others may become an integral part of the domain name registration process. For some franchise systems in particular, it may make sense strategically and economically to create a TLD with the brand name.

3. Combating Cybersquatting of Domain Names

As mentioned above, companies often encounter the problem of cybersquatting when attempting to register a specific domain name. Cybersquatting occurs when someone registers or otherwise uses a domain name with the intent to profit from the goodwill of a distinctive brand belonging to someone else, or holds the domain for ransom.[16]

The Lanham Act proved inadequate as a comprehensive resource for trademark owners seeking to compel transfer of domain names from a third party. While it provided businesses with a sufficient remedy against another company offering the same or similar products or services—based on a likelihood of confusion—it failed to work as a powerful tool for trademark owners pursuing claims against registrants that used the mark for other potentially improper purposes. For example, it was virtually impossible to prove several elements of Lanham Act claims against individuals who did not use the trademark in commerce and merely sought to extract a significant payment for the domain name. Indeed, the Lanham Act struggled to be effective in most cybersquatting cases unless the claimant could demonstrate that the mark at issue was deemed "famous" as contemplated under existing law.

In an effort to address some of the Lanham Act's weaknesses, in 1999, federal legislation known as the Anticybersquatting Consumer Protection Act[17] (ACPA) was enacted to prevent the registration of domain names containing third-party trademarks to registrants not intending to create a legitimate Web site, but rather intending to sell the domain name to the trademark owner at an inflated price. Pursuant to the ACPA, a trademark owner may bring a lawsuit against a domain name registrant who registers or uses a domain name that is "identical or confusingly similar" to either a distinctive trademark or dilutive to a "famous" trademark and has a bad faith intent to profit from such use of the domain name.

Filing a lawsuit alleging violations of ACPA can be expensive and time consuming—both major impediments to launching a successful online brand presence. It is thus important to know that ICANN implemented the Uniform Dispute

.Equipement, .lighting, .clothing, .technology, and .menu. Registration requirements include, among other things, a $185,000 evaluation fee and sufficient financial depth to keep the registry fully operational for at least three years.

16. *See* H.R. Rep. 106-412, at 6 (1999) (Background and Need for the Legislation).
17. 15 U.S.C. § 1125(d).

Resolution Policy (UDRP) as a mechanism for brand owners to easily and efficiently address the problem of cybersquatting better. Under the UDRP, as part of the registration of any domain name, the registrant consents to participation in the UDRP's form of alternative dispute resolution and agrees to abide by the dispute resolution's results. The success rate of reclaiming a domain name under the UDRP is high (near 85 percent).[18] The typical dispute resolution takes less than a month and costs less than $3,000. The recent trend of dispute resolution panels under the UDRP is to place a burden on the alleged cybersquatter to show some evidence of performing due diligence to determine whether registration of the domain name in question infringes the rights of any third party. This is noteworthy as it could expand the scope of registrations that might be subject to a bad faith argument. New registrants should therefore also be aware of potential affirmative duties in selecting and registering domain names.

4. Social Media Web Sites

The proliferation of social media Web sites has created new worlds of Internet real estate where establishment of the brand may be critical. Many social media Web sites enable a company to establish its own page to attract and communicate with consumers participating in the site's particular activity, i.e., www.[socialmediaWeb site].com/brandname. Registering a brand on social media sites is generally not complicated. Facebook.com, for example, encourages brands to develop a community on its Web site. Registering a brand on the site involves nothing more than clicking the link on the lower right portion of the facebook.com homepage and following the prompts.

Unlike domain names, however, registration of a Web page on a social media Web site is not subject to ICANN directives, and instead generally falls within the jurisdiction of the company administering the site. Oftentimes, this actually provides for a more orderly administration of Web pages. For example, unlike ICANN's administration of domain names, social media Web sites generally prohibit use of generic names—such as food, hotel or franchise—as the sub-domain name, thereby prohibiting one brand from dominating an entire generic category. Most social media Web sites also require the registrant to affirm that he or she is the brand's authorized representative to create the Web page, which can help deter or prevent others from taking a brand name subdomain without authorization or a legitimate business purpose. Because companies desire to have brand presence on multiple sites, and the preferred sites can change rather quickly, familiarity

18. *See* Alistair Payne, PowerPoint, WIPO Conference: 10 Years UDRP—What's Next (Oct. 12, 2009), *available at* http://world-intellectual-property-organization.com/export/sites/www/amc/en/docs/payne13.pdf.

with the unique terms and conditions of each of the most popular social media Web sites du jour has become increasingly critical for a practitioner desiring to be conversant in social media issues.[19]

5. Cybersquatting on Social Media Web Sites

Social media Web sites have established their own policies to address claims of infringement on trademarks and other intellectual property. A survey of the policies of some of the more popular social media Web sites is set forth below:

- **Facebook.** Facebook has established a procedure for parties that are either cybersquatting on a trademarked username or are falsely posing as another party. To report cybersquatting, a claimant must complete a form requesting that the username be transferred.[20] For impersonators, claimants must go to the impostor profile, click "Report this Person," check the "Report this Person" box, choose "Fake Account" as the reason, and add "Impersonating me or someone else."[21]
- **Pinterest.** Pinterest, in appropriate circumstances and in its discretion, may "disable and/or terminate the accounts of users who repeatedly infringe or are repeatedly charged with infringing the copyrights and other intellectual property rights of others." In accordance with the Digital Millennium Copyright Act of 1998, Pinterest will respond expeditiously to claims of copyright infringement that are reported to Pinterest's Designated Copyright Agent.[22]
- **Twitter.** Twitter maintains a trademark-specific policy that bars "using a company or business name, logo, or other trademark protected materials in a manner that may mislead or confuse others with regard to its brand or business affiliation."[23] In instances where there is "clear intent to mislead

19. *See Terms of Service*, Twitter, http://twitter.com/tos (effective Dec. 11, 2012); *Statement of Rights and Responsibilities* , Facebook; http://www.facebook.com/terms.php?ref=pf (last updated Dec. 11, 2012); *User Agreement*, LinkedIn, http://www.linkedin.com/static?key=user_agreement (last revised Sept. 12, 2013); *StumbleUpon Terms of Service*, StumbleUpon, http://www.stumbleupon.com/terms/ (effective Aug. 2012); *Foursquare Labs, Inc. Terms of Use*, foursquare, http://foursquare.com/legal/terms (last updated Jan. 29, 2013); and *Terms of Service*, Pinterest http://about.pinterest.com/terms/ (last visited December 8, 2013).

20. *Questions About Usernames*, Facebook, http://www.facebook.com/help/contact.php?show_form=Client_Username (last visited December 8, 2013) (Facebook "client username form").

21. Report Something at www.facebook.com/help/ and follow the prompts to intellectual property issues. (Last visited December 8, 2013).

22. For additional information, see *Copyright*, Pinterest, http://about.pinterest.com/copyright (last visited December 8, 2013).

23. Trademark Policy, Twitter, https://support.twitter.com/articles/18367-trademark-policy (last updated Oct. 3, 2012).

others" through the unauthorized use of a trademark, Twitter will suspend the account and notify the account holder. When there is confusion about the account, but it is not "purposefully passing itself off as the trademarked good or service," Twitter will notify the accountholder and provide him or her the opportunity to clear up any potential confusion.[24] Twitter allows for commentary, news feeds, and fan accounts to discuss trademarked material, as long as the account information does "make it clear that the creator of the account is not actually the company or business entity that is the subject of the news feed/commentary/fan account."[25] If the account is "reported to be confusing," Twitter may request that the accountholder make additional changes. Twitter also provides for a reporting process in the event that a claimant discovers a violation of the trademark policy.[26] The procedure allows for the claimant to specify the requested action, including "removal of infringing account, or transfer of trademarked username to an existing company account."

- **LinkedIn.** LinkedIn uses a general catch-all policy to prohibit all types of intellectual property infringement. The site requires that "information posted by Users be accurate, lawful and not in violation of the intellectual property rights of third parties."[27] In enforcing this policy, LinkedIn may remove or disable access to infringing content if it receives the proper notification that the content "infringes intellectual property rights, is inaccurate, or is otherwise unlawful."[28] LinkedIn also permits users to refute claims of infringement by submitting a counter-notice.[29] LinkedIn will, "in appropriate circumstances and in [its] discretion," disable the accounts of repeat infringers.

B. GRIPE SITES—THISBRANDSUCKS.COM

It is important for brand owners to understand that the ACPA, UDRP, and social media terms and conditions will not trump basic guarantees of free speech. Almost all successful brands face critical commentary at one time or another. Many online brands will find themselves the subjects of so-called gripe sites.[30] Gripe sites are Web sites or social media Web pages devoted to criticism and complaints of

24. *Id.*
25. *Id.*
26. Twitter, "What is a Trademark Policy Violation on Twitter?" https://support.twitter.com/articles/18367#
27. *Copyright Policy*, LINKEDIN, http://www.linkedin.com/legal/copyright-policy (last revised Mar. 24, 2010).
28. LinkedIn, Copyright Policy, http://www.linkedin.com/legal/copyright-policy?trk=hb_ft_copy
29. *Id.*
30. A "gripe site" is a term developed by Paul Levy to describe a Web site established to criticize an institution such as a corporation, union, government body, or political figure.

certain brands and can certainly test brand loyalty. For the most part, such Web sites are protected commercial speech. In a U.S. district court case arising out of the ACPA, the court reaffirmed that gripe sites are protected under the First Amendment, and in most circumstances will not be subject to a claim of bad faith under the ACPA.[31] In deciding whether the defendant had registered its domain names www.mayflowervanlinebeware.com and www.mayflowervanline.com with the bad faith intent to profit from the plaintiff, the court found the "Defendant's motive for registering the disputed domain name[s] was to express his customer dissatisfaction through the medium of the Internet" and was therefore not in bad faith. UDRP panels are likely to follow this reasoning as well.

While the battle may be difficult, there may be some relief for brand owners in challenging gripe sites. In *Career Agents Network, Inc. v. Careeragentsnetwork.biz*,[32] the court held that a site that has no commercial purpose, but merely contains commentary and criticism, is protected.[33] Such a decision suggests that, if there is any profit motive on the part of the owner of the gripe site, the brand owner might prevail. Profit motive may be established if the Web site is displaying search engine links using the brand or if the owner of the gripe site has some connection with a competitor.[34] Another way to prove profit motive is to offer the gripe site owner payment to take down the site or retract the criticisms. If the owner accepts or negotiates the payment amount, that evidence could be used in favor of the brand owner. However, the publicity of such an attempt could backfire on the brand owner.

IV. ESTABLISHING AND MANAGING WEB SITES AND SOCIAL MEDIA PAGES

With domain names and social media pages secured, the skeleton of an Internet presence has been created. Determining the content to be included on the Internet presents the next challenge. For company Web sites, it is essential to include Web 1.0 features, such as descriptions of offered products or services, available locations and contact information, competitive marketing information,

31. *See* Mayflower Transit, L.L.C. v. Prince, 314 F. Supp. 2d 362 (D.N.J 2004).
32. Career Agents Network, Inc. v. Careeragentsnetwork.biz, 09-CV-12269-DT, 2010 WL 743053 (E.D. Mich. Feb. 26, 2010).
33. The *Career Agents Network, Inc.* case has been appealed and such appeal presently remains pending.
34. *See Hillary Rodham Clinton v. Michele Dinoia*, National Arbitration Forum Claim No. FA0502000414641, Mar. 18, 2005 (full text available at http://www.arbforum.com/domains/decisions/414641.htm).

and promotional materials. Determining Web 2.0 content demands more ingenuity and forethought. The following includes a brief discussion of some generally applicable laws.

A. LAWS APPLICABLE TO SOCIAL MEDIA WEB SITES AND CONTENT

A primary concern with Web 2.0 content involves claims of infringement upon third-party rights for user-generated content. Two federal laws, The Digital Millennium Copyright Act and the Communications Decency Act, address this area of concern. Another major concern involves the rules of engagement with minors, addressed by additional federal legislation known as the Children's Online Privacy Protection Act.

1. THE DIGITAL MILLENNIUM COPYRIGHT ACT

Potential liability arising from a third party's works of art contained in user-generated content posted on the company's Web site or social media Web page is a legitimate and natural concern faced by all participants in the social media process. In 1998, well before the onset of social media, Congress enacted the Digital Millennium Copyright Act (DMCA), in part to address potential copyright liability occurring on the Internet due to acts of individuals other than the Web site owner/operator. Title II of the DMCA, called The Online Copyright Infringement Liability Limitation Act,[35] establishes a safe harbor for Web site operators from copyright infringement claims, provided that the Web site qualifies for such protection and the operator expeditiously complies with the statute's provisions in the event of an infringement claim.

To qualify for protection under the DMCA, a company or individual must be an Internet service provider (ISP) or an online service provider. What does that mean? Although the definition has yet to be heavily litigated, in its most simplistic sense, the term encompasses any company that provides an online service, such as Web sites, discussion forums, chat rooms, Web mail, etc. The limited cases interpreting the meaning of the term have embraced a Congressional directive to interpret the phrase broadly.[36] In addition to falling within the definition of "service provider," a Web site also must "not receive a financial benefit directly attributable to the infringing activity" and it must not have actual or constructive knowledge that it is hosting the infringing material.[37] The existence of a repeat

35. 17 U.S.C. § 512.
36. *See* AIS Scan v. RemarQ, 239 F.3d 619 (4th Cir. 2001) ("the Act defines service provider broadly").
37. 17 U.S.C. § 512.

infringer policy is also critical for service providers to avail themselves of the DMCA's safe harbor provisions. Service providers must have a "policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."[38]

A recent landmark case concerning DMCA protection is *Viacom Int'l, Inc. v. YouTube, Inc.*[39] Viacom filed suit for $1 billion in damages against the YouTube creators alleging deliberate copyright infringement allowance to build traffic to the Web site. Viacom had sent a list of 79,000 takedown notices for removal, and YouTube promptly removed the content the next day.[40] The trial court held that YouTube did not have actual or "red flag" knowledge of the copyright infringement, despite strong evidence in the form of e-mails amongst YouTube's founders stating otherwise. The court deferred to YouTube's repeat infringer policy: "three strikes and out."[41] Although YouTube gave one strike for any takedown notice with multiple videos and one strike for multiple takedown notices within two hours, the court accepted the policy as long as something was in place and enforced. However, on appeal, the court held that YouTube committed willful blindness, and did in fact have "red flag" knowledge of the copyrighted material. The reversal by the court of appeal suggests that service providers may be best served at least to have a moderate repeat infringer policy, generally consisting of a three-strike limit.[42] Further, if a service provider is made aware of infringing material, even without actual knowledge, courts may impute that the service provider still have "red flag" knowledge, thus exposing the provider to vulnerability. More importantly, however, the decision reiterates that there is no affirmative monitoring requirement for infringing material by service providers—it must be brought to their attention.[43]

Assuming the Web site qualifies for the safe harbor, the DMCA mandates that the Web site identify a designated agent to receive takedown notices and that it expeditiously comply with such notices. It also includes a counter-notification provision that offers a safe harbor from liability to their users upon notice from such users claiming that the material in question is not, in fact, infringing. While these provisions are set forth under United States law, the same basic procedures have generally been adopted worldwide: for example, in South Korea's Section 102 and 103 of Copyright Law of Korea, and in the European Union's Electronic

38. 17 U.S.C. § 512(i)(1)(A).
39. Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012).
40. *Id.* at 26.
41. *Id.* at 40.
42. *Id.* at 41.
43. *Id.* at 40.

Commerce Directive, which was subsequently implemented by its member states (i.e., France's Digital Economy Law).[44]

2. THE COMMUNICATIONS DECENCY ACT

In 1996, Congress enacted the Communications Decency Act (CDA).[45] Certain portions of the CDA have since been struck down as unconstitutional, but the operative portion for companies' social media features remains intact. In Section 230 of the CDA, Congress provided for protection for online service providers from actions against them based on the content of third parties. It provides, in pertinent part, that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[46] This immunity is subsequently qualified; however, in that Congress instructs courts to construe the immunity provided under the CDA "in a manner that would neither 'limit or expand any law pertaining to intellectual property.'"[47] "As a result, the CDA does not clothe service providers in immunity from laws pertaining to [federally recognized] intellectual property." [48]

The primary inquiry into whether an interactive computer service qualifies for protection under the CDA is whether it constitutes as an information content provider. Case law suggests that a provider does not have to provide tortious content overtly and actively to be found liable. For example, in *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, the plaintiff brought housing discrimination claims against a Web site designed to match people renting out space to live. The Web site required users to create a profile and disclose his/her sex, sexual orientation, and family status.[49] The Web site also provided a search engine with a drop-down menu to sort by these factors.[50] Based on these and other features, the Web site asserted immunity under the CDA, arguing that it did not provide any discriminatory information.[51] However, an information content provider is defined as someone who is "responsible, in whole or in part, for the creation or development of" the offending content.[52] The court held that the questions, profiles, and drop-down menus regarding private information were not immune from the CDA because they "elicited" and "induced" particular

44. France, Digital Economy Law no. 2004-575 of 21 June 2004.
45. 47 U.S.C. § 230.
46. 47 U.S.C. § 230(c)(1).
47. 47 U.S.C. § 230(e)(2).
48. Perfect 10, Inc. v. CCBILL LLC, 488 F.3d 1102, 1118-1119 (9th Cir. 2007) (recognizing federal intellectual property laws as excluded from CDA immunity provisions).
49. *Id.* at 1161.
50. *Id.*
51. *Id.* at 1165.
52. 47 U.S.C. § 230(f)(3).

responses, thus allowing the Web site to contribute to the information provided.[53] The court, however, further found that the "additional comments" section was protected under the CDA because it was a neutral tool that did not prompt or entice any comments. Thus, even asking certain questions and providing a standardized template for answers can leave a service provider open to liability. Service providers may be well served to exercise care in trying to obtain information from users in a neutral manner such as an open text box or "additional comments" section.

Subject to the above-described limitations, the CDA effectively shields ISPs and Internet users from liability for torts committed by others using their Web site or online forum, even if the provider fails to take action after receiving actual notice of the harmful or offensive content. The CDA's broad immunity has come under fire from time to time because it permits Web sites to disregard defamatory or other injurious content. If an issue presents itself, the best practice is to ensure that neither Congress nor the courts have narrowed its protections.

B. The Children's Online Privacy Protection Act

In addition to the safe harbor laws, Congress also imposed obligations on Web sites that enable interaction with users. One of the more notable is the Children's Online Privacy Protection Act[54] (COPPA) which, as modified and effective April 21, 2000, applies to the online collection of personal information from children under thirteen years of age. Personal, identifiable information typically includes name, e-mail, phone number, social security number, and address, and can also be combined with other distinguishing physical characteristics such as eye and hair color.[55] COPPA applies to commercial Web sites and online services that are either directed to children under thirteen years old or have actual knowledge that children under thirteen are providing information online. It mandates what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online, including restrictions on the marketing to those under thirteen.[56] COPPA mandates that a Web site operator must include in its privacy policy the following: (1) the contact information of all operators; (2) what information is collected as well as why and how it is used; (3) whether such information is divulged to third parties; (4) that parents must be able to consent to the service or action without consenting to third-party

53. *Roommates.com, LLC*, 521 F. 3d. at 1188.
54. 15 U.S.C. § 6501, *et seq.*
55. 15 U.S.C. § 6501, http://www.coppa.org/coppa.htm.
56. *Id.* For FTC guidance on how to comply with COPPA, go to http://www.COPPA.org.

dissemination; (5) that the operator cannot collect more personal, identifiable information than is necessary; and (6) that operators must give parents the option to review and delete any information collected. In addition, if the operator discloses personal, identifiable information to third parties, it must obtain verifiable parental consent.[57]

As of the date of publication, the Federal Trade Commission (FTC) has proposed updates to COPPA, intended to strengthen its protection further against the collection of personal, identifiable information for children under thirteen years of age and younger. The commission proposes to state within the definition of "operator" that personal information is "collected or maintained on behalf of" an operator, where it is collected in the interest of, as a representative of, or for the benefit of, the operator. This change would make clear that an operator of a child-directed site or service that chooses to integrate the services of others that collect personal information from its visitors should itself be considered a covered "operator" under the rule.[58] The commission also proposes to modify the definition of "website or online service directed to children" to clarify that a plug-in or ad network is included if it knows or has reason to know that it is collecting personal information.[59] To address the reality that some Web sites are appealing to both young children and adults, the proposed definition change would allow these mixed audience Web sites to age-screen all visitors to provide COPPA's protections to users under age thirteen.[60] Finally, the commission proposes to modify the rule's definition of "personal information" to make clear that a persistent identifier will be considered personal information where it can be used to recognize a user over time, or across different sites or services, and where it is used for purposes other than support for internal operations.[61]

The FTC enforces COPPA with regularity and tenacity. It has brought a number of actions against Web site operators for failure to comply with COPPA requirements, including actions against franchisors such as Mrs. Field's Cookies.[62] The FTC also has not been hesitant to pursue social media Web sites, fining social media Web site Xanga $1 million for repeatedly allowing children under thirteen to sign up for the service without getting parental consent.[63] And, when the FTC

57. *How to Comply with the Children's Online Privacy Protection Act*, COPPA, http://www.coppa.org/comply.htm (last visited December 8, 2013).
58. Children's Online Privacy Protection Rule, 16 C.F.R. pt. 312, *available at* http://www.ftc.gov/os/2012/08/120801copparule.pdf
59. *Id.*
60. http://www.ftc.gov/opa/2012/08/coppa.shtm
61. http://www.ftc.gov/opa/2012/08/coppa.shtm
62. *See* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2003/02/mrs-fields-famous-brands-inc-mrs-fields-holding
63. http://www.ftc.gov/news-events/press-releases/2006/09/

does take action, $1 million fines are not entirely uncommon. For example, the FTC recently settled with Sony BMG for $1 million because it collected personal, identifiable information from over 30,000 underage users without verifiable parental consent, even though Sony stated in its privacy policy that underage users would not be allowed access and personal information would not be collected from them.

While children under thirteen can legally give out personal information with their parents' permission, many Web sites altogether disallow underage children from using their services due to the amount of paperwork involved. To block users under the age of thirteen completely, many operators use "age-gating." The user's age should be verified in a way that does not invite falsification—i.e., not a drop-down menu, not stating that visitors under thirteen cannot enter, and not a check box that allows a user to click and confirm that he or she is over twelve years old. The operator should also use a "cookie" to prevent any "back buttoning" to change age. The recommended method is to have an open text box where the user would manually input his or her age. If an operator uses any of the methods listed above but then does not block the user, it may be in danger of a COPPA violation by having "actual knowledge" of users under thirteen years of age. This is certainly an area to watch as the FTC has stated it is actively seeking ways to expand the breadth and requirements of the statute.

C. Reporting Child Pornography

Anyone operating a Web site, particularly those with Web 2.0 features, must be aware of the affirmative obligations with respect to how to handle the discovery of child pornography posted on their Web sites. In 2008, Congress passed laws which, subject to a limited, narrow, affirmative defense, impose strict liability for the display of visual representations of sexual abuse of children.[64] The only stated affirmative defense in the act requires that the Web site operator "promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any such visual depiction," take reasonable steps to destroy each such visual depiction or report the matter to a law enforcement agency and provide the agency with access to such material.[65]

D. Franchise Sales and Disclosures Still Apply

The use of Web sites also poses two unique issues for franchisors and their

xangacom-pay-1-million-violating-childrens-online-privacy

64. 18 U.S.C. § 1466A.
65. 18 U.S.C. § 1466A(e).

counsel regarding the promotion of their franchise opportunity (as opposed to the franchise brand in general):

1. By advertising its franchise opportunity on its Web site, is a franchisor making an "offer" that would trigger registration obligations in franchise registration states?
2. Must franchisors file their Internet advertisements in those states that require the filing of all proposed advertising materials before they may be used?

Franchisors, like most other business operators, quickly found that the Internet was an invaluable marketing tool and began promoting their franchise on their Web sites and through other Internet marketing means. In response, in 1998 North American Securities Administration Association (NASAA) issued a recommendation so that if a customer visits a franchisor's Web site, a franchisor's online offer is not interpreted as "offering" the franchise in a particular state, and thus would be subject to the state's registration requirements. The states followed suit, and presently all of the franchise registration states provide a limited exemption for franchise advertisement "offers" made on the Internet. These exemptions generally require that: (1) the Internet advertising must clearly state that franchises are not being offered to residents of any state where the franchisor is not registered; (2) the advertising on the Internet may not be directed specifically (for instance, by e-mail) to residents of registration states where the franchisor is not registered; (3) the franchisor may not offer franchises to state residents through some other means, such as by direct mail or personal solicitation; and (4) the franchisor may not sell any franchises in the state until it has registered in the state and properly disclosed the prospect.

While these exclusions generally exempt "offers" made on a franchisor's Web site from registration (provided all of the conditions are met), they did not address whether registered franchisors were still required to submit copies of their Web page advertisements in the seven states that currently require the submission of proposed advertising materials.[66] States have therefore been forced, at minimum, to revisit their advertising filing laws and regulations and, in some cases,

66. These states are California, Maryland, Minnesota, New York, North Dakota, Rhode Island, and Washington. Also, franchisors are only required, where applicable, to file materials advertising their franchise opportunity—not the goods or services the franchise system offers. For example, a pizza franchise is not required to file materials advertising pizza specials or in-store promotions.

have made changes to exempt advertisements directed to the general public via the Internet.

For example, in 2003 California amended its franchise regulations to include an exemption for certain "internet advertising."[67] To qualify for the exemption, franchisors must file an annual notice of exemption with the state that includes: "(1) the Uniform Resource Locator (URL) address or similar address or device identifying the location of any Internet advertisement; (2) a statement that the franchisor, or anyone acting with the franchisor's knowledge, agrees to comply with the California Franchise Investment Law, and Rules thereunder, when posting any Internet advertisement on a Web site; and (3) the franchisor's name, address, telephone number, and contact person."[68] Also, the exemption is limited and applies only as long as the Internet advertisement is not directed to a particular prospect(s) in California. Thus, an e-mail sent to a specific person or group in California that contains a link to the franchisor's Web site would not qualify for the exemption.

To date, however, no specific regulations have addressed social media or the substance of communications exchanged in that medium. Until specific guidance is provided, practitioners should counsel to include disclosures in their Franchise Disclosure Document and on their social media pages consistent with those required of Internet advertisements.

What happens, however, if a franchisee independently publishes its financial performance on either the social media portion of the franchisor's Web site or the franchisor's social media Web pages? Will such conduct be attributed to the franchisor and taint subsequent sales? The issue has yet to be decided. One defensive measure may be to require the prospective franchisee to acknowledge in writing that it is not relying upon any such earnings claims or other franchisee-published information. This does not necessarily guarantee immunity from a subsequent rescission claim based on the posting, but may be viewed favorable by a court or regulator. To enhance the franchisor's position further, franchisors should include prohibitions against such activities in the franchisor's operations manual and consider temporarily suspending the implicated franchisee publisher from online marketing (if the operative agreements permit such remedy).

67. *See* CAL. CODE REGS. Tit. 10 § 310.156.3.

68. *Id.* Other states have also adopted similar filing exemptions for Internet advertisements. *See, e.g.,* N.Y. COMP. CODE R. & REGS., tit. 13 § 200.12; and WASH. ADMIN. CODE § 460-80-530.

V. MARKETING A BRAND ONLINE AND DRIVING TRAFFIC

Contrary to popular belief, establishing a brand online does not end with the registration of a trademark and domain name and the launch of a Web site. Those are merely prerequisites to participating on the Internet; establishing a brand online demands significantly more effort and navigation through myriad practical and legal pitfalls. Promotion of the brand commences well before consumers visit the brand Web site or its social media Web pages. Driving traffic to the Web site and social media Web pages requires deliberate strategy: managing search engine results, social networks and online forums, blogs, and other venues. Effective implementation of each of these online tools mandates the cooperation of legal and business development personnel.

A. SEARCH ENGINE MARKETING AND SEARCH ENGINE OPTIMIZATION

Search Engine Marketing (SEM) and Search Engine Optimization (SEO) are two of the most significant tools to increase the visibility of Web sites and Web pages and drive traffic. SEM is an Internet marketing strategy which includes the purchase of keywords and contextual advertising to heighten visibility of a Web site in response to pre-designated search terms.[69] Keywords are words that are used to search for information with search engines. SEO is the organic process of embedding a Web site's content with words, hyperlinks and other mechanisms to ensure the Web site appears at the top in search engine results.[70] Both of these methodologies may have legal ramifications, most prominently in the trademark area.

For example, a consumer seeking the nearest Highland Hot Dogs location types the brand name into a search engine. A link to Lowland Hot Dogs, its direct competitor, appears as the first listing in the natural search results and sponsored search results. Highland Hot Dogs, after learning of this issue, discovers that Lowland Hot Dogs purchased "Highland Hot Dogs" as a keyword with a number of search engines and embedded the competitor trademark at numerous points throughout the content of the Lowland Web site. The Highland president thereafter immediately inquires whether it has any recourse against Lowland Hot

69. *See* Rescuecom Corp. v. Google Inc., 562 F.3d 123, 125-126 (2009); *Platform-A Inc. v. Unique Vacations*, Civil Action No. 09-614, fn.1 (D. Del. Dec. 16, 2009).

70. *See* Xcentric Ventures, LLC, et al. v. Richeson, Case No. CV10-1931-PHX-NVW (D. Az. Dec. 8, 2010).

Dogs. The answer to the question is complex and, as of the date of publication, remains undecided.

1. Issues for SEM Strategies for Franchise Systems

SEM is a widely publicized search engine marketing technique involving keyword marketing.[71] The purchase of advertising in response to a user's input of keywords has now become one of the primary forms of online advertising—and it can be a powerful tool in developing a company's online presence.

Major search engines such as Google, Yahoo! and Bing allow Web site owners to purchase keywords so that when those keywords are used in a search query, the advertiser's Web site will appear at the top of the search results under a "Sponsored Links" or similar category, and in the search engine results. Keywords can include any words or phrases that a company believes would be associated with their business to draw the maximum number of users to its Web site. In describing its keyword advertising program, AdWords, Google says, "AdWords connects you with potential customers at the precise moment they're searching for your products or services."[72] It is indeed fairly impressive marketing but, as with everything else, it may be subject to overreaching in a competitive environment.

The most common form of overreaching occurs when one advertiser purchases a competitor's trademark as a keyword—which begs the question whether such conduct constitutes trademark infringement under the Lanham Act.[73] The Lanham Act establishes liability for unauthorized "use in commerce" of another's mark which is "likely to cause confusion, or to cause mistake, or to deceive . . . as to the affiliation . . . or as to the origin, sponsorship or approval of his or her goods [or] services . . . by another person." The law continues to develop, varying from circuit to circuit, addressing each element of any such claim.

Search engines—namely Google—opposed challenges to keyword advertising as a violation of the Lanham Act arguing, among other things, that a competitor's use of another's trademark as a keyword does not constitute "use in commerce." A split among the federal circuit courts ensued. The current trend recognizes that use of a trademark in keyword advertising is sufficient to demonstrate "use in commerce."[74]

The question remains open as to whether the use of a competitor's mark in a keyword search is "likely to cause confusion." In *Fair Isaac Corp. v. Experian Info.*

71. *See* Rescuecom Corp. v. Google Inc., 562 F.3d 123, 125-127 (2009).
72. For a greater explanation of Google's AdWords, see *Rescuecom Corp. v. Google Inc.*, 562 F.3d 123, 125-127(2009).
73. 15 U.S.C. §§ 1114, 1125.
74. Rescuecom Corp. v. Google, Inc., 562 F.3d 123, 130-31 (2d. Cir. 2009); Hearts On Fire Co. v. Blue Nile, Inc., 603 F. Supp. 2d 274 (D. Mass. 2009).

Solutions, Inc.,[75] the court held that the mere purchase of a competitor's mark as a keyword was insufficient to determine whether there was a likelihood of confusion, and that such a judgment would be a question of fact for the fact finder.[76] In *Designer Skin, LLC v. S & L Vitamins, Inc.*,[77] the court granted defendant summary judgment because the mere fact that a keyword search of plaintiff's trademarked name would include a link to the competitor's Web site was insufficient to prove likelihood of confusion. The state of the law continues to change, requiring a practitioner to be vigilant in monitoring developments in each circuit.

Because of the uncertainty in the law on this issue, major search engines have established trademark policies that seek to address this issue with respect to the purchase of keywords on their respective Web sites. Thus, when a competitor purchases a trademark as a keyword, the first step in evaluating legal recourse options should be consultation with the particular search engine's policies.

Take, for example, Yahoo! Sponsored Search, which expressly prohibits advertisers to bid on any keyword that is a trademark of its competitor. Yahoo!, however, makes an exception if the bidder either refers to the trademark "in a permissible nominative manner without creating a likelihood of confusion," as a reseller of the trademarked product, as a non-competitive information site, or otherwise uses the term in a generic or merely descriptive manner.

Similarly, Microsoft adCenter does not permit advertisers to bid on keywords that infringe on a third party's trademark unless the use is truthful and lawful, that either the bidder is a reseller of the goods that are distributed under the mark, the Web site provides information about goods or services represented by the trademark, or the bidder is using the "ordinary dictionary use of a term," and finally, the site does not sell a competing good.[78]

Google, on the other hand, implemented a less stringent policy. According to its published policy, if a trademark owner files a complaint with Google about the use of their trademarks in AdWords ads, Google will investigate and may enforce certain restrictions on the use of that trademark in AdWords ads and as keywords. Google will investigate and may restrict the use of a trademark within ad text, except under limited expressly excepted circumstances. These may include where: (1) the trademarks are used in ad text in compliance with the policy on resellers and informational sites in the United States, Canada, the United Kingdom, and Ireland; (2) the trademarked term is used in ad text as authorized by

75. Fair Isaac Corp. v. Experian Info. Solutions, Inc., 645 F. Supp. 2d 734 (D. Minn. 2009).
76. Fair Isaac Corp. v. Experian Info. Solutions, Inc., 645 F.Supp.2d 734, 761.
77. Designer Skin, LLC v. S & L Vitamins, Inc., 560 F. Supp. 2d 811 (D. Ariz. 2008).
78. *See*, *Editorial Guidelines: Intellectual Property*, Microsoft adCenter, http://advertise.bingads.microsoft.com/en-us/editorial-intellectual-property-guidelines.

the trademark owner; (3) the ad text uses the trademarked term descriptively in an ordinary meaning rather than in reference to a trademark; and (4) the ad is not in reference to goods or services corresponding to the trademarked item.[79]

The keyword situation is more complex for franchise systems, particularly with an increased presence of franchisees on the Internet. Unlike other companies, franchisors and franchisees need to be concerned about keyword strategies implemented by each other. While it may at first glance appear innocuous to have the franchisor and multiple franchisees each purchase keywords for the brand's trademark or other nonproprietary words, a closer look at the repercussions is more troubling.

The positioning of sponsored links is determined through a bidding process.[80] Advertisers willing to pay more for priority in the listing of sponsored links will receive a higher priority. For companies with one advertising agent, the bidding should be relatively straightforward. In a franchise system, however, there could be hundreds or thousands of franchisees bidding on the same trademarks or other keywords. This leads to an increased per-click cost—only benefiting the search engine—and it will dilute the effectiveness of keyword advertising for the entire system. The best practice dictates that the franchisor stake out the trademarks and other keywords it intends to purchase, driving traffic to the system's Web site, which, in turn, enables consumers to link to a local franchisee. This may generate two benefits: first, it will advance the interests of the brand as a whole over the interests of particular franchisees; and second, it may enhance search engine optimization for both franchisor and franchisee sites by including multiple hyperlinks.[81] Franchisees, on the other hand, should focus their keyword bidding on words particular to their specific locations, such as major nearby intersections, city buildings, or other widely recognized landmarks.

To avoid any confusion, franchisors should consider including provisions in their franchise agreements or operating manuals that expressly prohibit franchisees from bidding on keywords that contain the franchisor's trademarks and/or are not approved in advance by the franchisor.

2. Issues for SEO Strategies for Franchise Systems

Natural search results are driven by the actual content of each particular Web

79. *What is Google's AdWords and AdSense Trademark Policy?*, Google AdWords, https://support.google.com/adwordspolicy/answer/6118?hl=en.

80. *Rescuecom Corp.*, 562 F.3d at 125-127.

81. A detailed discussion about the various elements that contribute to how each search engine generates results is beyond the scope of this chapter. Hyperlinks to and from Web sites, however, may enhance the visibility of a particular Web site in search engine results.

site and its interaction with algorithms employed by the particular search engine. Historically, Web sites embedded their metadata with popular words relevant to the product or service offered on the Web site to facilitate a higher ranking in search engine results.[82] The case of *Brookfield Communications, Inc. v. West Coast Entertainment Corp.*[83] established that use of competitor trademarks as metatags (typically invisible words on a Web site) could result in trademark infringement where it was likely to result in initial interest confusion. While the *Brookfield* opinion was perhaps groundbreaking at the time, the search engine industry has moved away from reliance on metatags to drive natural search engine results and the law is well-established enough to deter most others from engaging in such conduct. The value of the *Brookfield* decision in today's Internet environment is therefore probably limited.

Nevertheless, for the reasons articulated in the *Brookfield* case discussed above, when using a competitor's trademark to drive traffic to your Web site, the best practice is to make sure that consumers understand the source of the content and Web site—even before they arrive.[84] As with SEM strategy, franchisors and franchisees are encouraged to coordinate regarding the manipulation of their metadata to ensure that each does not have a dilutive impact on the others. Indeed, the prudent course of practice for franchisors may be to set forth explicitly each party's rights and obligations regarding metadata in the franchise agreement or franchise manual.

B. ASTROTURFING AND ENDORSEMENTS

Social media has quickly become a popular methodology to spark interest in products or services and to drive traffic to particular Web sites. A branded sub-domain on a social media page is one of the more widely recognized implementations of a social media marketing strategy. Other methods involve Internet "ambassadors" or affiliates paid either for successfully driving traffic to Web sites through

82. "Metadata" is technically defined as data about data. In the Internet context, Web sites embed metadata to describe the information contained on the Web site, geographical information, creation and update chronological information and other data to facilitate further development.

83. Brookfield Commc'ns, Inc. v. W. Coast Entm't Corp., 174 F.3d 1036 (9th Cir. 1999).

84. Indeed, many circuits continue to apply the initial interest confusion test in reviewing trademark infringement claims involving keywords, metatags and other Internet search practices. *See Brookfield Communications*, 174 F.3d at 1062; Australian Gold, Inc. v. Hatfield, 436 F.3d 1228, 1239 (10th Cir. 2006); Promatek Indus., Ltd. v. Equitrac Corp., 300 F.3d 808, 812-13 (7th Cir. 2002); JR Cigar, Inc. v. GoTo.com, Inc., 437 F. Supp. 2d 273 (D.N.J. 2006). "Initial interest confusion" refers to a potential purchaser's temporary confusion about the actual source of goods or services under consideration, even where that confusion is resolved by the actual moment of sale. *Hearts on Fire Co., LLC*, 603 F. Supp. 2d at 279.

the use of what is represented to be first-hand positive experiences with the particular advertiser.

Commercial benefit from social media initially developed through genuine product reviews by actual consumers seeking to share brand experiences with other consumers. Readers reasonably believed the postings to constitute a reliable source for independent and objective product reviews. As social media proliferated, however, it became fertile ground for creative and stealthy marketing. Posts began to appear which contained overly enthusiastic statements remarkably well tuned to a brand's marketing campaigns. Almost surreal anecdotes surfaced about posting wars between dissatisfied consumers and other surprisingly defensive posters. As it turned out, many of the defensive postings were not, in fact, published by consumers, but instead were published by company employees paid to suppress negative postings with positive counter-posts.

This type of conduct is now often referred to as "astroturf marketing"—so dubbed because the aim is to create bogus grassroots buzz about a product.[85] In 2009, New York Attorney General Andrew Cuomo settled a claim resulting in a $300,000 settlement against a company engaged in astroturfing.[86] Lifestyle Lift, a medical enhancement provider, became one of the first companies to be penalized for astroturf marketing. Lifestyle Lift had required employees to pose as satisfied customers in online ads which were presented in the form of Web sites created to highlight the employees' reviews as legitimate, unsolicited testimonials.

The FTC subsequently promulgated *Guidelines Concerning the Use of Endorsements and Testimonials in Advertising,* which became effective in December 2009.[87] The guidelines focus on the use of "endorsements," which are defined to include "any advertising message . . . that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsoring advertiser." Advertisements which feature a consumer and convey his or her message with a product or service as typical when that is not the case will be required to disclose the results that consumers can generally expect clearly. The FTC guidelines also require that "material connections" between advertisers and endorsers—connections that consumers would not expect—be disclosed and, according to FTC press releases, the scope of the guidelines expressly include

85. The term was reportedly coined by Senator Lloyd Bentsen in 1985. In the August 7, 1985 edition of the Washington Post, Bentsen used the term to refer to a "mountain of cards and letters" sent to his office. The newspaper quoted Bentsen as saying "A fellow from Texas can tell the difference between grass roots and Astro Turf. . . This is generated mail." *See* Ryan Sager, *Keep Off the Astroturf*, N.Y. TIMES, August 18, 2009.

86. *See* http://www.ag.ny.gov/press-release/attorney-general-cuomo-secures-settlement-plastic-surgery-franchise-flooded-internet.

87. 16 C.F.R. pt. 255, *available at* http://www.ftc.gov/os/2009/10/091005endorsementguidesfnnotice.pdf.

messages conveyed by bloggers or other "word-of-mouth" marketers. They also include celebrity endorsers when they are making endorsements outside the context of traditional advertisements, such as on talk shows and in social media.[88]

The following are examples in which disclosures may be required:

1. Twitter/Facebook: Any poster recommending a product should disclose if he or she was compensated for publishing the post.
2. Blogs: Any receipt of complimentary products or services or other consideration should be disclosed in connection with a review.
3. Bulletin Boards: When an employee—even on his or her own volition—posts favorable comments, the nature of employment should be disclosed, even if the nature of employment does not involve marketing.

The ramifications of the new FTC guidelines are not yet entirely clear, but there is a need to police brand-sponsored social media Web pages and rein in posts by individuals with a material connection to the brand. With respect to brand-sponsored social media Web pages, companies may now be required to ensure that the pages fairly reflect the experience a consumer can reasonably expect. If there are multiple negative posts on the Web site, it is unclear whether the Web page fairly reflects the experience a consumer can expect if the negative posts are deleted without the publisher's permission. Further, for franchisors, directions not to publish any post on the Web site without a proper disclosure probably need to be conveyed not only to employees, but also to franchisees.[89] It may be worth including such a provision in franchise agreements going forward to provide evidence that any such unrestrained franchisee posts are not condoned by the brand.

Appropriate disclosures may be more problematic for users on Twitter and other social media Web sites that limit the number of characters to each post. In the case of Twitter, for example, posters are limited to 140 characters. Other mediums of communication have maximum limits of 160 characters. While 140 characters may typically be sufficient to communicate a thought, it may not be enough to convey a thought and disclose the poster's affiliation with the brand. Indeed, to comply with the FTC guidelines, it could be argued that almost the entire post must be a disclosure. Solutions to this issue vary and perhaps none

88. *Id.* These disclosures are in addition to the "public figure" disclosures required in Item 18 of a franchisor's Franchise Disclosure Document.

89. The guidelines specifically state that the FTC will take into consideration a company's efforts to comply with its own social media practice guidelines in determining whether to prosecute for violations. *See id.*

perfectly address business preferences and legal requirements. Options previously have varied from banning all posts by individuals with material connections to the brand, to requiring that affiliated posters include a tiny URL or similar service containing a clear and conspicuous disclosure of the affiliation after the jump, or otherwise using appropriate hashtags.[90] The FTC, however, continues to promulgate guidelines in 2013 that address these issues, most of which increasingly require the disclosures to be clear and conspicuous concurrent with the appearance of the endorsement or other affiliated message, and that potentially render ineffective solutions that include tiny URL and hyperlinked disclosures.[91]

C. CAN-SPAM Act and TCP Act

Driving traffic to Web sites is also commonly accomplished through e-mail and telephone marketing, but those forms of media are also not without regulation. To regulate unsolicited e-mail, Congress instituted the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003.[92] To send unsolicited marketing e-mails, the sender must include (1) an accurate subject matter; (2) the sender's physical mailing address; and (3) a hyperlink to unsubscribe. The sender must also maintain a "do not send" list and "scrub" the lists before sending any subsequent batch of marketing e-mails. The CAN-SPAM Act also applies to direct messaging on Twitter and Facebook. Remedies available for recipients of unsolicited e-mail in violation of the CAN-SPAM Act can be significant enough to make addressing the delivery of unsolicited e-mail quite cumbersome.

Congress has also taken steps to regulate text message marketing. The Federal Telephone Consumer Protection Act (TCPA) prohibits commercial text messages unless there is consent by the recipient.[93] Consent is made by either checking a box online, or sending a number to that commercial texting number. Violations of the TCPA can result in class action lawsuits with penalties in the amount of $500 per text message.

D. The Rising Popularity of QR Codes

The number of tools available to drive traffic to Web sites may become endless as innovators increasingly focus on Internet traffic software and applications. QR codes—a relatively new arrival to the U.S. marketplace (though they have been in use in Japan and South Korea for a number of years)—enable brands

90. A "tiny URL" is a service that enables a publisher to use a shorter hyperlink to send users to another Web page that has a lengthy URL.
91. *See* http://www.ftc.gov/opa/2013/03/dotcom.shtm.
92. 15 U.S.C. § 7701.
93. 47 U.S.C. § 227.

to sidestep SEO and display advertising and social media Web sites when seeking to drive consumer Web traffic. A QR code, which stands for quick response code, is essentially a two-dimensional bar code in which a design replaces the bars and numbers consumers have grown accustomed to seeing on consumer packaging. By downloading a free app to a smartphone or other mobile device with the necessary functionality, consumers can scan the QR code, which in turn, becomes the functional equivalent of a hyperlink to the device's browser. The QR code can convert traditional offline consumers into online consumers, immediately providing them with pertinent information about product features, pricing, sales, and other information.

The legal consequences of QR codes are unclear given their recent rise in popularity in the U.S. marketplace. Counsel should understand how their brands intend to implement this technology, ensuring that the appropriate measures are in place to avoid violating the applicable laws discussed elsewhere in this chapter (e.g., COPPA, FTC guidelines, etc.).

VI. TERMS OF USE, PRIVACY POLICY, AND ADA COMPLIANCE

Establishing the rules of engagement between a Web site publisher and user is a mandatory legal component for every Internet Web site. Web site publishers should take the opportunity to avail themselves of the protections afforded to them under applicable law and, where prudent and possible, obtain additional protections by way of contractual agreement with users accessing the Web site.

A. TERMS OF USE

All Web sites should contain a set of Terms of Use. The Terms of Use reflect the agreement between the company and user with respect to the user's rights to visit and interact with the Web site.[94] A comprehensive Terms of Use agreement is imperative to the Web site's ability to control proper access to the Web site, protect itself from untoward or otherwise inappropriate conduct, limit its liability, and establish the reasonable expectations of the parties with respect to one

94. *See* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248 (S.D.N.Y.2000) (where Web site's terms of use stated "by submitting this query, you agree to abide by these terms," court held "there can be no question that [the user of website] manifested its assent to be bound" by the terms of use when it electronically submitted queries to the database); Hotmail Corp. v. Van Money Pie Inc., 1998 WL 388389, *2, 6 (N.D. Cal. 1998) (granting preliminary injunction based in part on breach of "Terms of Service" agreement, to which defendants had assented).

another. Presumably, practitioners reading this chapter are at least aware of the existence of Terms of Use on Web sites, but it would not necessarily be surprising if most have not read many of those agreements or otherwise considered provisions that should be included. The need for many provisions may vary by the nature of the Web site and the dynamic of its interaction with users; however, some provisions are necessary regardless of the site's intended purpose and use.

1. Proscribed Permissible Conduct

Perhaps the most important part of the Terms of Use contains provisions addressing the scope of permitted conduct and authorized access to the Web site. Grant the user limited, nonexclusive, and revocable authorization to access the Web site for either personal or lawful business purposes. Consider also authorizing the users to hyperlink to the Web site for legitimate, nonderogatory purposes. Except for these purposes, the Terms of Use should set forth a non-exhaustive list of prohibited uses.

2. Reserving All Intellectual Property Rights

The Terms of Use should clearly state that all intellectual property rights associated with the Web site are reserved. If the Web site will involve Web 2.0 features, the Terms of Use should conspicuously state that the Web site will honor all intellectual property rights of others and grant the Web site a non-exclusive, royalty-free right to use any posted content. The Terms of Use should oblige the user to notify the Web site promptly if violations of intellectual property rights are discovered on the Web site.

3. Limitation on Liability

Liability for the operation of a Web site can come in many forms and often from some of the least expected sources. The Terms of Use should state clearly the scope of liability accepted by the Web site, if any, and explain to users that the functionality and content of the Web site are provided "as is" to the extent they are sourced from the Web site itself. Companies often also include a release of liability in the Terms of Use (including a California Civil Code Section 1542 waiver), but Web sites should be cognizant of potential limitations on such a release agreed upon in advance of use.

4. Warranties

The Terms of Use should contain warranties on behalf of the user that it is accessing the Web site solely for lawful, noncompetitive purpose, and that the Web site

shall not be used to infringe upon the rights of others, invade privacy rights, or otherwise interfere with reasonable expectations of noninterference.

5. DMCA COMPLIANCE

The Terms of Use should state the Web site's commitment to compliance with the DMCA and set forth the process which it commits to undertake in the event of receipt of a takedown notice.

6. COMPLIANCE WITH ALL LEGAL SUBPOENAS

As explained in section VII.B below, the law is quickly changing with respect to the ability of litigants to compel the production of secured social media Web pages. To the extent that a Web site includes a social media feature, companies would be well served to include a provision in the Terms of Use expressly authorizing them to produce material from individual social media pages in response to legally enforceable subpoenas.

7. GENERAL PROVISIONS

The provisions of a Terms of Use agreement should establish, in succinct terms, that they govern the nature of the relationship between the Web site and the user, and that accessing the Web site constitutes the user's consent to the terms. It should reserve the right of the Web site owner to make changes to or discontinue the Web site and the terms of use at the owner's discretion. Consider including in the Terms of Use a forum selection clause and choice of law provision, both of which have been previously enforced with respect to litigation arising out of the terms of use.[95] The relatively recent ruling in *AT&T Mobility LLC v. Concepcion*[96] has also caused many Web site operators and franchisors to consider including class arbitration waivers in the terms of use on Web sites, though the enforceability of this particular type of provision in such a context has yet to be judicially reviewed.

The importance of the explicitness of the provision becomes evident when it needs to be enforced. Not only does a violation of these provisions constitute a breach of contract, such conduct may also constitute a violation of the Computer Fraud and Abuse Act,[97] which contemplates both civil and criminal remedies. Indeed, four of the seven violations of the act are based upon accessing without

95. *See* Meier v. Midwest Recreational Clearinghouse, LLC, 2010 WL 2738921 (E.D. Cal., July 12, 2010) (enforcing forum selection clause in crankyape.com's terms of use); Krause v. Chippas, 2007 WL 4563471 (N.D. Tex. 2007) (enforcing forum selection clause in futurescom.com's terms of use).

96. AT&T Mobility LLC v. Concepcion, 131 S. Ct. 1740 (2011).

97. 18 U.S.C. § 1030, *et seq.*

authorization, or exceeding authorized access to a protected computer—including a Web site. Most significantly, the Computer Fraud and Abuse Act permits a Web site owner to "spell out explicitly what is forbidden" or not authorized access on its Web site in its Terms of Use.[98] In other words, if a user engages in conduct in violation of the Terms of Use, it has also either accessed without authorization or exceeded authorized access to the Web site.

While the Computer Fraud and Abuse Act provides a hammer to users engaged in nefarious conduct, practitioners should be circumspect in their enforcement of its provisions to be sure that the relief sought is commensurate with the violation. Practitioners have, from time to time, become overly optimistic about a court's willingness to impose the full weight of the remedies on relatively insignificant violations of the Terms of Use.

B. PRIVACY POLICY

Privacy policies govern the use of user information by a Web site owner. The nature of the business to be conducted on the site will dictate most of the substantive content required.[99] A good privacy policy should provide in plain English the following: (1) a general statement regarding your position on the use and protection of user information; (2) a description of the types of information that will be collected; (3) the methodology used to collect such information; (4) the intended uses by you of users' information; and (5) various measures that you undertake to protect users' personally identifiable information—including explanations about how users can review, change, and remove any personal, identifiable information that has been collected. The inclusion of contact information for inquiries about privacy protection and an explanation about how users are notified about changes in the privacy policy are also important.

1. LAWS APPLICABLE TO PRIVACY POLICIES

There are laws enacted to protect all types of personal information including, without limitation, information about individual financial information,[100] health information,[101] and personal identification.[102] In the United States, however, there

98. EF Cultural Travel B.V. v. Zefer Corp., 318 F.3d 58, 63 (1st Cir. 2003).

99. Also, it is beyond the scope of this book, but the laws of many foreign jurisdictions regulate privacy much more stringently than does the United States. For example, the EU Data Privacy Directive, Directive 95/46/EC, regulates the management of personal information throughout the member states. In addition, the member states each have enacted additional privacy laws.

100. *See*, e.g., Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 and Fair Credit Reporting Act, 15 U.S.C. §1681, *et seq.*

101. *See*, e.g., HIPPA privacy provisions, 45 C.F.R. 164.501.

102. CAL. CONST., art. 1, § 1; CAL. GOVERNMENT CODE § 11549.5.

are relatively few laws directly governing an Internet Web site's privacy policy. Rather, the FTC—relying on the aforementioned laws and others (many of which are mentioned elsewhere in this chapter, i.e., COPPA) generally regulates use of privacy information by enforcing these laws and promulgating its own regulations.

In 2005, California enacted its own statute directly addressing consumer rights with respect to information obtained by marketers.[103] It affords California citizens certain protections regarding restricting use of their personal information and enabling them to obtain additional facts about the use of their information. For example, the Shine the Light law provides a consumer with the right, upon request, to a list of "all third parties that received personal information from the business for the third parties' direct marketing purposes during the preceding year and, if the nature of the third parties' business cannot reasonably be determined from the third parties' name.[104]

Privacy laws in other jurisdictions are significantly different. The EU Data Privacy Directive of 1995, for example, broadly defines personal data and imposes restrictions on collecting and using consumer data.[105] A failure to implement a privacy policy under the directive may limit a Web site owner's ability to defend itself in the event of an inadvertent or negligent misuse of such material.

It goes without saying that it is generally the best practice to implement a uniform privacy policy that meets the privacy laws of all applicable jurisdictions. Doing so avoids the need for a protracted evaluation of which privacy laws apply to each particular individual and the information collected on such person.

2. Drafting Strategies for Privacy Policies

Privacy policies can be drafted to afford your company broad liberties with respect to user information (i.e., "Permissive Policies") or be drafted to limit your company's use of user information restrictively (i.e., "Restrictive Policies"). Like all Web site policies, your privacy policy should be clear and conspicuous, and users should be alerted when changes to the policy are made.

The benefit of a Permissive Policy is that it allows your company to engage in more aggressive marketing efforts to advertise your products or services and potentially generate revenue by marketing third-party products or services to your user base. In addition, as long as you adhere to Permissive Policies, they are less likely to be violated by your company. Many larger companies prefer Permissive Policies as a safeguard against aggressive and unsupervised marketing

103. Cal. Civil Code § 1798.83, referred to as the "Shine the Light" law.
104. Cal. Civil Code § 1798.83.
105. The Center for Democracy and Technology Web site maintains an easily accessible version of the law at http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

initiatives, which are more likely to occur online than offline. While regulators and plaintiff lawyers may not look favorably upon Permissive Policies, companies most likely will not have any legal issues as long as those policies do not violate applicable privacy laws.

The main drawbacks of Permissive Policies relate to public perception and user alienation. Sophisticated Web users do not want their e-mail addresses and other information sold, licensed, or rented to third parties. This information in the wrong hands leads to spam, at best, and identity theft, at worst. Many companies deal with privacy backlash often (see Facebook). These companies employ experienced privacy experts to handle privacy matters. Companies without the budget to hire knowledgeable employees or consultants run the risk of users revolting against their privacy policy and potentially, the company in general.

The benefit of a Restrictive Policy is that it may actually be a catalyst to drive Web traffic to your company's site. Companies that maintain good reputations related to safeguarding user information are often praised in the online world, thereby creating favorable press. Furthermore, complying with a Restrictive Policy usually coincides with a good user experience, which can help build a loyal customer base.

There are two main drawbacks of Restrictive Policies. First, your company will be limited in its marketing practices. Restrictions on how your company uses personal information of your customers may keep your company from realizing third-party revenue opportunities and may even restrict your company from marketing your own products to your user base in certain ways. Second, your company is more likely to violate a Restrictive Policy, which may lead to lawsuits, consumer complaints, and/or regulatory scrutiny.

The decision to post a Permissive Policy or a Restrictive Policy really comes down to what type of online business your company is trying to build. A typical brand site where users can visit to gain product or service information is probably best served using a Restrictive Policy. A typical e-commerce site where users interact and purchase products and services is most likely best served using a Permissive Policy.

C. ADA Compliance

It is not unusual to see lawsuits against brick and mortar retail locations for violations of the Americans with Disabilities Act (ADA). The ADA and the attendant litigation, however, may not be limited to those locations. Web sites which are accessible to fully abled individuals may not be accessible to people with disabilities. Drop-down menus may not be viewable by individuals with blindness,

low vision, or other learning disabilities, and streaming audio feeds may be inaccessible to deaf people.

The federal circuit courts are split on whether public accommodations must be physical places or, alternatively, can include Internet Web sites. Courts which hold that Web sites fall within the scope of the ADA include *Doe v. Mutual of Omaha Ins. Co*.[106] More recently, the Northern District of California held that Web sites constitute "public accommodations," which must be accessible to the disabled in *National Federation of the Blind v. Target*.[107] Other courts have held to the contrary, finding that the term "public accommodations" is limited to physical places.[108]

Despite the split in authority, the best practice is to ensure Web sites are, in fact, compliant with ADA mandates. For instructive insight, refer to the government's own directives for making Web sites accessible to the disabled.[109] Addressing these needs does not typically require an expensive or massive Web site overhaul. Some simple steps should be able to address most, if not all, of the issues. Technology personnel are better equipped to make the necessary changes, but counsel are presumably more attuned to the features which may not be accessible by all individuals with disabilities.

To identify the portions of the Web site which may not be ADA compliant, many organizations for the disabled recommend viewing the Web site with a text-based Internet browser (eliminating all of the frames, fonts, and graphics). If all of the links are not visible, then programs which assist the disabled in viewing the Internet will not be able to navigate the Web site fully. Other features to focus on include pdfs (which most screen readers cannot read) and video streaming without subtitles. Most social media Web sites have ADA capabilities as well, and as a secondary benefit, the steps necessary for compliance are also known to affect search engine optimization favorably. Regarding the coordination of compliance with franchisees, most franchise agreements already require compliance with the ADA which, in turn, embeds in the pre-existing relationship an obligation to ensure that Internet media is accessible to the disabled.

Nevertheless, the majority of the general public (including most franchisees) is not aware of the potential implications of the ADA on Web sites, and prudent franchisors may therefore choose to address the issue explicitly in their franchise agreement or operations manual.

106. Doe v. Mut. of Omaha Ins. Co., 179 F.3d 557, 559 (7th Cir. 1999).
107. Nat'l Fed'n of the Blind v. Target, 452 F. Supp. 2d 946 (N.D. Cal. 2006).
108. Parker v. Metropolitan Life Ins. Co., 121 F.3d 1006, 1014 (6th Cir. 1997); Weyer v. Twentieth Century Fox Film Corp., 198 F.3d 1104, 1114 (9th Cir. 2000).
109. *See* Rehabilitation Act of 1973, 29 U.S.C. § 701, *et seq.*

VII. LITIGATION ISSUES WITH THE INTERNET AND SOCIAL MEDIA

A. Managing Franchisor-provided E-mail Accounts

Many franchise systems offer each franchisee one or more e-mail accounts with the brand's primary domain name, e.g., joe.marketing@brandname.com. These may be used for quality assurance reporting, marketing, intra-system business, or any other stated purpose.

The franchise agreement or franchise manual should contain provisions which address the franchisor's rights, if any, to access or terminate the account, as well as address the scope of the account user's expectations of privacy, if any. The knee-jerk response by the franchisor may be simply to retain unrestricted access to the e-mail account, thereby eviscerating any expectation by privacy by the user. However, such a policy may have an adverse impact to the franchisor, depending on the purpose fulfilled by the account. Assume, for example, the e-mail account receives a particular franchisee's complaints from employees and customers, including repeated e-mails which contain complaints by an employee about disturbing sexual advances made by a particular store manager. Attorneys representing the complaining employee may be quick to argue that the franchisor is directly and/or vicariously liable for the manager's conduct because the franchisor had notice of the issue and, under inopportune circumstances, an obligation to ensure such conduct was discontinued.[110] More moderated rights to access the account may best serve all parties' interests.

The United States Supreme Court has lightly weighed in on this issue in the context of employer-provided e-mail accounts to employees.[111] The Court addressed, in part, whether the city maintained the right to review text messages sent on

110. *See, e.g.*, Myers v. Garfield & Johnson Enters., Inc., 679 F. Supp. 2d 598 (E.D. Pa. 2010), and Awuah v. Coverall N. Am., Inc., 707 F. Supp. 2d 80 (D. Mass. 2010). Although these cases do not directly address the issue of a franchisor's vicarious liability due to e-mail communications, they do provide examples of the seemingly increasing willingness of courts to consider vicarious liability arguments raised by franchisee employees. For example, the issue in *Myers* was whether a franchisor can be liable under federal law for sexual harassment of a franchisee's employee allegedly perpetrated by the franchisee's managers. The employee alleged that the franchisor required the franchisee's employees to undergo training by the franchisor, and required the franchisee to implement certain personnel policies and implement a code of conduct applicable to franchisees' employees. The court determined that these allegations were sufficient to establish a potential joint employer relationship and sufficient to assert discrimination claims based on vicarious liability. Imagine that the employee could also argue that the franchisor had prior knowledge of the alleged discrimination by way of a prescribed e-mail account or other internal communication system used to monitor franchisees and their employees. These facts may bolster employees' claims against the franchisor.

111. City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

police officers' city-issued pagers when the city's computer usage, Internet, and e-mail policy advised the officers that they had no expectation of privacy. In reversing the Ninth Circuit, the Court concluded that the city did not violate the officers' Fourth Amendment rights because the search was reasonable, was motivated by a legitimate work-related purpose, and was not excessive in scope.

The issues involving employers accessing employee work e-mail and other electronic communication accounts is far from settled, making the landscape for franchisor-provided e-mail accounts to franchisees even less so. The best practice includes implementing a policy that allows for the franchisee to use the e-mail account for legitimate business purposes, but also permits the franchisor to access the account when necessary to protect the integrity of the brand and to comply with lawful subpoenas. Such a policy should provide the franchisee with a meaningful e-mail account and provide the franchisor with a reasonably narrow basis to access the account. In addition, under such provisions, it may be more difficult for third-party counsel to argue the franchisor had knowledge of contents of e-mailed complaints if it did not have another independent basis to suspect the existence of the e-mails in the account. Franchisors should also consider requiring their franchisees to use a disclosure as part of every message sent from the account that includes the standard "independently owned and operated franchised business."

B. SUBPOENAS FOR INFORMATION ON SOCIAL MEDIA WEB PAGES

Since their advent, social media Web sites have uniformly cited the Stored Communications Act[112] (SCA) to support their opposition to motions to compel compliance with subpoenas seeking the production of the contents published by a particular social media participant. The SCA, enacted in 1986, prevents the disclosure of private communications without authorization. For litigants, this has proven frustrating as parties have been able to cloak their private communications with the SCA's protections.

The law is now in a state of flux, with recent developments arguably going in opposite directions. The Central District of California, in *Crispin v. Christian Audigier, Inc.*,[113] granted in part motions to quash subpoenas by Facebook and Myspace. The court held that the SCA applied to social media Web sites and, therefore, protected from disclosure messages that are not publicly available. On the other hand, a New York trial court, in *Romano v. Steelcase*,[114] focused on

112. 18 U.S.C. § 2701, *et seq.*
113. Crispin v. Christian Audigier, Inc., 2010 WL 2293238, at *3 (C.D. Cal. May 26, 2010).
114. Romano v. Steelcase, 907 N.Y.S.2d 650 (Sept. 21, 2010).

the privacy concerns raised by the plaintiff in a personal injury lawsuit when it issued an order compelling the plaintiff to produce both the public and private content of her Facebook and MySpace Web pages.[115] In reaching its decision, the court observed that the public portions of the plaintiff's social media Web pages already contained information that contradicted her claim and held it to be inequitable to permit her now to conceal her private messages. The court stated that it "not only would go against the liberal discovery policies of New York favoring pretrial disclosure, but would condone Plaintiff's attempt to hide relevant information behind self-regulated privacy settings."[116]

There are a few important takeaways from these decisions. First, if a Web site contains social media features with account numbers and privacy settings, be prepared to understand the scope of obligations in responding to subpoenas to avoid violations of the SCA. Second, if the need arises to seek content from a social media Web site, the best practice would be to direct the subpoena to the account holder, not the Web site itself. If there remains a need to serve the Web site with the subpoena, review each site's policies and procedures for subpoenas.[117] Third, understand the difference in utilities between hold notices and subpoenas. The SCA may prohibit social media Web sites from producing certain information in response to a subpoena, but the SCA does not prevent the same social media Web sites from taking steps to comply with a document hold notice.

VIII. INTERNET AND SOCIAL MEDIA POLICIES: INTEGRATING THE INTERNET AND SOCIAL MEDIA INTO THE FRANCHISE RELATIONSHIP

To date, the majority of the franchise community has responded with some degree of fear to the growing force of Internet and social media and the potential ramifications associated with franchisee participation. The fear is driven by insecurity about what can happen due to the high-speed dissemination of postings once published. While exercising caution in authorizing franchisee use of social media is prudent, imposing wholesale bans may materially hinder the brand and the franchisees. The best practice is to embrace social media as another form of

115. Importantly, the court did not need to address the SCA because the subpoena was served on the account holder, not the social media Web site.

116. *See In re* Facebook, Inc., C 12-80171 LHK PSG, 2012 WL 7071331 (N.D. Cal. Sept. 20, 2012) (quashing subpoena seeking deceased family member's social media Web site from Facebook based on protections of the Stored Communications Act).

117. *See*, *e.g.*, https://www.facebook.com/help/ and then input "subpoenas" to obtain the most recent information.

marketing and impose limitations on use to the extent necessary to protect the brand.

First, establish rules on domain names and social media Web site addresses that franchisees may be permitted to register. The franchisor may consider allowing use of the trademark in the address so long as it is affiliated with the franchisee's city, street, neighborhood or other geographic region or, alternatively, is associated with the franchisee's company name. Depending on the nature of the franchise, this may be accomplished in the franchise agreement, the marketing manual, or the operations manual.

Second, establish restrictions on the nature of franchisee-published posts on its own social media pages as well the company's. It may be prudent to prohibit the posting of earnings claims and other specific and material information that may be of interest to a prospective franchisee, and the disclosure of which may be regulated by the FTC Rule or other state franchise investment laws. In addition, with respect to other content about the brand, make sure the franchisee (and any of its agents) readily understands that social media posts about the brand must contain a disclosure that the post was published by a brand franchisee that operates an independently owned and operated franchised business. Examples of potentially problematic posts may include a franchisee (or its employee) publishing posts on its Web site or elsewhere, which contains a rave review of the brand, a particular product or service, or promotion. Perhaps more troubling, the same individual publishes such a post that also falsely compares it to a competitor's products or services.

Third, consider requiring the franchisee to police its Web site not only for inappropriate material, but also for negative feedback regarding consumer experiences. This is an excellent opportunity to reach out to consumers who have had an underwhelming experience with the brand and try to recover them. In addition, it is not implausible that a consumer who describes a negative experience on the social media page will also describe the subsequent positive experience which, in turn, will mitigate the sting of the initial post. Thus, franchisors may consider even requiring franchisees to respond actively to each negative post.

Fourth, include an acknowledgment with the franchisee that the franchisor shall be assigned the domain name and/or social media addresses upon termination of the franchise agreement. In addition, the franchisor should consider including a right to instruct the franchisee to shut down the Web site and/or social media pages if the content contains inappropriate conduct or otherwise reflects poorly upon the integrity of the brand.

Fifth, franchisees should identify their Web sites as associated with independent franchisees and should be cautious about how they maintain their Web site.

Negative feedback published where your most loyal customers look can hurt the brand. As much as there is a desire to delete the genuine negative posts, doing so may result in consumer backlash and run afoul of FTC regulations.

While all of these suggested provisions may be helpful, the franchisor should proceed cautiously regarding how far it goes with respect to the franchisee's use of the domain name and/or social media page. First and foremost, the franchisor should not extend its control so far as to expose itself to vicarious liability for the franchisee's conduct. Second, the franchisor needs to be circumspect regarding its limitations to ensure that it does not interfere with the rights of franchisees to associate in violation of various franchise relations acts.

IX. PREPARING FOR WEB 3.0

It is difficult to prepare for events whose timing and outcomes are unpredictable. Web 3.0 is similarly difficult to prepare for, though limited definition and manifestation already exist. In one anticipated format particularly relevant to franchising, Web 3.0 is expected to be the ultimate combination of personal information management, social media, and search engine technology. Perhaps litigators have heard the phrase "the lancet is to be preferred over the sledgehammer" in the context of permissible litigation discovery strategies. Web 3.0 is destined to become the ultimate personal lancet for surfing the Internet—replacing the current sledgehammer approach to Internet searches.

Imagine, for example, planning a day of running personal errands, which requires the identification of places to eat and to stay overnight on a trip to the city, purchase gasoline, replace tires, and frame photographs. With Web 2.0, planning may require a series of fifteen or twenty separate keyword queries to a search engine to identify each potential stop and to obtain reviews or additional consumer feedback. Web 3.0, on the other hand, may only require one query, which will provide results based on the individual user's personal preferences and feedback from others with similar user preferences.

Such developments could cause local marketing to supplant global branding online substantially. A series of negative feedback about a particular location could wipe the remainder of brand marketing from personalized search results, making quality assurance all the more important. Other outcomes could mandate additional coordination of online marketing and co-locating of complementary vendors or service providers. Pervasive use of machine-readable technology—also contemplated as part of Web 3.0—may favor certain brands over others unless compensating technologies are implemented.

The possibilities are endless but the potential effects are already palpable. Web 3.0 has the potential to accentuate or undermine brand recognition and consumer experiences. Unless they stay current on technological developments and the legal governance regarding their implementation, legal practitioners may be ill-equipped to assist brands as they seek to maintain and enhance their online presence.