PROTECTING THE FRANCHISE BRAND
IN THE AGE OF SOCIAL MEDIA

Corby C. Anderson
McGuire Woods LLP, Charlotte, North Carolina

and

Carol Anne Been
Sonnenschein Nath & Rosenthal LLP, Chicago, Illinois

October 13 - 15, 2010
The Hotel Del Coronado
San Diego, CA

©2010 American Bar Association
<table>
<thead>
<tr>
<th>I. OVERVIEW</th>
<th>..........................................................</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Social Media Platforms</td>
<td>..........................................................</td>
<td>2</td>
</tr>
<tr>
<td>B. Integrating Social Media into a Business</td>
<td>..........................................................</td>
<td>2</td>
</tr>
<tr>
<td>II. ADVERTISING ISSUES</td>
<td>..................................................................</td>
<td>3</td>
</tr>
<tr>
<td>A. FTC ‘Rules of the Road’ for Advertising on the Internet</td>
<td>..........................................................</td>
<td>4</td>
</tr>
<tr>
<td>B. Endorsements and Testimonials: The New FTC Guides</td>
<td>..........................................................</td>
<td>4</td>
</tr>
<tr>
<td>C. User-Generated Content</td>
<td>..........................................................</td>
<td>7</td>
</tr>
<tr>
<td>D. Dealing with Brand Crises Stemming from Social Media</td>
<td>..........................................................</td>
<td>12</td>
</tr>
<tr>
<td>E. Platform-Specific Terms and Conditions</td>
<td>..........................................................</td>
<td>14</td>
</tr>
<tr>
<td>F. Practice Tips</td>
<td>..................................................................</td>
<td>15</td>
</tr>
<tr>
<td>III. PRIVACY IN SOCIAL MEDIA</td>
<td>..........................................................</td>
<td>16</td>
</tr>
<tr>
<td>A. Behavioral Advertising</td>
<td>..........................................................</td>
<td>17</td>
</tr>
<tr>
<td>B. Contextual Advertising</td>
<td>..........................................................</td>
<td>19</td>
</tr>
<tr>
<td>C. Aggregate and Anonymized Data</td>
<td>..........................................................</td>
<td>19</td>
</tr>
<tr>
<td>D. Privacy Actions Against Social Media</td>
<td>..........................................................</td>
<td>20</td>
</tr>
<tr>
<td>E. State Privacy Statutes</td>
<td>..........................................................</td>
<td>21</td>
</tr>
<tr>
<td>F. CAN-SPAM Regulation of Outbound Commercial Email Messages</td>
<td>..........................................................</td>
<td>21</td>
</tr>
<tr>
<td>G. Privacy of Children Under 13 Years Old (COPPA)</td>
<td>..........................................................</td>
<td>23</td>
</tr>
<tr>
<td>H. Practice Tips</td>
<td>..................................................................</td>
<td>25</td>
</tr>
<tr>
<td>IV. DEFAMATION AND DISPARAGEMENT IN USER GENERATED CONTENT</td>
<td>..........................................................</td>
<td>26</td>
</tr>
<tr>
<td>A. Defamation and Product Disparagement Claims</td>
<td>..........................................................</td>
<td>26</td>
</tr>
<tr>
<td>B. The CDA’s Safe Harbor Provision for UGC</td>
<td>..........................................................</td>
<td>27</td>
</tr>
<tr>
<td>C. CDA Immunity Not Granted to Quiznos</td>
<td>..........................................................</td>
<td>29</td>
</tr>
<tr>
<td>D. Defamation Liability for Statements by Employees</td>
<td>..........................................................</td>
<td>29</td>
</tr>
<tr>
<td>E. Defamation Liability of Consumers</td>
<td>..........................................................</td>
<td>31</td>
</tr>
<tr>
<td>F. Review, Rating Sites Generate Claims from Defamation to Extortion</td>
<td>..........................................................</td>
<td>31</td>
</tr>
<tr>
<td>G. Terms of Use</td>
<td>..................................................................</td>
<td>33</td>
</tr>
<tr>
<td>H. Practice Tips</td>
<td>..................................................................</td>
<td>34</td>
</tr>
<tr>
<td>V. COPYRIGHT INFRINGEMENT CLAIMS FOR USER GENERATED CONTENT</td>
<td>..........................................................</td>
<td>35</td>
</tr>
<tr>
<td>A. DMCA Section 512 Takedown Demands</td>
<td>..........................................................</td>
<td>35</td>
</tr>
<tr>
<td>B. Compliance with DMCA to Benefit from Safe Harbor</td>
<td>..........................................................</td>
<td>37</td>
</tr>
<tr>
<td>C. Practice Tips</td>
<td>..................................................................</td>
<td>39</td>
</tr>
<tr>
<td>VI. TRADEMARK INFRINGEMENT IN SOCIAL MEDIA</td>
<td>..........................................................</td>
<td>39</td>
</tr>
<tr>
<td>A. Contributory Infringement for Counterfeit Goods Posted by Users</td>
<td>..........................................................</td>
<td>39</td>
</tr>
<tr>
<td>B. Infringement in Entertainment Software (Computer Games)</td>
<td>..........................................................</td>
<td>40</td>
</tr>
</tbody>
</table>
VII. INFORMATION DISCLOSURE THROUGH SOCIAL MEDIA ........................................ 44
   A. Employee Disclosure of Business Secrets ...................................................... 44
   B. Social Media Sites that Request Disclosure of Proprietary or
      Commercially Sensitive Information .......................................................... 45
   C. Disclosures in Violation of Specific Laws .................................................... 45
   D. Anonymous Postings ............................................................................... 46
   E. Discoverability of Electronically Stored Information .................................... 47
   F. Practice Tips ............................................................................................. 48

VIII. EXAMPLES OF INTERNATIONAL CONCERNS .................................................... 48
   A. How Social Media Platforms Deal with Different Laws ................................ 49
   B. The European Union: Privacy Is Paramount .......................................... 49
   C. Asia: Penalties Stiffer for Online Offenses than for Offline Offenses .......... 50
   D. Practice Tips ............................................................................................. 51

IX. FRANCHISE ISSUES .......................................................................................... 51
   A. Establishing a Policy and a Code of Online Conduct ................................. 51
   B. Using Social Media for Franchise Sales .................................................... 53

X. CONCLUSION .................................................................................................... 54

Appendix A - SOCIAL MEDIA PLATFORMS
I. OVERVIEW

In a YouTube video of a business executive taking a sledgehammer to a Tiffany-style lamp, franchisor Ruby Tuesday invited viewers to watch it blow up the chain’s last old-style restaurant “live, August 5 at 3 p.m. EST” by visiting www.rubytuesday.com. The demolition was billed as a graphic demonstration of the chain’s commitment to changing its brand. Those who visited the website at the appointed time saw video footage of a crowd across the street from a Ruby Tuesday in Mount Holly, Ohio, looking on in shock as a blast went off and a restaurant was indeed reduced to a pile of rubble and a cloud of dust – but the restaurant was Cheeky’s Bar and Grill, next door to Ruby Tuesday.

The video footage popped up on YouTube, and the press began to cover it. Ruby Tuesday then aired a national television commercial apologizing to Cheeky’s Bar and Grill for the error, with Ruby Tuesday’s senior vice president for marketing explaining: “We had intended to blow up our own restaurant, to mark our departure from the sea of sameness in the casual dining industry. Ironically, the demolition crew mistook Cheeky’s for the last of our old restaurants.” Of course, the video was a hoax. And for Ruby Tuesday, the hoax was a success, by any measure. The advertising agency that staged the 2008 campaign reported the numbers: 1,016,100 visitors to the Ruby Tuesday website (up 300 percent); 20,000 new Ruby Tuesday email club members; a three-point increase in sales; a 25.15-percent increase in stock price; and 365,000,000 PR impressions – all in one week.

This story illustrates the power of social media to benefit a company’s brand. Of course, other companies may have equally compelling stories about the damage inflicted on their brands through social media. Such stories have become not only famous, but infamous: The rogue restaurant employees who posted a YouTube video of one of them doing terrible things to a pizza intended, they said, for a customer. The airline passenger who became a cause célèbre on the internet after Tweeting of how the airline ordered him off the plane for being too large. The woman driven to the point of sleeping with a machete by her bed (and filing a $10 million lawsuit for her psychic scars) by a car company’s PR campaign allowing people to set friends up for pranks in which an actor stalked them with emails, text messages, and phone calls.

As these examples show, social media can offer significant rewards and significant risks. Yet many companies lack a basic understanding of what social media is and how they can use it as a tool to promote and protect their brands. Toward that end, this paper will:

• Provide a brief overview of social media platforms and how they can be integrated into a business;

---

3 BooneOakley.com – Ruby Tuesday, http://www.youtube.com/watch?v=BA5ik9b4C8 (last visited July 26, 2010).
• Outline the basic laws and regulations that govern use of social media in the areas of advertising, privacy, defamation and product disparagement, copyright and trademark infringement, and information disclosure (concluding with practice tips for each of these substantive areas);

• Touch on a few of the international concerns involved with social media, stemming from the borderless nature of the internet; and

• Examine issues specific to franchisors and franchisees, including policies for the system’s use of social media with consumers and special considerations for franchisors’ use of social media in connection with franchise sales.

A. Social Media Platforms

In a nutshell, “social media” is a network of services that let people communicate online and form communities around shared interests and experiences. Users of social media typically are both creators and users of content. As one expert has stated: “Social media is, at its most basic sense, a shift in how people discover, read, and share news and information and content. It’s a fusion of sociology and technology, transforming monologue (one to many) into dialog (many to many).”

The primary forms of social media are discussed in detail at Attachment A.

B. Integrating Social Media into a Business

With so many social media platforms available, how does a company decide which ones to use? In choosing where to establish a presence, companies should consider what they want to accomplish through social media and which sites have cultures and audiences that are compatible with their brands.

Social media can be used for many purposes, including: providing broad exposure for a company’s brand; engaging consumers in a conversation; informing consumers about sales, new developments in products and services, tips, and breaking news; driving consumers to other marketing channels; improving a company’s knowledge of its markets and exposing it to different ideas; testing products, services, or concepts and getting feedback about them; building loyalty among existing customers and attracting new customers; helping to “start fires,” by generating buzz about a product or service; and helping to “put out fires,” by responding early and proactively to PR crises in the making.

In deciding which social media platforms to use to reach a target audience, a company first must understand where that target audience is connecting online. A recent campaign by Burger King illustrates this “know where your audience connects” principle in action. Burger King wanted a social media campaign for increasing its breakfast business in the United Kingdom. As a Burger King spokesperson explained, “Our research showed that breakfast is a male-centric audience for Burger King; it doesn’t resonate as well with women -- we are

---


targeting the people who are buying breakfast.” So Burger King created a “microsite,”
singingintheshower.co.uk, featuring a model in the role of “the shower babe.” It invited
consumers to visit the site every morning at 9:30 to “watch the shower babe shake her bits to
the hits.” Visitors to the site could also vote on which song the model sings and which bikini
she wears in the shower, enter a contest to win a date with her, and download coupons.

The most effective users of social media are those who have a well thought out strategy
that integrates social media with all other forms of marketing that they undertake. For example,
a video posted on YouTube may invite viewers to the company’s website. The website may
offer coupons redeemable at a store. The store may use point-of-sale advertising to invite
visitors to blog about a new product purchased there. Traditional advertising media, such as
radio and television spots, and even news media may fit into the strategy. (In the PR campaign
discussed above for Ruby Tuesday, for example, website and YouTube efforts were integrated
with a television commercial, and the campaign attracted news coverage as well.)

Companies should also take an integrated approach to social media in their internal
operations. Launching and maintaining a social media campaign should involve a broader
segment of the company than marketing. It should also involve information technology, sales,
legal, communications, and human resource departments.

Finally, companies using social media generally must meet all of the legal and regulatory
requirements that govern regular media - although a few notable exceptions exist for statutory
safe harbors. These requirements are discussed in detail in Sections IV and V below.

II. ADVERTISING ISSUES

In the era of social media, advertising is no longer a one-way communication, in which
brand owners craft a message, create advertising content, and convey it to consumers. Today,
social media platforms empower consumers to participate in shaping brands by telling
companies what they want and don’t want, creating advertising content (known as user-
generated content, or “UGC”), sharing their experiences and opinions about products and
services, and acting as “brand ambassadors,” whose communications often carry more weight
with other consumers than the messages that originate with the company itself, or occasionally
as “brand bashers.”

The benefits to companies from social media advertising are clear: They can reach
huge numbers of current and prospective customers almost immediately, and for relatively low
cost, with information about their products and services. And because social media platforms
are interactive, they can be used to get information and feedback from consumers and to build
relationships with them, generating brand loyalty. The potential challenges are also clear:
Because the companies are not the only ones doing the talking, they have less control over
what is said about their products and services, increasing both the business risks and the legal
risks. Moreover, when a business starts a social media campaign, it is starting a relationship

---

7 Stephanie Startz, Burger King’s Shower Girl Still Serving Up Breakfast, BRAND CHANNEL, Dec. 18, 2009,
8 Id.
9 Franchisors also use social media for identifying and marketing to prospective franchisees. An in-depth
discussion of this topic is beyond the scope of this paper, but the legal implications of using social media in
connection with franchise sales are discussed briefly in Section IX.B. below.
with its customers. And relationships, as we all know, take time. Establishing a presence on social media platforms is only the first step – it must be followed by listening to the audience created, responding, and maintaining a steady supply of real-time, informative content.

A. FTC ‘Rules of the Road’ for Advertising on the Internet

The Federal Trade Commission Act\textsuperscript{10} authorizes the FTC to take enforcement action against deceptive and unfair advertising in any medium. According to the FTC’s \textit{Rules of the Road for Advertising and Marketing on the Internet},\textsuperscript{11} advertising is “deceptive” if it is likely to mislead consumers and affect their behavior or decisions about a product or service. An act is “unfair” if the injury it causes, or is likely to cause, is substantial, not outweighed by other benefits, and not reasonably avoidable. An advertising claim can be misleading if it omits relevant information or implies something that is not true. Claims also must be substantiated, especially when they concern health, safety, or performance.

The FTC points out that not only sellers, but third parties acting on their behalf, may be liable for making or disseminating deceptive representations if they participate in preparing or distributing the advertising or know about the deceptive claims. Creators of UGC, such as entrants in contests to create video ads for products, seemingly would be third parties for this purpose. But the Rules of the Road, issued in September 2000, before the advent of social media and UGC, do not address this point.

The FTC’s guide on \textit{Dot Com Disclosures, Information About Online Advertising},\textsuperscript{12} also makes clear that the same consumer protection laws that apply to commercial activities in other media apply online. The FTC Act’s prohibition on unfair or deceptive acts or practices encompasses internet advertising, marketing, and sales. As the Commission acknowledged: “Many of the general principles of advertising law apply to online ads, but new issues arise almost as fast as technology develops. The FTC will continue to evaluate online advertising, using traditional criteria, while recognizing the uniqueness of the new medium.”\textsuperscript{13}

B. Endorsements and Testimonials: The New FTC Guides

The FTC made a start in acknowledging social media in October 2009 by revising its \textit{Guides Concerning the Use of Endorsements and Testimonials in Advertising} (the “FTC Guides”)\textsuperscript{14}, in part to clarify their application to “new media,” including blogs, message boards, street teams, and other social media platforms. The revisions to the FTC Guides – the first since 1980 – became effective in December 2009.

\textsuperscript{13} Id. at 17.
\textsuperscript{14} 16 C.F.R. § 255 (2009), available at http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=3960bb237fe4e26e00a15221a202acf&rgn=div5&view=text&node=16:1.0.1.2.22&idno=16. The FTC Guides are “administrative interpretations of the law” providing the basis for voluntary compliance. But the FTC may bring an enforcement action against advertisements that violate the Act’s prohibition on unfair or deceptive acts or practices.
The central theme to the revisions in the FTC Guides is transparency. “Material connections” between the endorser and the seller of an advertised product or service that are unclear or unexpected to consumers must be disclosed. This disclosure requirement is aimed at the types of connections between the seller and the endorser that could affect the credibility consumers give to the endorser’s statements. Examples of such material connections include the receipt of money, free or loaner products or services, in-kind gifts, and special access privileges, as well as employment relationships.

The FTC Guides define an “endorsement” as “any advertising message that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsoring advertiser.” If the speaker is acting on behalf of an advertiser or its agent, rather than acting independently, then the speaker’s statement is an endorsement. The FTC Guides offer a number of examples to illustrate what constitutes an endorsement when a message is conveyed by “word of mouth” marketers using various social media:

- **Bloggers:** If a manufacturer of a newly released video game system sends a free copy of the system to a college student known as a video game expert and asks him to write about it on his blog, the blogger should clearly and conspicuously disclose that he received the gaming system at no charge from the manufacturer. The manufacturer should advise the student, when it sends him the gaming system, that this connection should be disclosed, and the manufacturer should monitor his postings for compliance.

- **“Street team” participants:** If people sign up to be part of a “street team” program that awards points redeemable for prizes each time a member discusses an advertiser’s products with a friend, these incentives should be clearly and conspicuously disclosed, and the advertiser should take steps to ensure that these disclosures are being provided.

- **Employees:** If an employee of a leading manufacturer of playback devices posts messages promoting the manufacturer’s product on an online message board for discussions of new music download technology, frequented by MP3 player enthusiasts, the poster should clearly and conspicuously disclose her relationship to the manufacturer.

As the FTC acknowledges, bloggers and others who speak about products in the context of social media may be subject to different (and more stringent) disclosure requirements than those who speak about them in traditional media. The FTC states that one factor it will consider in determining whether disclosure is necessary is the type of medium used to disseminate an endorsement, and “whether or not the nature of that medium is such that consumers are likely to recognize the statement as an advertisement (that is, sponsored speech).”

The FTC Guides make clear that advertisers are subject to liability for false or unsubstantiated statements made through endorsements, even if they lack control over the

---

15 Id. at § 255.0(b).

endorsements. “[I]f the advertiser initiated the process that led to these endorsements being made . . . it potentially is liable for misleading statements made by those consumers.”

Endorsers also may be liable for statements made in the course of their endorsements. To illustrate, the FTC Guides cited an example in the social media context involving an advertiser that participates in a blog advertising service, which matches up advertisers with bloggers who will promote the advertiser’s products on their personal blogs. In the FTC’s example, the advertiser asked a blogger to try a new body lotion and write a review of the product on her blog. The advertiser made no specific claims about the lotion’s ability to cure skin conditions, and the blogger did not ask the advertiser about substantiation for any such claims. Nevertheless, in her blog, she wrote that the lotion cures eczema and recommended the product to her blog readers who suffer from eczema.

In that case, the FTC stated, both the advertiser and the endorser would be subject to liability for misleading or unsubstantiated representations made through the blogger’s endorsement. The blogger also would be liable if she failed to disclose clearly and conspicuously that she is paid for her services. The advertiser should also monitor bloggers paid to promote its products and take steps necessary to halt the continued publication of deceptive representations when they are discovered, the FTC stated. Responding to concerns that consumers would not feel free to speak out about products, the FTC clarified that its enforcement activities “will continue to focus on advertisers,” not on consumer endorsers.

The FTC Guides state that celebrities also must disclose their relationships with advertisers when making endorsements outside the context of traditional advertisements, such as on social media. This includes the popular media of celebrity blogs and Twitter. The advertiser has a duty to inform the celebrity that disclosure is necessary.

The fact that “Tweets” are limited to 140 characters will not permit endorsers to avoid complying with disclosure obligations. The Word of Mouth Marketing Association has issued guidelines, discussed in Section 2 below, suggesting the use of hashtags for this purpose: #spon for sponsored Tweets, #paid for paid Tweets, and #samp for having received a sample.

1. FTC Closes Its First Investigation Under the New Guides

The FTC in April 2010 completed its first investigation under the revised FTC Guides, focused on the disclosure of gifts to bloggers. In that case, retailer Ann Taylor LOFT promoted a January fashion preview to bloggers with a notice stating that: “Bloggers who attend will receive a special gift, and those who post coverage from the event will be entered in a mystery gift card drawing where you can win up to $500 at LOFT!” To participate in the drawing, bloggers had to send Ann Taylor LOFT’s publicist a link to their posts within 24 hours; the publicist then announced the value of the gift card they had won. Bloggers’ posts were almost uniformly positive. Some disclosed the gift card, but others did not.

The FTC’s Division of Advertising Practices investigated but declined to take any enforcement action against Ann Taylor LOFT. In explaining its decision, the FTC noted that the

17 Id. At 14-15.
18 Id. at 39, n. 79.
company had posted a sign at the preview telling bloggers they should disclose the gift if they posted comments about the event. The FTC also noted that the company had subsequently adopted a written policy that it would not issue any gift to any blogger without first informing the blogger that the gift must be disclosed in the blog. The FTC said it expects the store to honor that policy and to “take reasonable steps to monitor bloggers’ compliance with the obligation to disclose gifts they receive from LOFT.”  The FTC concluded by reserving the right to take further action if deemed necessary.

2. WOMMA, DMA Issues Guides

At least two industry groups have attempted to provide guidelines about how to make the disclosures required by the FTC Guides. In February 2010, the Word of Mouth Marketing Association (“WOMMA”) released a Social Media Marketing Disclosure Guide. The WOMMA Guide provides sample disclosures for messages on blogs, online discussions, microblogs such as Twitter, and status updates on social networks, among other forms of communication.

In January 2010, the Direct Marketing Association announced changes to its Guidelines for Ethical Business Practice for endorsements and testimonials that apply to social media. Among other things, the new guidelines require marketers to disclose any material connections with endorsers that a consumer would not expect and to ensure that celebrity endorsers disclose their relationships with marketers when making endorsements in social media.

C. User-Generated Content

Integrating UGC into an advertising campaign can be a relatively low-cost way to encourage consumers to interact with a brand, share information about products and services, and generate excitement. UGC can go viral on the internet and spread through different social networking sites, which increases exposure and publicity for the product or service at little or no additional cost. UGC is a highly credible source of information from the consumer’s perspective, especially when the content is created by someone known to the consumer – for example, through a friend’s post on Facebook or “Tweet” on Twitter.

Advertisers may contend that they should not be liable for content they do not create. But it is by no means certain that they can avoid liability for advertising featuring UGC on that basis. The FTC explained the rationale for holding an advertiser liable for potentially misleading statements made by an endorser: “[T]he advertiser chose to sponsor the consumer-generated content such that it has established an endorser-sponsor relationship. . . . In employing this means of marketing, the advertiser has assumed the risk that an endorser may fail to disclose a material connection or misrepresent a product, and the potential liability that accompanies that risk.” The FTC added, however, that in any enforcement action, it will consider the advertiser’s efforts to advise endorsers of their responsibilities and to monitor endorsers’ conduct.

---

20 Id.


In addition to the FTC, state attorneys general and state and federal judges have held that advertisers may be liable for UGC in advertising, as discussed below.

1. **UGC and ‘Astroturfing’: The Lifestyle Lift Enforcement Action**

UGC typically consists of content created by users of a company’s products or services. Yet companies on occasion have launched marketing efforts featuring their own communications disguised as those of customers. The New York State Attorney General’s Office last year brought what it touted as the first enforcement action against a company that engaged in this practice, known as “astroturfing.” The enforcement action involved Lifestyle Lift, a cosmetic surgery franchise with more than 40 locations across the country.

According to the Attorney General’s Office, Lifestyle Lift’s president believed that negative internet postings had significantly hurt the company’s reputation and that “the success of the company hinged on controlling messages posted online.” The company’s management instructed employees to open accounts with internet message boards posing as satisfied customers of Lifestyle Lift and to create sites with testimonials that appeared to be third-party sites. Internal emails showed that one employee was told to “put your wig and skirt on and tell them what a great experience you had.” The company’s management also instructed employees to attack legitimate message board posters who criticized Lifestyle Lift and try to get their postings removed.

According to the Attorney General’s Office, these tactics constituted deceptive commercial practices, false advertising, and fraudulent and illegal conduct under New York and federal consumer protection law. In July 2009, Attorney General Andrew Cuomo announced a settlement requiring Lifestyle Lift to pay $300,000 in penalties and costs and to discontinue fabricated positive reviews on internet message boards and other internet sites.

2. **UGC and Contests: Doritos and Chevrolet**

Company-sponsored internet video contests are a popular form of incorporating UGC into advertising campaigns. Typical UGC video contests require entrants to submit a video explaining why they like a company’s product or service. Visitors to the company’s website vote on their favorite video, and the highest vote-getter wins a prize. In September 2009, Doritos invited consumers to participate in its fourth annual “Crash the Super Bowl” contest by creating and submitting to them online a 30-second ad promoting Doritos. Winners’ ads were broadcast during the Super Bowl, and the creators of the ads that claimed the top three spots of the USA Today Ad Meter had a chance to win a $5 million bonus. More than 4,000 entries were submitted for the contest. None of the winning entries cost more than $1,000 to produce. The

---


25 Id.

26 Id.

“House Rules” ad, created for only $80, was the most popular ad on the web after the Super Bowl, gaining 9.1 million views and nearly 10,000 viewer comments.

But not all UGC advertising campaigns run so smoothly. When a company encourages consumers to create advertisements, the company runs the risk that those consumers will tarnish, rather than enhance, its brand. For example, when Chevrolet launched an advertising contest inviting entrants to create a commercial for its Tahoe brand SUV, anti-SUV activists took advantage of the opportunity to create videos condemning the vehicle. The contest ran for four weeks and drew more than 30,000 entries. Chevrolet furnished video clips and music for the videos and invited users to mix and match the material and add their own captions.

Most of the videos that resulted praised the Tahoe. But the rogue entries “subverted the Tahoe message with references to global warming, social irresponsibility, war in Iraq, and the psychosexual connotations of extremely large cars.” After the anti-Tahoe videos were uploaded on Chevrolet’s website, they went viral on YouTube and ended up being far more popular than the videos designed to promote the SUV. Chevrolet chose not to take down the Tahoe-bashing videos, reasoning that it would lose credibility by doing so. Instead, it posted information on GM’s FastLane blog intended to counter the criticism, stating, for example, that the Tahoe can run on ethanol and gets better mileage than other comparable SUVs.

Despite the negative ads, many considered the campaign a success. As one reviewer of the campaign noted, the microsite that hosted the contest attracted 629,000 visitors by the time the contest winner was announced. On average, those visitors spent more than nine minutes on the site, and nearly two-thirds of them went on to visit Chevy.com. For three weeks running, the contest site funneled more people to the Chevy site than either Google or Yahoo did, and many of those visitors, once there, requested information or went on to visit dealers’ sites. Sales rose as well, even though it was the off season for SUV purchases.

3. **UCG in Comparative Advertising: Subway versus Quiznos**

Some companies have used UGC advertising contests not only to tout their own products, but also to compare their products to those of their competitors. The FTC has actually encouraged advertisers to compare directly the attributes of their product or service against a competitor’s, reasoning that truthful, nondeceptive comparative advertising is a source of important information for consumers and helps them make rational purchase decisions, encourages product improvement and innovation, and can lead to lower prices. The FTC defines comparative advertising as “advertising that compares alternative brands on objectively measurable attributes or price, and identifies the alternative brand by name, illustration or other distinctive information.” The FTC’s Statement of Policy Regarding Comparative Advertising, issued in 1979 and not updated since, does not expressly address social media.

---


30 *Id.*

An ad contest using UGC to compare the sandwiches of rival franchises Subway and Quiznos spawned the most well known litigation in social media advertising. In a summary judgment ruling in Doctor’s Associates v. QIP Holder LLC, a federal court in Connecticut held that a video contest using UCG to compare the products of two rivals does indeed constitute advertising, and may constitute false advertising, as well as state unfair trade practice violations and product disparagement.

In 2006, Quiznos partnered with video-sharing site iFilm to promote its Prime Rib Cheesesteak sandwich through a video contest called the “Quiznos vs. Subway TV Ad Challenge.” Entrants were invited to submit videos comparing a Quiznos sandwich to a Subway sandwich and show “why you think Quiznos is better.” Quiznos created a website for the contest, “meatnomeat.com,” and posted four videos created by its ad agency to serve as examples of appropriate entries. Contestant videos that complied with the contest rules were posted at the site. These rules prohibited “any false or misleading statement, or any libelous, slanderous, or disparaging statement regarding Quiznos or Subway or . . . either company’s products or services.”

Subway’s parent company, Doctor’s Associates, Inc., sued Quiznos’ parent company, QIP Holder LLC, and iFilm, in October 2006, claiming that both the company-created videos and the contestant-created videos included false and misleading statements. The contestant-created videos that Subway complained of included, for example, a Subway sandwich portrayed as a submarine unable to dive because it did not have enough meat. Subway asserted that the internet-based contest violated the Lanham Act, which prohibits any “false or misleading representation of fact which . . . in commercial advertising or promotion, misrepresents the nature [or] characteristics . . . of another person’s goods, services, or commercial activities.” Subway alleged four specific violations: First, the contest advertised itself as a “meat-no-meat comparison,” thus claiming that Subway’s sandwich had “little or no meat in it.” Second, Quiznos claimed that its sandwich was superior to Subway’s even though the products were materially different. Third, the contest solicited videos depicting Subway’s sandwich as having no meat. Fourth, Quiznos continued to compare its sandwich to a sandwich that Subway no longer offered for sale.

Quiznos moved for summary judgment in October 2009. Quiznos argued, among other things, that it could not be held liable for the content in either its four sample videos or the contestants’ videos because they were not “commercial advertising or promotion” under the Lanham Act. The court rejected this argument, noting that although the Lanham Act does not define “commercial advertising or promotion,” the Second Circuit has adopted a test for determining what constitutes such activity, and the contest videos meet that test. The court held that a statement must be (1) “commercial speech” (2) made “for the purpose of influencing consumers to buy defendant’s goods or services,” and that (3) “although representations less

33 Id. at *1.
34 Id. at *7.
36 Id. at *3, *7.
formal than those made as part of a classic advertising campaign may suffice, they must be disseminated sufficiently to the relevant purchasing public.\textsuperscript{37}

Quiznos argued that the contest materials were not commercial speech made to influence consumers to buy its goods, because the sample videos were created for a different purpose: to provide examples of how consumers could enter the contest. Quiznos also argued that the videos were not disseminated sufficiently to the relevant purchasing public because the videos were available only to an “extremely narrow” range of viewers who had to go to the contest website to see them.

The court was not persuaded. It found that the contest was “obviously an internet-based commercial advertising or promotional campaign intended to influence potential consumers to purchase Quiznos’ products over Subway’s products, and was undisputedly part of Quiznos’ national campaign aimed at highlighting the differences between its products and Subway’s products.”\textsuperscript{38} The court also concluded that it “defies logic and common sense” to argue that the videos were not widely disseminated, because “there would be no purpose to sponsoring such a Contest intended to promote a national chain such as Quiznos if the Contest was accessible to only an ‘extremely narrow’ range of viewers.”\textsuperscript{39} The court also noted that because the videos were available to anyone with internet access, they were widely disseminated to the purchasing public. It noted, as well, the posting of the winning entry on VH1 and on a billboard at Times Square, “no doubt in order to generate consumer interest in the Contest and convey the message to consumers that Quiznos’ products are superior to Subway’s products.”\textsuperscript{40}

The court also concluded there were genuine issues of fact as to whether Quiznos made false representations in connection with the contest. It found that the domain name used to solicit entrants for the contest, “meatnomeat.com,” “is arguably a literal falsity, because it clearly implies that the Subway sandwich has ‘no meat’.”\textsuperscript{41} The four sample videos depict the Subway sandwich as having no meat or less meat than a Quiznos sandwich. And the judging criteria for the contest explicitly required that the contestants’ videos make a direct comparison between Subway and Quiznos depicting Quiznos as superior. Although Quiznos argued that the representations made in connection with the contest were not literal falsities because no reasonable consumer would have been deceived by them, the court concluded that “what a person is or is not likely to believe is an issue best decided by the jury after viewing the relevant evidence, not as a matter of law on summary judgment.”\textsuperscript{42}

After the court denied Quiznos’ motion for summary judgment, in February 2010, Quiznos and Subway settled their dispute, ending the lawsuit.

\textsuperscript{37} Id. at *22.

\textsuperscript{38} Id.

\textsuperscript{39} Id.

\textsuperscript{40} Id.

\textsuperscript{41} Id. at *21.

\textsuperscript{42} Id.
D. Dealing with Brand Crises Stemming from Social Media

Just as social media can amplify the positive effects of marketing and promotion activities, it can also turn what starts out as a modest problem into a full fledged brand crisis. One of the most visible recent illustrations of this phenomenon is the now-infamous video titled “Domino’s Pizza’s Special Ingredients,” posted on YouTube in April 2009 by two rogue Domino’s employees. In the video, set in the kitchen of a Domino’s Pizza in Conover, North Carolina, one employee narrates while the other makes pizzas that the narrator says will soon be on their way to customers. The “chef” puts cheese up his nose, puts “boogers” on the pizzas, “farts” on the salami, and sneezes over the finished pizzas, while the narrator says, “that’s the way we roll at Domino’s.”43 The video went viral and within less than a week was viewed more than one million times on YouTube. References to it were in five of the 12 search results for “Domino’s” on Google. And discussions of it had spread throughout Twitter. Brand survey results showed that consumers’ perception of Domino’s quality went from positive to negative. As a company spokesperson told the New York Times: “Even people who’ve been with us as loyal customers for 10, 15, 20 years, people are second-guessing their relationship with Domino’s.”44

Domino’s responded quickly, after learning of the video from a blogger. Based on a copyright claim, the video was removed from YouTube. The president of Domino’s made another video, posted on YouTube, in which he expressed his frustration and outrage and said he was “sickened” by the video, which he termed a hoax. He thanked the social media community for bringing it to Domino’s attention. He said that Domino’s had closed the restaurant and was cleaning it “from top to bottom.” He reported that the employees had been fired and that federal warrants for their arrest had been issued. (They were indeed arrested.) He added that this experience had prompted the company to review its hiring practices “across the board.” He spoke of Domino’s emphasis on cleanliness and high-quality food. And he thanked Domino’s customers for “sticking with us.”45 In addition to posting the YouTube video, Domino’s created a Twitter account, @dpzinfo, to address the wave of Tweets generated by the earlier video and used its Facebook page to communicate its message about the incident.

To see how far companies have progressed in their ability to handle a brand crisis spawned by social media, contrast Domino’s response with a similar situation in March 2007 involving Yum Brands and a video of rats skittering through a Taco Bell/KFC restaurant in Greenwich Village. Video footage of the rats was first aired on early-morning television by WNBC-TV (which filmed the rats after a consumer had called the station’s tip line). As a Business Week writer noted, reporting on the incident: “Nobody likes to think of rats and restaurants in the same sentence. But as I scan the Net for news, I keep seeing Taco Bell and KFC in digital headlines with the words . . . “Pests” “Rats” “Rodents.” That can’t be good for business.”46

44 Id.
The company did not issue any response to the video until after 2 p.m. That response, a videotaped message from Yum Brands’ president, was posted on the KFC and Taco Bell websites. In it, the president apologized to customers, reassured them of the company’s efforts to prevent this from happening again, and announced that the company had hired a “renowned expert” on “pest control in challenging urban environments” to “thoroughly and independently review the application of the high standards we require of our operators in New York City.” The video emphasized the isolated nature of the incident and the overall food safety of Taco Bell and KFC. Brand watchers have criticized the response for not taking into account the speed of the internet and the “visceral impact of a viral video, and for not showing passion in dealing with the deeper problem of a breach of trust created by this type of situation.”

These incidents highlight the need to have a crisis management plan in place, because there will be no time to develop one once a video or posting hits the internet. Experts agree that the basic elements of such a plan should include at least the following:

- **Monitor social media for complaints and problems.** This will permit a quicker response. The case, noted above, of the Southwest Airlines passenger who became a cause célèbre on the internet after Tweeting of how he was ordered off the plane for being too large illustrates the value of being watchful. By the time his story had gained traction on Google, Southwest Airlines had apologized to him via Twitter and had posted on its blog an apology and an explanation of its policy regarding passengers who cannot fit into their seats.

- **Accept responsibility from the start**, even if it is not yet known who is at fault. As one expert observed: “It is far easier to act as if it is a problem you’ve created and take responsibility for making it right. If later events prove the brand was blameless, its ethical reaction to the problem will increase brand loyalty. If it was the company’s fault then the brand will retain consumers with its forthright, straightforward acceptance of responsibility.”

- **Don’t get defensive.** When Chevrolet’s ad contest for the Tahoe, discussed above, was subverted by Tahoe-bashing videos that went viral on YouTube, Chevrolet chose not to take down the videos, but to counter by posting factual information on its blog responding to criticisms leveled at the Tahoe. The company’s rationale, that it would lose credibility by attempting to hide the videos, seems to have been affirmed by the success of the ad campaign. Although some advise trying to prevent replays of an offending video or post, the realities of the internet show that this advice is virtually impossible to follow. The Domino’s video, for example, was quickly taken down, but other copies made their way onto the internet and can still be seen to this day.

- **‘Put out the fire’ with the same media that ‘started the fire.’** Domino’s, for example, posted its own video on YouTube to counter the video that rogue

---


49 Id.
employees had posted there. Southwest Airlines likewise responded to its would-be passenger’s complaints on Twitter with an apology on Twitter.

E. **Platform-Specific Terms and Conditions**

Companies that choose to advertise on a social media platform also must comply with any rules on advertising that the platform imposes. The social media platforms can—and do—change these rules often, and companies are responsible for keeping current with such changes. Representative rules are discussed below.

Facebook has the most detailed advertising guidelines among the major social media platforms. Its Advertising Guidelines\(^{50}\) apply to all advertisements that appear on Facebook. They prohibit advertisers from creating or managing multiple accounts for advertising purposes or using programs to automate the creation of accounts or ads without permission by Facebook. Ads must “clearly represent” the company, product, or brand being advertised, and the claims they make must be substantiated. They cannot “insult, harass, or threaten” users. They must abide by restrictions on playing audio and automated animation.

The Facebook guidelines include more than 20 categories of “prohibited ad content.” Ads must not be “false, misleading, fraudulent, or deceptive.” Ads will not be permitted if they “receive a significant amount of negative user feedback” or if they “contain, facilitate, promote, or reference” a host of items, from tobacco products to weapons to “adult toys” to spy cams to uncertified drugs. Ads cannot include contests or sweepstakes unless the advertiser gets permission from Facebook for them.

Facebook also has Promotions Guidelines\(^{51}\) governing sweepstakes, contests, and competitions held through Facebook. These guidelines provide different sets of rules for administering promotions and for publicizing promotions. Publicizing a promotion on Facebook means promoting, advertising or referencing the promotion on Facebook or using any part of the Facebook platform. Administering a promotion on Facebook means operating any element of the promotion on Facebook or using any part of the Facebook Platform, for example, by collecting submissions or entries, conducting a drawing, judging winning entries, or notifying winners. An advertiser must get prior written consent from Facebook for administering a promotion on Facebook, but not for publicizing one there.

Unlike Facebook, Twitter has no specific guidelines on advertising or promotion, but it does have a special guide for businesses, called “Twitter 101 for Business.”\(^{52}\) Twitter 101 offers “best practices,” including offering Twitter exclusive coupons or deals; taking people “behind the scenes” of the company; posting pictures from the company’s offices, stores, warehouses, or other locations; or sharing “sneak peaks” of projects or events in development.

Twitter has also launched “Promoted Tweets,” a platform that will allow advertisers to buy key words that will link to their ads. When a Twitter user searches for a word that an advertiser has purchased, for example, the promoted message will appear at the top of the


user’s search results, even though the message was written earlier. The Tweet will disclose that it is promoted by the advertiser. Unlike a regular Tweet, however, a Promoted Tweet will disappear if users do not interact with it by replying to it, forwarding it, or Retweeting it. Advertisements that appear in Twitter are subject to traditional advertising laws, and complying with those laws can be a challenge given Twitter’s 140-character limit.

Most social media platforms provide less explicit guidance on advertising. For example, Foursquare, a Web and mobile application that awards “points” redeemable for discounts and special offers for “checking in” at various locations, has Terms of Use that prohibit users from taking any action or distributing any content that involves commercial activities or sales without Foursquare’s prior written consent, “such as contests, sweepstakes, barter, advertising, or pyramid schemes.”

F. Practice Tips

Companies advertising through social media must meet the standards applicable to advertising in more traditional media for prohibiting deceptive and unfair messages and being able to substantiate claims. In the area of endorsements and testimonials, they must meet even stricter standards, especially regarding disclosure of “material connections” between a company and the person speaking about its products or services. Transparency is key. To avoid an FTC enforcement action, it is critical to have sound policies on disclosure for endorsers and to monitor compliance with those policies.

Companies must recognize that incorporating UGC in advertising can have both great upside potential and great risks. It is important to have a strategy for dealing with negative UGC before it gets disseminated. That strategy should start with terms and conditions for any ad contest or other program that involves public participation. These terms and conditions should:

- Clearly state entry criteria and the duration of content hosting on the sponsor site;
- Set out any restrictions on content – particularly content that could lead to liability for false or deceptive advertising claims (as well as claims of defamation or infringement of trademarks, copyrights, publicity rights, or privacy rights, discussed below);
- Allow maximum discretion to take down content that does not comply;
- Provide for disclaimers of responsibility for the UGC (although as the Quiznos case shows, it can be difficult to encourage creation of content and then disclaim responsibility for it);
- Include a provision for the creator of UGC to indemnify the company in any legal action over the UGC (recognizing, however, the practical limitations of such indemnification);
- Consider whether to restrict participation to any particular geographic area, based on the laws that would apply outside that area.

UGC should be reviewed regularly, to ensure that it complies with the company's requirements. Companies should monitor third party social media sites regularly as well.

Companies must be sure to comply not only with applicable laws, but with the terms and conditions of the social media platforms they are using.

For additional protection, companies that use UGC should consider obtaining insurance coverage for advertising-related injuries, through a commercial general liability policy, a media liability policy, or a cyber liability policy.

III. PRIVACY IN SOCIAL MEDIA

Social media allows advertisers and the public to form an intentional community of interest. As is expected when forming relationships, the parties knowingly disclose information about themselves and learn or gather information about each other. Through online connections, other types of information can be gathered about consumers’ online activities that consumers may not consciously share. Some of that information enables the advertiser to drill down to target the affinity group or others who are more likely (according to analysis of their online activities based on certain algorithms) to be interested in purchasing a product or service. However, not all consumers are receptive to the directed types of marketing messages and media of communication that are possible through the information that may be gathered online and through social media.

The FTC and some states, such as California, have established guidelines and laws on the use of privacy policies to inform consumers using a website of what information may be collected and how that information may be used. The general approach in the United States is self-regulatory, assuming that consumers read the privacy policies posted on the websites they visit and are notified in advance of how their personally identifiable information and other information about them may be gathered, used or shared. Most FTC actions have concerned companies that violated their own privacy policies by, for example, sharing information with third parties when they promised they would not or applying newly instituted policies to information acquired under old policies. For example, in *In the Matter of Gateway Learning Corp.*[^54] the first FTC case to challenge changes to a business’ privacy policy as an unfair and deceptive act or practice, Gateway, the seller of “Hooked on Phonics” products, rented consumers’ personal information even though its privacy policy stated it would not do so. After Gateway revised its privacy policy, it continued to rent personal information collected under the prior policy. Gateway agreed to settle the FTC charges with an order that it may not share personal information collected under the prior policy, and it may not materially change its privacy policy in the future in a manner that has retroactive effect without obtaining consumers’ consent.

However, with the advent of social media, users are providing much more information about themselves, potentially on multiple sites. New types of technology enable personal data to be analyzed and used in ways not previously possible. This section provides a general overview of the privacy issues raised in certain types of web-based social media.

The information collected about a person can be divided into two categories: (1) personally identifiable information that can be linked to a specific individual, such as a person’s name, email address, postal address, date of birth, Social Security Number, or credit card

number ("PII"); and (2) non-personally identifiable information ("non-PII"). Non-PII is anonymous data that without additional information cannot be used to identify a specific person, such as general internet searching. Most privacy concerns arise from the use of PII gathered about an individual to generate user-specific banner or pop-up ads, commercial email messages, and the like. However, privacy issues also may arise concerning aggregate or anonymized information, such as five-digit zip code, birth date, gender, city or area code for likely customers, or profiles of consumers who purchased a product within the last month. Given the number of laws, regulations and industry standards in this area, a business should consult legal counsel before implementing a new advertising approach to ensure that privacy issues are handled appropriately.

A. Behavioral Advertising

Behavioral advertising is a targeted form of advertising that collects information on an internet user’s broad online behavior, not limited to a particular site, to develop a marketing profile for the consumer. Behavioral advertising may consider the user’s browsing habits, search queries and website history to display more relevant advertisements or information to the user. The FTC and the industry trade group Network Advertising Initiative ("NAI"), among others, have issued self-regulatory guidelines for behavioral advertising.

A pending class action challenges one of the first applications of behavioral advertising in the marketplace. In *Valentine v. NebuAd, Inc.*, the plaintiff alleged that the NebuAd advertising company engaged in behavioral advertising in violation of federal and state privacy laws. The NebuAd system is designed to allow Internet Service Providers ("ISPs") to provide targeted advertisements to people surfing the Web by engaging in what is called “deep packet sniffing.” The case is pending in the Northern District of California; however, the various ISPs included in the complaint obtained dismissal for lack of personal jurisdiction, leaving NebuAd as the sole defendant. The plaintiff followed up with an action in the Northern District of Illinois against WideOpen West, Finance, LLC ("WOW"), an ISP dismissed from the *Valentine v. NebuAd* case. In this action, the plaintiff alleges that WOW violated its users’ privacy by installing spyware on its broadband networks in violation of privacy rights, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the Illinois Criminal Code’s eavesdropping restrictions.

The FTC issued public reports on online data collection practices, hosted various public workshops and released a set of proposed principles for public comment, all of which were considered in its 2009 Report on Self Regulatory Guidelines for Online Behavioral Advertising. These guidelines consist of four basic principles for behavioral advertising: (1) transparency and

56 See Fed. Trade Comm’n, FTC Staff Report at 46.
consumer control; (2) reasonable security and limited data retention for consumer data; (3)
affirmative express consent for material changes to existing privacy promises; and (4)
affirmative express consent to (or prohibition against) using sensitive data for behavioral
advertising. The principles are geared toward collection of data over time, where a consumer
profile is developed and shared with third parties for marketing purposes.60

Any website where data is collected for behavioral advertising should provide “a clear,
concise, consumer-friendly, and prominent statement that (1) data about consumers’ activities
online is being collected at the site for use in providing advertising about products and services
tailored to individual consumers’ interests, and (2) consumers can choose whether or not to
have their information collected for such purpose.” The opt-out provision for data collection
should be “clear, easy-to-use, and accessible.”61

The guidelines also include a provision for data that is collected outside the traditional
website context, such as mobile devices, social media where users interact with each other as
contributors to a website, and ISPs. In these instances, the business gathering information
should develop alternative methods of disclosure and consumer choice that meet the same
standards as traditional website data collection, i.e., a clear, prominent, easy-to-use statement
and an opt-out provision.

A business that collects and/or stores consumer data for behavioral advertising
purposes should provide reasonable security for the data and retain the information only “as
long as necessary to fulfill a legitimate business . . . need.”62

The promises a business makes concerning how it will handle and protect consumer
data must be kept. Therefore, if a business considers using previously collected data in a
manner materially different from its initial promise, the business “should obtain affirmative
express consent from affected consumers”63 before using the data under the new conditions.
An example of this type of situation is a corporate merger that changes the manner in which
consumer information is collected, used, and shared or changes to a terms of use or privacy
policy that materially effects the data collection from when a user initially signed up.

Lastly, a business should collect sensitive data, such as medical history or sexual
orientation information, only if it has obtained affirmative express consent from the consumer to
receive advertising based on sensitive data.

The NAI also published guidelines for online behavioral advertising in July 2009 together
with the American Association of Advertising Agencies, Association of National Advertisers,
Council of Better Business Bureaus, Direct Marketing Association and Interactive Advertising
Bureau. These self-regulatory principles for online behavioral advertising64 consist of seven
principles that are generally aligned with the February 2009 “Self-Regulatory Principles for
Online Behavioral Advertising” proposed by the FTC.

60 FTC STAFF REPORT, supra note 55.
61 Id. at 46.
62 Id. at 46-47.
63 Id. at 47.
64 American Association of Advertising Agencies et al., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL
The seven NAI principles are: (1) education; (2) transparency; (3) consumer control; (4) data security; (5) material changes; (6) sensitive data; and (7) accountability. Unlike the FTC guidelines, the NAI principles also include an obligation to educate consumers and businesses about online behavioral advertising and have mechanisms by which online behavioral advertising can be policed.

In April 2010, the NAI also issued the CLEAR Ad Notice Technical Specifications to provide consumers with notice of online behavioral advertising and their choices. The CLEAR (Control Links for Education and Advertising Responsibilities) Specifications include an icon leading to metadata tags with information on the entity that served the ad, where to find its advertising policies, and how to opt-out of such ad targeting in the future.65

B. Contextual Advertising

Unlike behavioral advertising, which analyzes a consumer’s broad online activities across sites over time, contextual advertising is based on the conduct of a user within a single website or a search query. For example, a user who conducted a search for the “Bahamas” may see advertisements for hotels in the Caribbean or airfare to the Bahamas or the Caribbean. Generally, this type of advertising is considered less intrusive because it is based on a user’s one-time visit or search, not browsing habits and search queries that are collected over a period of time.66

In fact, the FTC recognizes that contextual advertising is more transparent and more likely to be consistent with an internet user’s expectations. Additionally, the FTC recognizes that this type of advertisement may provide revenue for websites, which allows them to offer free content. For these reasons, contextual advertising is explicitly omitted from the FTC’s Self Regulatory Guidelines for Online Behavioral Advertising, but still is subject to FTC and state laws and regulations concerning privacy protection generally. Accordingly, at least some kind of reasonable privacy and security measures should be used for any personal information that is collected and maintained.67

C. Aggregate and Anonymized Data

Aggregate or anonymized information is customer information from which customer names and other personal identifiers have been removed. Anonymized information can be released to third parties such as website advertisers for a fee and shared within an organization for purposes of marketing. Most privacy policies include a statement that the site host may use aggregate or anonymized data. Anonymized data is often afforded less protection than data that identifies a particular person, because it is thought to be untraceable.68


66 FTC STAFF REPORT, supra note 55, at 29.

67 Id. at 28 n 56, 30.

68 See, e.g., Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, SOCIAL SCIENCE RESEARCH NETWORK, 7-8 (Aug. 18 2009), http://ssrn.com/abstract=1450006; C. Christine Porter, De-
However, sometimes anonymous data can raise privacy issues for internet users. Non-
PII information may be collected in a manner that allows it to be linked to PII information and
"re-identified" once a user has registered for a site, or it can create a detailed "anonymous"
profile of a person that makes that person easily identifiable. For example, AOL disclosed
internet search histories of more than 500,000 AOL users in 2006. Using the anonymized data,
New York Times reporters identified an individual based on the searches that were disclosed.69
This re-identification can pose significant risk to a company that releases or sells anonymized
data.70 As a result of the information release, AOL users sued AOL in the Northern District of
California for breach of privacy and filed a complaint against AOL with the FTC.71

D. Privacy Actions Against Social Media

Although the FTC guidelines on privacy are considered self-regulatory, the FTC is active
in bringing actions against companies that fail to protect adequately consumer information.
Since 2001, the FTC has brought more than 20 actions against companies failing to adequately
protect sensitive consumer information both online and offline.72 The FTC recently settled a
case against Twitter, its first case against a social media service. The FTC charged Twitter with
failing to adequately protect consumer information, which enabled hackers to access non-public
user information. Through this unauthorized access, hackers were able to send out Tweets
from any user account, and in fact sent a Tweet from the account of then President-elect Barack
Obama. The FTC alleged that Twitter did not implement adequate procedures for its employees'
access to consumer information to prevent unauthorized hacking into administrative control of
its system. Twitter failed to follow reasonable security measures such as requiring employees
to use hard-to-guess administrative passwords, suspending or disabling administrative
passwords after a number of unsuccessful login attempts, enforcing periodic changes to
administrative passwords and restricting access to administrative controls. The terms of the
settlement include a requirement that Twitter establish and maintain a security program that will
be independently audited every other year for ten years.73

Additionally, several consumer groups including the Electronic Privacy Information
Center, the Center for Media and Democracy and Consumer Watchdog filed a complaint and
request for investigation with the FTC for material changes to Facebook's privacy policy. The
complaint alleges that Facebook discloses information to third parties that was previously
unavailable to them and makes information public that was previously restricted. For example,
Facebook discloses personal information to Microsoft, Yelp and Pandora without user consent.

69 FTC STAFF REPORT, supra note 55.
70 Id.; Ohm, supra note 68.
71 FTC STAFF REPORT, supra note 55, at 24; Ellen Nakashima, Internet Privacy Group Files Complaint Against AOL,
72 Docket, Ramkissoon v. AOL, LLC. (N.D. Cal.) (06-cv-05866).
73 Twitter Settles Charges that it Failed to Protect Consumers’ Personal Information, FED. TRADE COMM’N, June 24,
The complaint alleges that these practices violate Section 5 of the Federal Trade Commission Act, which governs unfair and deceptive trade practices.\textsuperscript{74}

E. State Privacy Statutes

California has adopted online privacy laws to help protect consumer information. For example, Section 1798.83 of the California Civil Code, which is applicable to online businesses that collect personal information about California residents, requires those businesses to disclose their information sharing practices upon request. This requirement may be avoided if a business has a privacy statement (posted privacy policy) giving the consumer the opportunity to opt out of information sharing. Additionally, Section 22575 of the California Business and Professions Code requires commercial websites or online services that collect personal information on California residents to post a privacy policy and comply with it.\textsuperscript{75}

In addition to California, various other states have laws related to internet privacy that vary in scope. For example, Minnesota and Nevada have statutes that prohibit the disclosure of personally identifiable information and require certain information to remain private unless the consumer gives permission to disclose the information. Some states, including New York, Arizona, Colorado, Illinois and Virginia, have statutes that require government websites to establish privacy procedures or privacy policies for the websites.\textsuperscript{76}

In the related area of maintaining the security of PII once collected, Massachusetts requires that a business develop and have in place a written security policy if the business owns or licenses any "personal information," defined as a first and last name or first initial and last name, in combination with a credit or debit card number, driver's license number or Social Security number.\textsuperscript{77} The statute took effect March 1, 2010 and has not yet been interpreted by the courts. Many other states have data breach laws.\textsuperscript{78}

F. CAN-SPAM Regulation of Outbound Commercial Email Messages

One of the main uses of the PII gathered through social media is to send commercial email messages to a targeted list of consumers who are likely purchasers of the business' products or services. The federal CAN-SPAM Act in general prohibits fraudulent, abusive and deceptive commercial email\textsuperscript{79} using the "one-bite" rule. A business may send an unsolicited commercial email message, properly labeled, to a consumer, with an easy means for the consumer to opt-out of receiving future messages. If the consumer opts out, the business may no longer send emails to that consumer, and further emails are in violation of the CAN-SPAM act.


\textsuperscript{75} CAL. CIV. CODE § 1798.83 (2009); CAL. BUS & PROF. CODE § 22575 (2008).

\textsuperscript{76} See MINN. STATS. §§ 325M.01-.09 (2004); see also NEV. REV. STAT. § 205.498 (2009); NAT'L CONFERENCE OF STATE LEGISLATURES, STATE LAWS RELATED TO INTERNET PRIVACY (2009), http://www.ncsl.org/default.aspx?tabid=13463.

\textsuperscript{77} 201 MASS CODE REGS. 17.00 (2010).


Act. If the consumer does not opt out, the business may continue to send email messages until receiving an opt-out from the consumer.

A commercial email message is broadly defined as having a primary purpose to advertise or promote some type of commercial product or service. Therefore, the CAN-SPAM Act applies to all commercial emails, not just bulk emails or what is commonly known as “spam.” The Act does not apply to transactional emails, which facilitate an agreed upon transaction or provide an update for a transaction. Examples of a purely transactional email include emails that confirm a sale; give warranty, recall or safety information about a product; or provide an update about a change in terms for an account or membership. If a message contains both commercial and transactional content, the primary purpose of the email determines if compliance under the CAN-SPAM Act is required, although the primary purpose itself may be subject to debate.

The CAN-SPAM Act sets forth several requirements for commercial email messages. The information in the header cannot be false or misleading, that is, the routing information, originating email address and domain name must accurately identify the person or business sending the email. Additionally, the subject line of the email must accurately reflect the email content or subject matter and the email itself also must identify that it is an advertisement. The email must give a valid physical postal address of the sender.

Each commercial email message also must include a clear and conspicuous opt-out provision that tells recipients what they can do to stop receiving emails. The opt-out usually provides a link that opens an email message back to the sender in which the recipient can request the opt-out. Once a business receives an opt-out request, it must comply by removing the recipient’s email address from its mailing lists within ten business days. List management thus can be highly complicated and important to ensure compliance with the CAN-SPAM Act.

In 2009, the FTC provided additional guidance on the CAN-SPAM Act, which reiterated the requirements discussed above. Of particular note was the FTC’s statement that a business should monitor a third party that is handling email marketing to ensure compliance with the CAN-SPAM Act.

A violation of the CAN-SPAM Act is subject to penalties of up to $16,000 for each separate email. Additionally, a violation can be attributable to more than one person such as the original sender and the company promoted in the email itself. Even though the CAN-SPAM Act pre-empts state statutes, states may enforce the sections of the Act addressing fraudulent or deceptive acts, computer crimes and restrictions on non-wireless spam against a business sending out email advertisements.

Social media sites often post their own policies against spamming in their terms of use. In some instances a spamming violation can result in permanent suspension of an account on

80 Id. § 7702(2)(A).
82 Id.
that social networking site. The sites may consider different factors to identify objectionable spamming. For example, Twitter considers creating mass accounts at one time, following a large number of users in a short time and updates that consist mainly of links or misleading links and not personal posts as flags for spammers.84 Facebook states that, “[advertisements] cannot contain, facilitate or promote ‘spam’ or other advertising or marketing content that violates applicable laws, regulations or industry standards.” Arguably, advertisers on Facebook must at least comply with CAN-SPAM and FTC guidelines. Indeed in 2009, Facebook was awarded over $700 million under the CAN-SPAM Act in a default judgment against a spammer who sent pornographic websites to account holders.85

G. Privacy of Children Under 13 Years Old (COPPA)

The Children’s Online Privacy Protection Act (“COPPA”) affords additional privacy protections to children under the age of 13 in the context of website advertising.86

COPPA applies to operators of commercial websites and online services directed to children under the age of 13 that collect information from the children. It also applies to operators of commercial websites and online services directed to a general audience, but that knowingly collect information from children under the age of 13 or have a separate section that collects information from children under the age of 13.87

In general, COPPA requires that operators of websites and online service must obtain parental consent before collecting information from children under the age of 13. The website or online operator must make reasonable effort to obtain parental consent or provide notice to the parents that the child has provided personal information to the website. A number of methods may be used to obtain verifiable parental consent; however, the method must be reasonably calculated to ensure that the person providing consent is, in fact, the child’s parent.88

Options to obtain parental consent include providing a form for the parent to print, fill out, sign, and mail or fax back to the website operator; requiring the parent to use a credit card in connection with a transaction; maintaining a toll-free telephone number for parents to call in their consent; and obtaining consent with a digital signature via email. If the child’s information is only used for internal purposes, and it will not be disclosed, then the “email plus” option may be used. The email plus option is a direct notice to the parent asking that the parent provide consent in an email message. However, after receiving the parent’s email consent, the website operator must verify that the parent provided consent by contacting the parent by telephone, fax or mail. A subsequent confirmation email also may be sent after a reasonable time delay to confirm the original consent email. This follow-up consent email should include (1) all the

87 Id. § 6502.
original information contained in the direct notice; (2) inform the parent that consent can be revoked; and (3) indicate how the consent can be revoked.89

A few exceptions to the parental consent requirement exist. For example, parental consent is not required if information collected from a child is (1) used to respond directly to a specific request from the child; (2) not used to re-contact the child; and (3) not maintained in a retrievable form by the operator.

In addition to parental consent, COPPA requires operators of child-oriented websites to provide notice on the website of (1) what information is collected from the children by the operator; (2) how the operator uses such information; and (3) the operator’s disclosure practices for such information. COPPA also prohibits conditioning a child’s participation in a game, contest or activity on the disclosure of more personal information than is reasonable necessary to participate in such activity.90

COPPA also provides certain rights to a parent or guardian whose child has provided personal information to a website or online service. Upon request, the online service provider must provide (1) a description of the specific types of personal information collected from the child by that operator; (2) the opportunity to refuse to permit the operator’s further use, collection, and maintenance of personal information from that child; and (3) a means for the parent or guardian to obtain any personal information collected from the child.91

To encourage active industry self-regulation, COPPA also includes a safe harbor provision allowing industry groups and others to request FTC approval of self-regulatory guidelines to govern participating websites’ compliance with COPPA. The Children's Advertising Review Unit of the Council of Better Business Bureaus Inc., www.caru.org; ESRB Privacy Online, A Division of the Entertainment Software Rating Board, www.esrb.org; TRUSTe, www.truste.com; and Privo, Inc., www.privo.com, all have self-regulatory guidelines for children’s privacy that have been approved by the FTC and are posted on their sites.92

The FTC has fined several businesses for COPPA violations for improperly collecting, maintaining and disclosing information about children under the age of 13 without parental consent. Sony BMG Music eventually settled with the FTC for $1 million.93 Iconix Brand Group also settled charges that its apparel websites violated COPPA by collecting information from children under the age of 13 without parental consent despite its privacy policy stating that it would not collect such information without parental consent.94

89 Id.
90 Section 6502 supra note 86.
91 Id.
The saying that “no one knows you’re a dog on the internet” is especially true for children, who can easily misrepresent their age in online communications. The Facebook and MySpace terms of use require users to be at least 13 years of age. Twitter does not have an age requirement set forth in its terms of use. Although social networking sites typically impose age restrictions, children can easily misrepresent their age to join a particular site. For example, a lawsuit filed on behalf of a minor against MySpace alleged that MySpace was negligent in failing to take steps to prevent a minor from lying about her age, which led to a sexual assault on the minor by a 19 year old. The claim was dismissed based on a finding that it was barred under the Communications Decency Act, which protects internet service providers from liability based on their publication of information created by third parties (in this case, a false profile created by the minor).

H. Practice Tips

Often businesses want to reassure site users about privacy issues by stating on their sites or in their privacy policies that they protect consumers’ information and do not share it. However, one of the key areas of exposure is an overpromise misrepresenting the business’ privacy practices. For example, in the FTC action against Twitter described above, the FTC not only acted against Twitter’s lack of privacy controls, but also its promises to consumers that their personal information would be secure, thus misleading the public about its privacy practices. Even if a business initially intends to keep PII for internal use only, at some point most businesses will want to understand their users more fully, and may seek to analyze and then monetize the personal information that is readily available through common analytical tools by sharing that information with third parties.

Businesses should think carefully about their current privacy practices and potential future business needs and expansion plans when crafting privacy policies or promises. Avoid the attraction of copying a privacy policy found on someone else’s site with the assumption that it has the required language. Privacy policies must be specific to each business’ own practices. In anticipation of possible changes in handing PII in the future, a business may want its policy to give it some leeway for broader usage than it initially intends. However, for more wholesale changes in the future, the privacy policy should reserve the right for the business to revise the policy in the future, explain how consumers can learn that the privacy policy has been changed, and state that the then-current policy will apply to all PII collected after the change has been implemented. This may create an obligation on the business to track which PII was collected under different versions of the policy, and ensure that each group of PII is handled in accordance with the policy applicable when collected.

To convey a strong privacy approach to increase public confidence, a business can consider becoming certified by one or more of the privacy certification programs such as TRUSTe, the most commonly used privacy certification, see www.truste.com; or Better Business Bureau Online Accredited Business seal, see www.bbb.org. If venturing into behavioral advertising or some other activity outside the consumer’s expectations, be sure to disclose those practices and keep in mind the FTC’s guideposts for behavioral advertising.

---


96 Doe v. MySpace, Inc., 528 F.3d 413, 418, 422 (5th Cir. 2008).
For those websites that serve California residents, consider whether your privacy policy should include the consumers’ rights notice under California Civil Code Section 1789.3, stating how consumers may obtain additional information about the business’s privacy practices.

Businesses should check their internal data security practices and consider whether to adopt a data security plan.

A privacy policy also should disclaim responsibility for the privacy practices of third party advertisers on the site, and for any other websites reached by links from the site to another site.

When planning an email advertising campaign, consult the anti-spam policies of any social media involved and carefully adhere to the CAN-SPAM Act requirements for outbound email messages. Many companies use established list maintenance vendors and commercial email services with experience in managing opt-outs or “suppression lists”. For businesses that want to be especially accommodating of consumers’ privacy concerns or that use affiliate networks and other third party programs to build email lists, consider an opt-in program whereby your email lists consist only of consumers who have requested email communications.

If considering a new website, contest or other program via social media, think twice when considering whether to include children under the age of 13. If you choose to include young children, take advantage of the many resources and alternatives to assist in your compliance with COPPA requirements. For sites that are not directed to children or have other age restrictions (such as bar/lounge sites for businesses that serve alcohol), make sure the site programmers include technological controls so that users providing a birthdate that is under age are barred from the site.

Many websites that enable consumers to register to receive email updates or otherwise send outbound marketing emails provide consumers the opportunity to change their privacy settings to opt in or out of receiving emails and to correct or update their contact information.

IV. DEFAMATION AND DISPARAGEMENT IN USER GENERATED CONTENT

Comments posted on social media platforms have given rise to an increasing number of lawsuits for defamation and product disparagement. When companies sponsor blogs, Facebook pages, and other social media sites that invite people to express themselves online, the companies can face risks of defamation liability for these postings. The Communications Decency Act (“CDA”)\(^97\) can offer those who host internet sites a safe harbor against liability for defamation claims arising from UGC posted on their sites. But companies face a dilemma in trying to minimize the risk of defamatory or disparaging statements in UGC: On one hand, they can monitor UGC and ensure that such statements are edited out or taken down from their sites. On the other hand, the more “hands on” they are in dealing with UGC, the more they risk losing their safe harbor immunity by being deemed the provider of the content itself, not merely the provider of the interactive computer service hosting the content.

A. Defamation and Product Disparagement Claims

Defamation is a state-law claim. The elements of a defamation claim vary from state to state, but the basic elements in most cases are: a false and defamatory statement concerning an identifiable person; an unprivileged publication of the statement to a third party; fault

amounting to at least negligence on the part of the publisher of the statement; and resulting injury to the person’s reputation or business.98

Trade defamation, or product disparagement, also a state-law claim, involves false statements made about a company or its products or services. Product disparagement claims are asserted to protect property rights, rather than reputational rights. A claim for product disparagement requires a showing that: a false statement was published; the publisher either intended, or reasonably should have recognized, that the publication would cause pecuniary loss; pecuniary loss did in fact occur; and the publisher either knew that the statement was false or acted in reckless disregard of its truth or falsity.99

B. The CDA’s Safe Harbor Provision for UGC

The CDA, enacted in 1996, offers interactive computer service providers and website operators broad protection from liability for defamatory or disparaging statements made by third parties. In Zeran v. America Online, the Fourth Circuit explained the rationale for this immunity:

The amount of information communicated via interactive computer services is . . . staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.100

This immunity does not extend to those who violate criminal laws, intellectual property laws, state laws that are not in conflict with the CDA, or certain privacy laws.101

The CDA’s safe harbor provision states 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.”102 This “publisher” designation is key, given that publication is an essential element of any defamation claim. Essentially, the safe harbor provision creates a “federal immunity” from causes of action that would make interactive computer service providers liable for information originating with third-party users of the service.103 Courts across the country have held that the CDA’s grant of immunity should be construed broadly.104

98 Restatement (Second) Torts § 558 (1997).
100 Zeran v. America Online, 129 F.3d 327, 331 (4th Cir. 1997).
102 Id.
103 Zeran, 129 F.3d at 330.
104 See, e.g., Doctors Associates Inc., 2010 WL 669870 at * 23 (other case citation omitted).
The CDA does not draw any distinctions based on whether the interactive computer service provider or website owner, by its terms of service, has acquired ownership of the UGC posted on its site or has in effect sponsored the content. But courts have considered these factors in deciding whether providers qualify for immunity under the CDA, as the cases discussed below will show.

To encourage self-regulation, the CDA’s “Good Samaritan” provision also protects providers and users of interactive computer services from liability for any good faith efforts they make to restrict access to or availability of material they consider to be “obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.” The Fourth Circuit has interpreted this to mean that lawsuits seeking to hold an interactive computer service provider liable for its exercise of a publisher’s traditional editorial functions, “such as deciding whether to publish, withdraw, postpone or alter content,” are barred by the CDA.

The CDA’s safe harbor provision protects interactive computer service providers even if they are on notice that a posting is potentially defamatory. The rationale behind this rule is that imposing liability on service providers who are on notice “would defeat ‘the dual purposes’ of section 230, by encouraging providers to restrict speech and abstain from self-regulation.”

Although the safe harbor provision offers broad protection to those who provide interactive computer services and those who access the services, it does not protect “information content providers,” defined as those who are “responsible, in whole or in part, for the creation or development of information provided through the internet or any other interactive computer service.” To the extent that interactive computer service providers develop or sponsor the content that third parties post on their sites, they put their immunity at risk by becoming “information content providers.”

Two widely cited circuit court decisions issued in 2008 illustrate where courts have drawn the line between a protected provider of an interactive computer service hosting content and an unprotected provider of the content itself. In Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, the Ninth Circuit held that Roommates.com, which operated a Web-based service for finding roommates, could not rely on CDA immunity because it was a content provider. Participants in the Roommates.com service were required to fill out a questionnaire listing their sex, sexual orientation, and whether they would have children living with them. The housing authority sued Roommates.com, asserting that this violated the federal Fair Housing Act by inducing users to disclose characteristics protected under the Act and by sorting search results based on those characteristics. The court concluded that Roommates.com became an information content provider by designing its website to develop unlawful content as a condition precedent of use.

106 Zeran, 129 F.3d at 330.
109 521 F.3d 1157 (9th Cir. 2008) at 1167-75.
On the other hand, in *Chicago Lawyers Committee for Civil Rights Under the Law, Inc. v. Craigslist, Inc.*\(^\text{110}\) the Seventh Circuit held that Craigslist, a for-profit service that provides “an electronic meeting place” for those who want to buy, sell, or rent housing and other goods and services, did not violate the federal Fair Housing Act by allowing the posting of ads that included statements such as “no minorities” and “no children” -- content that disclosed characteristics protected under the Act -- because Craigslist did not induce any user of the service to post any particular listing or express a preference for discrimination. Instead, it merely provided a place where users could post their messages, and thus, it was entitled to CDA immunity as a provider of an interactive computer service.

C. **CDA Immunity Not Granted to Quiznos**

CDA immunity was a key defense asserted by Quiznos in *Doctor’s Associates Inc. v. QIP Holder LLC.*\(^\text{111}\) In that lawsuit, discussed at length in Section II above, Subway asserted a claim for commercial disparagement under Connecticut law, among other claims.

Quiznos argued that entrants who posted videos in its advertising contest were the exclusive creators of the videos Subway complained of, and that Quiznos was merely an interactive computer service provider with respect to the entrants’ videos. Subway argued that Quiznos went beyond the role of a traditional publisher by “soliciting disparaging material” and “shaping the eventual content” of the contestant videos such that they were “responsible” for the creation and development of information provided through the contest’s website.

The court said the question of CDA immunity hinged on whether Quiznos merely published information provided by third parties or instead was “actively responsible” for the creation and development of disparaging representations about Subway in the contestant videos. The court concluded it could not rule, as a matter of law, that Quiznos was not responsible for creating or developing the videos, citing evidence that: Quiznos invited contestants to submit videos comparing Subway and Quiznos and showing “why you think Quiznos is better”; the www.meatnomeat.com domain name used to solicit entries “is arguably literally false because it implies that the Subway sandwich has no meat”; and the sample videos designed by Quiznos to shape contest submissions arguably contained false representations, showing a Subway sandwich as having no meat or less meat than a Quiznos sandwich.

The court concluded that this question was best submitted to a jury, adding that a reasonable jury might well conclude Quiznos did not merely post the arguably disparaging content in the contestant videos, but instead actively solicited disparaging representations about Subway, and thus was responsible for the creation or development of the contestant videos. The court also noted that a party may be responsible for information created or developed by another without actually creating or developing the information itself, and that suffices for imposing liability.

D. **Defamation Liability for Statements by Employees**

Companies may be liable for defamatory statements made by employees using social media sites when those employees are acting within the scope of their employment. The CDA’s safe harbor provision may not apply in that case, because the company no longer can claim that

\(\text{110} 519 \text{ F.3d 666 (7th Cir. 2008) at 671-72.}\)

\(\text{111} 2010 \text{ WL 669870 at *22-24.}\)
it merely posted content created by a third party; instead, it may be deemed through the employee to be providing the content itself.

For example, the technology company Cisco Systems Inc. found itself defending against two defamation lawsuits because of statements made by one of its lawyers, Richard Frenkel, about patent lawyers outside the company in an anonymous “Patent Troll Tracker” blog. Frenkel started the popular and controversial blog in May 2007. It was generally dedicated to sniffing out “patent trolls,” shell companies that buy patents for no other reason than to exploit them through enforcement. No one from Cisco edited his postings or required him to write on any topic. And no one beyond his immediate supervisor knew he was the author of the Patent Troll Tracker blog until he admitted it in early 2008.112

In separate but nearly identical cases, two Texas attorneys, Eric Albritton and John Ward Jr., sued both Frenkel and Cisco for defamation based on the blog posts on Patent Troll Tracker. In the Albritton case, the court denied key aspects of each side’s motions for summary judgment, and the case settled in September 2009, during trial.113 In the Ward case, the plaintiff voluntarily dismissed Frenkel but continued to pursue claims against Cisco. After Cisco lost a motion to dismiss, that case also settled, in January 2010, on terms that are not disclosed.114

In March 2008, Cisco issued a revised blogging policy based on “lessons learned” from the Patent Troll Tracker experience.115 The revised policy provides that if employees comment on any aspect of the company’s business, or any issue in their field in which the company is involved, they must clearly identify themselves in their postings as Cisco employees and must include a disclaimer that their views are their own and not those of Cisco. The company also said it believed Cisco employees used poor judgment when they suggested topics to Frenkel for his anonymous blog or pointed third parties to the blog without disclosing that the content was created by a Cisco employee.

Companies also must be prepared to deal with employees who disparage customers on social media sites. Franchisor Brixx Pizza had a ready response in one such recent case, firing a waitress at after she complained on Facebook about customers who had lingered for three hours over lunch and then left her only a $5 tip. When she got home from work that day, she vented her frustration by posting: “Thanks for eating at Brixx, you cheap piece of - - - - camper.” Within a day, she was called in by the restaurant manager, shown a copy of her comments, and fired for violating the franchisor’s policies against speaking disparagingly about customers and casting the restaurant in a negative light on social networks.116

116 Eric Frazier, Facebook Post Costs Waitress Her Job, CHARLOTTE OBSERVER, May 17, 2010, available at http://www.charlotteobserver.com/20100517/1440447/facebook-post-costs-waitress-her.html. Note, however, that many states have “off-duty laws” that may prohibit employers from disciplining or terminating employees for posts made on their own time, using their own computers -- even if these posts violate the employer's guidelines or policies.
E. Defamation Liability of Consumers

Comments on Facebook and Twitter can land the commenters in court defending against claims of defamation and disparagement. After a Michigan college student had his car towed, he created a Facebook page, “Kalamazoo Residents against T&J Towing,” on which he claimed that the service improperly towed his car. 117 The group had 800 members after only two days. In April 2010, the company sued the student for defamation, alleging that he “falsely and publicly claimed that Plaintiffs have towed vehicles where no violation has occurred” and that he was responsible for the postings of other Facebook users, alleging that he had “absolutely no way of knowing whether or not all of the written submissions to his website have any truth or validity.” 118 The student asserted counterclaims for violations of the Michigan Consumer Protection Act and abuse of process. After his story drew the attention of the New York Times, his Facebook group grew to some 14,000 members.

Even a Tweet can be subject to a defamation claim. In Horizon Group Management LLC v. Bonnen, the owner of a Chicago apartment complex sued a tenant for defamation after it learned of the following Tweet that she sent to a friend who planned to visit: “You should just come anyway. Who said sleeping in a moldy apartment was bad for you? Horizon realty thinks it’s okay.” 119 The apartment complex owner alleged that the tenant “maliciously and wrongfully” composed and published the false and defamatory Tweet on Twitter, “thereby allowing the Tweet to be distributed throughout the world.” 120 Upon the tenant’s motion, the Cook County Circuit Court on January 20, 2010, dismissed the case with prejudice, finding the Tweet “nonactionable as a matter of law.” 121

F. Review, Rating Sites Generate Claims from Defamation to Extortion

Review and rating sites, a popular feature of social media, are quickly gaining ground with consumers and, therefore, quickly attracting the attention of businesses that have products and services featured there. Businesses that contend they are harmed by these sites are invoking a variety of legal theories to fight back – including claims for defamation, disparagement, unfair trade practices, and even extortion.

Nemet Chevrolet Ltd. filed a lawsuit against the operators of a consumer advocacy website, Consumeraffairs.com, claiming that the operators did far more than simply create a platform where consumers could post complaints, and were so involved in soliciting and developing complaints that they should be liable for defamation and tortious interference with


120 Id. (Complaint ¶ 8).

121 The court’s handwritten order said nothing more about the grounds for dismissal, but the motion to dismiss had argued that the Tweeted statement was imprecise, contained no verifiable facts, and when considered in the context of her other Tweets, should be subject to Illinois’ innocent construction doctrine. Id. (Jan. 20, 2010) (Order of Dismissal), available at Citizen Media Law Project, http://www.citmedialaw.org/sites/citmedialaw.org/files/2010-01-20-Horizon%20v.%20Bonnen%20Dismissal%20Order.pdf.
business expectancy. Specifically, the dealership alleged that Consumeraffairs.com solicited complaints, steered the complaints into a specific category designed to attract consumer class action lawyers, contacted consumers to ask questions about the complaints and help them draft and revise the complaints, and promised consumers they could obtain some financial recovery by joining a class action lawsuit. The dealership then argued that the structure and purpose of the website encouraged users to post allegedly tortious content, transforming Consumeraffairs.com into an information content provider, and not a mere poster of content generated by others. Thus, Nemet Chevrolet argued, Consumeraffairs.com should be liable for the content of the complaints and should not be entitled to immunity under the CDA.122

The district court disagreed, granting a motion to dismiss on the ground that the CDA’s safe harbor provision shielded Consumeraffairs.com from liability, and the Fourth Circuit affirmed that decision. The Fourth Circuit noted that in this case, the dealership merely alleged that the site operators structured the website to solicit information related to class action lawsuits, and that was not an illegal activity. Thus, the court held, the CDA’s safe harbor provision conferred immunity on Consumeraffairs.com and barred the dealership’s lawsuit.

Another recent dispute between businesses and a review site, this one involving Yelp.com, has generated claims of extortion against the site operator.123 Yelp.com, with the trademarked slogan “Real reviews. Real people,” describes itself as “an online urban city guide that helps people find cool places to eat, shop, drink, relax and play, based on the informed opinions of a vibrant and active community of locals in the know.”124 Yelp creates a page for an individual business, including its contact information, and invites anyone who signs up for a free Yelp account to review the business and rate it on a five-star system. Yelp.com features more than 9 million reviews for businesses across more than 30 markets in North America and Europe, and it claims to have some 30 million visitors each month. The company relies solely on advertising for revenue.

Since February 2010, California businesses have brought at least three class action lawsuits against Yelp, alleging that the company manipulates reviewer content on its site to benefit businesses that agree to advertise with it and punish businesses that refuse to advertise with it.125 The complaints quote Yelp sales personnel promising to remove negative reviews or move them to the bottom of a listing page where fewer searchers will read them if the business agrees to buy a monthly advertising subscription from Yelp. Companies that refused to advertise, on the other hand, found that their positive reviews disappeared from the site,

122 Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250 (4th Cir. 2009); Nemet Chevrolet argued that the actions of Consumeraffairs.com were akin to those of Roommates.com, which prompted the Ninth Circuit to hold that it was a content provider because it required users to post content that violated the federal Fair Housing Act.


according to the complaints. Thus, as one complaint alleges, Yelp “capitalizes on the presumed integrity of the Yelp.com ratings system to extort business owners to purchase advertising.”

Yelp has responded that it has no control over which comments are removed or flagged and that the reviews at issue are deleted by an automated filter designed to weed out “shill” ratings, those encouraged or actually written by the businesses in question, to ensure that only independent and relevant comments remain.

G. Terms of Use

Hosts of social media sites and other websites rely in part on terms of use, sometimes called terms of service, to try to limit liability for defamation and disparagement claims arising from posts by third parties. Most terms of use include provisions that are duplicative and sometimes contradictory. They require users to agree not to post defamatory or disparaging content. They provide that the host has no responsibility for the content posted, but they also provide that the host acquires ownership of the content posted, or at least full rights to exploit it. They provide that the host will not monitor content posted, but they also provide that the host may edit or remove the content posted for a laundry list of reasons or for no reason at all. They also provide that users will indemnify the host for any liability arising from any content posted.

Twitter’s terms of service illustrate this attempt to limit liability. They state:

All Content, whether publicly posted or privately transmitted, is the sole responsibility of the person who originated such Content. We may not monitor or control the Content posted via the Services, and we cannot take responsibility for such Content. . . . . We do not endorse, support, represent or guarantee the completeness, truthfulness, accuracy, or reliability of any Content or communications posted via the Services or endorse any opinions expressed via the Services. . . . Under no circumstances will Twitter be liable in any way for any Content.

At the same time, however, Twitter takes a worldwide, royalty-free license to use and sublicense the content and make it available to its partners for syndication, broadcast, and publication, “all without any compensation to the user.”

Foursquare’s terms of use are more stringent with respect to how the service may deal with defamatory or disparaging content. Foursquare tells users of its site:

You are responsible for all of your activity in connection with the Service. . . . [Y]ou shall not . . . either (a) take any action or (b) upload, download, post, submit or otherwise distribute or facilitate distribution of any Content on or through the Service, including without limitation any User Submission, that: . . . you know is false, misleading, untruthful or inaccurate; [or] is unlawful, threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent,

126 Christine LaPausky d/b/a D’ames Day Spa, No. 2:10-cv-01578 (Complaint ¶ 43).
129 Id.
invasive of another’s privacy, tortious, obscene, offensive, or profane . . .
Foursquare has no obligation to monitor the Site, Service, Content, or User Submissions. However, Foursquare reserves the right to (i) remove, edit or modify any Content in its sole discretion, including without limitation any User Submissions, from the Site or Service at any time, without notice to you and for any reason . . . or for no reason at all and (ii) to remove or block any User Submissions from the Service.\(^\text{130}\)

Many social networking sites, such as Facebook, do not allow any alteration of their terms of use – including having companies create their own terms of use. Some companies have tried to avoid this by creating their own binding terms and posting them on their profile, but this strategy by and large has not been successful.\(^\text{131}\) Even if a business puts its own terms of use on its Facebook page, Facebook can restrict the content of those terms.

**H. Practice Tips**

The practical reality that prompted the passage of the CDA is one that every business owner contemplating social media must face: The amount of information communicated on the internet is staggering. The sheer volume makes it impossible to screen every post for defamatory or disparaging content – even if screening were a good thing, which is by no means a given. Businesses that engage in social media relinquish exclusive control over the content of their websites and, arguably, as a result, they accept an increased risk of liability for defamatory or disparaging statements made on their sites.

To take full advantage of the safe harbor from liability that the CDA provides, businesses must make sure they do not engage in activities that can transform their status from interactive computer service providers, which are protected under the statute, to information content providers, which are not protected. Activities that might result in a business being deemed an information content provider include encouraging users to post illegal content or designing a site that fosters the submission and publication of illegal content; soliciting content that is actionable as defamation or disparagement; and trying to influence the content that users submit, either by providing examples or by giving guidelines to users for that purpose.

Although the CDA’s “Good Samaritan” provision permits businesses acting in “good faith” to take down content that is objectionable, they must be careful not to go too far in altering text. It is safer to withdraw posts altogether if they contain objectionable or actionable material, rather than try to edit them. Editing creates a fact issue as to how, why, and how much the original text was altered, making any quick disposition of a case hard to achieve. Editing also may put safe harbor status at risk, in that the more editors alter text, the more they risk being deemed unprotected “information content providers” under the statute.

Terms of use permit businesses to lay the groundwork for avoiding liability for defamation and disparagement in several important ways. Terms of use should:

- Prohibit the posting of defamatory or deceptive content, as a condition of using the site;

---


• Allow the company maximum discretion to take down any content that violates this prohibition;
• Disclaim all responsibility and liability for the content of the UGC; and
• Include a provision for the creator of UGC to indemnify the company in any legal action over the UGC (recognizing that this protection is only as good as the resources of the party giving the indemnification);

It is not enough to have terms and conditions; UGC must be monitored regularly to ensure compliance.

It is also important for businesses to have policies in place for dealing with defamatory or disparaging content posted by their own employees – including requirements for the employees to identify their status as employees when commenting on matters related to the business and to make clear that the views they express are their own, not the company’s.

For additional protection, companies should consider obtaining insurance coverage against defamation and disparagement claims, through a commercial general liability policy, a media liability policy, or a cyber liability policy.

V. COPYRIGHT INFRINGEMENT CLAIMS FOR USER GENERATED CONTENT

Social networking communities are developed by users sharing not only information about themselves and their interests, but materials such as movie clips, photographs and music to show what they like or dislike or to engage others in discussion. On any site that allows users to post content, the possibility exists that such content may contain materials that infringe the copyright of a third party. For example, a user may post content that includes recorded music or a film clip without authorization from the copyright owner. To protect the site host from potential liability for copyright infringement from user generated content (“UGC”) in the interests of fostering online communications, Congress passed Section 512 of the Digital Millennium Copyright Act (“DMCA”) in 1998. The DMCA includes a notice and demand procedure for copyright owners to use, with a “safe harbor” from copyright infringement for online service providers that follow certain prescribed conduct.

A. DMCA Section 512 Takedown Demands

The DMCA provides a “takedown” mechanism for a copyright owner to request removal of material the owner believes infringes its copyright. Upon receipt of proper notice from a copyright owner, the online service provider may remove the copyrighted material to avoid liability for copyright infringement as a publisher of the infringing material. For example, to report a copyright infringement claim for material posted on Facebook, Facebook provides the option of filling out an automated DMCA form or submitting a DMCA notice to its designated agent. The technical aspects of the obligations of the copyright owners and online service providers have been the focus of disputes under the DMA takedown provisions.132

To provide an effective takedown notice of claimed infringement, the copyright owner must provide the designated agent of an online service provider with a written communication

---

that includes substantially the following: (i) a physical or electronic signature of a person authorized to act on behalf of the copyright owner; (ii) identification of the copyrighted work claimed to be infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site; (iii) identification of the material that is claimed to be infringing and that is to be removed, and information reasonably sufficient to permit the service provider to locate the material; (iv) contact information for the copyright owner; (v) a statement that the copyright owner has a good faith belief that material is infringing; and (vi) a statement notice is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the copyright owner.133

The requirement that the copyright owner state “a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law”134 has been the subject of several disputes. A colorable cause of action for copyright infringement would support such a good faith belief.135 If the basis for the takedown notice is improper but the service provider takes down the material in response to a demand, the takedown will have no effect in creating potential liability for the service provider. Further, if a court finds that a material misrepresentation was made by claiming infringement in the takedown notice, the copyright owner may be exposed to liability for issuing its takedown notice in bad faith.136

The copyright owner must form a “subjective” good faith belief that there is infringement before issuing a takedown notice.137 As was recently held in Lenz v. Universal Music Corp., the consideration of the fair use defense by the copyright owner is a factor in the subjective good faith analysis.138 In Lenz, a YouTube user filed an action against the copyright owner for issuing a takedown notice in bad faith against the user’s home video showing her toddler son dancing to a recording of the copyrighted Prince song, “Let’s Go Crazy.” The user claimed to have posted the 29-second video to show friends and family members. In denying a motion to dismiss by the defendant copyright owner, the court stated that copyright owners should consider the applicability of the fair use defense in their initial review of potential infringing material before sending a takedown notice under the DMCA. The court found that an allegation that a copyright owner acted in bad faith by issuing a takedown order without properly considering possible application of the fair use doctrine to this video was sufficient to state a misrepresentation claim under Section 512(f) of the DMCA.139

Cases discussing improper takedown notices are fact specific, but have established a few general principles limiting copyright owners’ use of takedown notices to address widespread copyright infringement. A blanket infringement notice that does not specifically identify the

---

134 Id. § 512(c)(3)(A)(v).
135 Rossi v. Motion Picture Ass’n of America, Inc., 391 F.3d 1000, 1004 (9th Cir. 2004) (subjective standard of review applies to takedown notice; affirming decision that MPAA takedown notice was not sent in bad faith).
136 Sections 512(f), (g)(1) supra note 133.
137 Rossi, 391 F.3d at 1004; see also Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004).
138 Lenz v. Universal Music Corp., 572 F. Supp 2d. 1150, 1155-56 (N.D. Cal. 2008); see also, 17 U.S.C. § 107 (the fair use defense to copyright infringement provides protection from infringement claims for such works such as criticism, comment, news reporting, teaching, scholarship and research).
139 Lenz, 572 F. Supp 2d. at 1153-56.
allegedly infringing work is improper. For example, in *Arista Records, Inc. v. MP3Board, Inc.*, the court found that a takedown notice was not effective notification because it did not specify links to the potentially infringing posts or identify specific songs that were infringed among a list of representative artists.\(^{140}\) The court found a second takedown letter sent by Arista ineffective because it did not provide “location information reasonably specific to locate” the infringing material. Additionally, in *Hendrickson v. Amazon.com, Inc.*, the court stated that “[t]he DMCA places the burden on the copyright owner to monitor the internet for potentially infringing sales . . . it was not the intention of Congress that a copyright owner could write one blanket notice to all service providers alerting them of infringing material, thus relieving him [the copyright owner] of any further responsibility and, thereby, placing the onus forever on the ISP.”\(^{141}\)

Similarly, the recent decision in Viacom’s suit against YouTube resulted in a grant of summary judgment to YouTube based on YouTube’s lack of knowledge of “specific and identifiable infringements of particular individual items.” Viacom claimed that YouTube (owned by Google) was generally liable for intentional infringement of thousands of Viacom’s copyrighted works, through both direct and vicarious infringement, because the copyright infringement occurring through YouTube was apparent, YouTube received a financial benefit from the infringement, and YouTube’s conduct was more active than the hosting protected by Section 512. YouTube had removed the specific materials that Viacom identified in takedown notices, including one massive takedown notice that identified 100,000 videos. The court held that the DMCA’s requirement of the service provider’s “knowledge” of an alleged infringement refers to specific infringements of particular items, not general knowledge of infringing behavior. The court also noted that the infringing material likely constitutes a small fraction of the material posted to a user-generated content site such as YouTube, and YouTube had in place an effective notification and response procedure under the safe harbor provisions of the DMCA.\(^{142}\)

### B. Compliance with DMCA to Benefit from Safe Harbor

The DMCA safe harbor provisions providing immunity from copyright infringement claims are available only to certain types of web hosting services and other online service providers. Qualified service providers are those engaged in (1) transitory digital network communications (e.g., transmitting digital information from one point on a network to another at user’s request); (2) system caching (e.g., data storage); (3) storage of information on systems or networks at users direction (e.g., chat rooms); or (4) information location tools (e.g., search engines).\(^{143}\)

For the service provider to benefit from the DMCA safe harbor provisions, it must designate an agent to receive notices of claimed copyright infringement; provide notice of the agent and its contact information to the public, usually in its terms of use; and notify the Copyright Office of its agent and contact information.\(^{144}\) In addition, a court must find that the service provider (1) adopted and reasonably implemented a policy that informs subscribers/account holders that service may be terminated if they are repeat infringers; and (2)


\(^{142}\) *Viacom Int’l Inc. v. YouTube, Inc.*, 2010 WL 2532404, at *1-*9 (S.D.N.Y. June 23, 2010). According to the opinion, over 24 hours of new video are uploaded to the YouTube site every minute.

\(^{143}\) Section 512, *supra* note 133.

\(^{144}\) *Id.* § 512(c)(2).
accommodates and does not interfere with standard technical measures used by copyright owners to identify protected works on reasonable and nondiscriminatory terms.145

Upon receipt of a proper notice from the copyright owner, the service provider must take down the allegedly infringing materials and notify the user who posted the materials. The site user or subscriber who posted the materials then has ten days to provide a counter-notification explaining why the materials are non-infringing. To be effective, a counter-notification must be a written notice that includes (1) a physical or electronic signature of the subscriber, (2) identification of the material that has been removed or disabled, (3) location of the material before it was removed or disabled, (4) a statement under penalty of perjury that “the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material removed or disabled,” and (5) the subscriber’s name, address, telephone number and a jurisdictional consent statement. This counter-notification must be sent to the service provider’s designated agent.146

Upon receipt of the counter-notification, the service provider must promptly provide the copyright owner with a copy of the counter-notification, and inform the copyright owner that it will restore the removed material in ten business days. The service provider may restore the removed material between ten and fourteen business days following receipt of the counter-notification unless it receives notice from the copyright owner that it has filed litigation to enjoin the infringement.147

If the service provider is in compliance with these statutory provisions, its liability for copyright infringement based on materials posted by users of the social media may be limited by the DMCA. Specifically, monetary damages are completely barred and injunctive relief is limited to (1) restraining the service provider from providing access to infringing material; (2) restraining the service provider from providing access to a subscriber who has infringed; or (3) other relief if least burdensome to the service provider.148

The failure to qualify under the safe harbor provision does not necessarily make the service provider liable for copyright infringement because general defenses available to claims of copyright infringement, such as fair use, are still available.

While the notice and takedown procedures help protect copyright owners’ works in many situations, the procedures address the infringement through the online service provider rather than directly with the infringer. When their postings are removed from one site in response to a DMCA takedown notice, some recidivist infringers will simply move the infringing material to another site. Copyright owners may need to chase an infringer from site to site, if they cannot identify the infringer and pursue the infringer directly.

145 Id. § 512 (i); Perfect 10, Inc. v. CCBill LLC, 82 U.S.P.Q.2d 1161 (9th Cir. 2007). See also Perfect 10, Inc. v. Google, Inc., No. CV 04-9494 (C.D. Cal. July 26, 2010) (Google benefited from safe harbor for nearly all of Perfect 10’s takedown notices, including one that included “nested electronic folders containing over 70,000 distinct files”, and other notices that provided links to the infringers’ home pages, rather than specific URLs to the location of infringing material).

146 Section 512(g)(3), supra note 133.

147 Id. §§ 512(g)(2)(B)-(C).

148 Id. § 512 (j).
C. Practice Tips

Businesses that host user generated content should take all the necessary steps to protect themselves from possible liability for copyright infringement under the DMCA safe harbor provisions. These steps should include:

- Designating an agent for receipt of notice of claims of copyright or other intellectual property infringement;
- Registering that agent with the U.S. Copyright Office using the form provided at http://www.copyright.gov/onlinesp/;
- Responding to notices of claimed infringement, and any counter-notifications, in a timely manner; and
- Including a section in the site’s terms of use explaining the procedure for notice of claims of copyright infringement and informing the public of the designated copyright agent and his or her contact information.

Copyright owners concerned about infringing materials posted on third party sites by users should make a careful, subjective assessment whether the works are infringing when used in this manner. If so, the copyright owner or its representative should craft a DMCA takedown notice that carefully follows all the statutory requirements. The copyright owner can check the list of designated agents posted by the U.S. Copyright Office at http://www.copyright.gov/onlinesp/list/a_agents.html, and direct the notice to that agent. The copyright owner should consult with counsel before sending a notice, since penalties may be imposed for false claims under the DMCA. Of course, the copyright owner also can consider bringing a copyright infringement action directly against the infringer.

VI. TRADEMARK INFRINGEMENT IN SOCIAL MEDIA

Trademark owners have long been concerned about unauthorized use of their marks in the sale of genuine and counterfeit goods through user postings on auction sites and other social media. Unlike the protections for online service providers of the Communications Decency Act against defamation claims and the DMCA safe harbor provisions against claims of copyright infringement based on UGC, there is no comparable protection for online service providers against claims of trademark infringement based on user conduct. Yet trademark owners have an affirmative duty to police unauthorized uses of their marks to maintain their trademark rights. Further, the social media provide new avenues for users to “squat” on the brand names of trademark owners, which some social media address in their policies.

A. Contributory Infringement for Counterfeit Goods Posted by Users

The Second Circuit’s recent decision in Tiffany v. eBay sheds light on the obligations and accountability of an internet service provider concerning consumers’ use of third party marks on its website.

eBay is an internet marketplace that allows users to post listings to sell various goods, including “Tiffany” jewelry. As part of its advertising campaign, eBay purchased the keyword

---

149 “Cybersquatting” is the unauthorized use of another’s mark in a domain name in bad faith.
“Tiffany” to trigger placement of online advertisements of its auction services through sponsored links on Google and Yahoo! search results.\textsuperscript{150} This campaign notified someone searching for Tiffany goods on the internet that Tiffany products could be purchased through eBay.

Tiffany sued eBay for trademark infringement, claiming that eBay directly infringed its Tiffany trademark by displaying the mark and purchasing the sponsored links. The court held that eBay’s use of the mark on its website and in the sponsored links was not infringing. Specifically, the court stated that a mark may be lawfully used when its use is necessary to describe the trademark owner’s goods and does not imply false affiliation or endorsement. This type of use is known as nominative fair use and is considered a non-infringing use of a trademark. Specifically, the nominative fair use defense requires that (1) the particular product or service is not readily identifiable without the use of the trademark, (2) the trademark is only used in an amount that is reasonably necessary to identify the product or service; and (3) the use of the trademark does not suggest sponsorship or endorsement by trademark owner.\textsuperscript{151}

Tiffany also alleged that eBay was liable for the extensive marketing of counterfeit products identified by the Tiffany mark by users of its auction service. Third parties selling counterfeit products on eBay offered them as “Tiffany” products. The court found that eBay was not liable for contributory trademark infringement for facilitating the infringing conduct of counterfeit vendors. The court held, “for contributory infringement to lie, a service provider must have more than a general knowledge or reason to know that its service is being used to sell counterfeit goods [and] [s]ome contemporary knowledge of which particular listings are infringing or will infringe in the future is necessary.” eBay had adopted procedures for handling trademark owner’s claims concerning alleged counterfeit listings by removing the listings from the website, notifying sellers and buyers of the listing, canceling fees it earned from the listings, and directing purchasers not to complete the sale of the potentially counterfeit item. Because eBay promptly removes a listing after a counterfeit notice, it was not liable for any of the terminated listings. As explained by the court, eBay’s generalized knowledge that some of the “Tiffany” goods sold on its website could be counterfeit was not enough “to impose an affirmative duty to remedy the problem” without some evidence that eBay knew or had reason to know a listing was continuing to sell counterfeit “Tiffany” items. Indeed, “some contemporary knowledge of which particular listings are infringing or will infringe in the future is necessary.”\textsuperscript{152}

B. Infringement in Entertainment Software (Computer Games)

Second Life is a virtual world entertainment environment created by Linden Labs. Within the Second Life game, users interact with each other, participate in activities, acquire virtual products and use virtual services, and can create, trade and sell virtual property. According to statistics compiled by Second Life, in the first quarter of 2010 Second Life had 517,349 active users in March and 826,214 unique users with repeat logins.\textsuperscript{153} Some real-world brands, such as American Apparel, Starwood Hotels and Cisco, have created a presence on Second Life with a

\textsuperscript{150} Tiffany (NJ), Inc. v. eBay, Inc., 600 F.3d 93, 102 (2nd Cir. 2010).

\textsuperscript{151} Id. at 102-03.

\textsuperscript{152} Id. at 106-107.

separate island or other presentation and/or sales of their genuine products. These companies believe that they can promote their products and create new customers for their real-world products by marketing to the many users of the Second Life virtual world.

Other real-world brands have objected to third party sales of “counterfeit” virtual versions of their products or services on Second Life outside their control. In April 2009, Taser International filed a trademark infringement lawsuit against Second Life for the sale of Taser items in Second Life. However, shortly after filing the lawsuit, Taser filed a notice of voluntary dismissal and the case was dismissed without prejudice. Taser has not taken any additional public action against Second Life.

In another computer game case, a real-world nightclub in East Los Angeles known as the Play Pen objected to a virtual nightclub in the Grand Theft Auto: San Andreas game that it believed was too close to its trademark and identity. The Grand Theft Auto game took place in a setting based on East Los Angeles and featured a nightclub named Pig Pen. The defendant asserted nominative fair use, but the court held that defense did not apply because the game did not use the trademarked logo of the real-world nightclub. The virtual nightclub was a combination of various locations around East Los Angeles, which included some characteristics of the plaintiff’s real-world nightclub but lacked other identifiable characteristics. Nonetheless, the court found no trademark infringement because the virtual nightclub was protected under the First Amendment as an artistic work that was not explicitly misleading.

Some companies have created new brands for virtual goods that exist only in the virtual realm and not in real life. Eros is an example of such a company. It offers a range of adult-themed virtual products for sale on Second Life and is the owner of a U.S. Trademark Registration for SEXGEN, for “[p]roviding temporary use of non-downloadable software for animating three-dimensional virtual characters.” After bringing several actions against individual counterfeiters purporting to sell Eros products on Second Life, Eros filed a putative class action for copyright and trademark infringement against Linden Labs in the Northern District of California in September 2009. The suit alleges that Linden Labs permits the sale of unauthorized virtual goods, enabling others to infringe and failed to prevent infringement of Eros’ marks. The pending case appears to be the first to assert real-world branding rights for products that exist entirely in a virtual world/computer game. Another plaintiff in the action is an individual who alleges that Second Life permits the infringement of her copyright for clothing designs, which she, too, sells in Second Life.

The Second Life Terms of Service includes provisions that state, “in connection with Content you upload, publish, or submit to any part of the Service, you affirm, represent, and warrant that you own or have all necessary Intellectual Property Rights, licenses, consents, and

---


158 U.S. Registration No. 3,483,253.

159 First Amended Complaint, Eros, LLC v. Linden Research, Inc., ¶ 74 (N.D. Cal.) (No. 09-cv-04269).
permissions to use and authorize Linden Lab and users of Second Life to use the Content in the manner contemplated by the Service and these Terms of Service.\textsuperscript{160}

For protection of trademarks for virtual property, use of a trademark only in social media sites is sufficient use for trademark registration. The U.S. trademark registration owned by Eros, discussed above, is for temporary use of non-downloadable software. Use of a real-world brand in social media sites is another manner of use that brand owners may protect through registration. The United States Patent and Trademark Office has not identified a single class where all social networking services fall, so applications that recite typical social media activities are presently channeled into any or all of International Classes 38, 42 and 45.\textsuperscript{161}

C. Name Squatting on Social Media Sites

By now brand owners are all too familiar with cybersquatting, the reservation of a domain name including the brand owner’s mark by a third party with a bad faith intent to profit from use of the mark to generate web traffic or in other ways. As the social media have offered opportunities for users to identify themselves and their communities with page names or user names, “squatting” of brand owners’ marks for these page or community names also has grown.

Some unauthorized users of brand names in the social media context may be fans or offer criticism or commentary. Others deliberately intend to draw traffic intended for the brand owner through confusing use of the brand name so that the page or user name appears to originate from the brand owner. While the Uniform Domain Name Dispute Resolution Policy (UDRP) of the Internet Corporation for Assigned Names and Numbers (ICANN), and the federal Anti-Cybersquatting Consumer Protection Act (ACPA) may be invoked against domain name cybersquatters, they are not applicable to name squatting in social media. The recourse for name squatting in social media is reliance on the site’s terms of use and name policies, and trademark infringement litigation.

Several social media sites have taken steps to discourage users from name squatting by prohibiting and offering takedowns for page or user names that cause confusion with a brand owner’s rights. Social networking sites have different terms of use that state their policies for trademark infringement and offer different forms of relief. For example, Twitter has a name squatting policy that reserves to Twitter the “right to reclaim user names on behalf of businesses or individuals that hold legal claim or trademark on those user names.”\textsuperscript{162}

If a brand owner reports name squatting that may amount to trademark infringement, Twitter will consider the report filed by the brand owner and determine whether to take action. Twitter requires that the trademark infringement report includes specific information from the brand owner including the name of the reported account, the business account, the trademarked word or symbol, and the trademark registration number. A description of the violation must be included in the report along with a requested action, such as removing the account or transferring it to an existing business account of the brand owner. Since Twitter


\textsuperscript{162} Twitter Rules, supra note 84.
explicitly requires a trademark registration number in the report of a violation, a brand owner may have difficulty causing Twitter to remove a common law trademark.

Twitter treats as a trademark violation when an account uses “[a] company or business name, logo, or other trademark-protected materials in a manner that may mislead or confuse others or be used for financial gain.” Twitter will suspend an account only when it determines the holder has a “clear intent to mislead others through the unauthorized use of a trademark.” If the use of the account “appears to be confusing users, but is not purposefully passing itself off as the brand/company/product, the account holder will be notified and given an opportunity to clear up any potential confusion.” ¹⁶³

Twitter has guidelines that an account user should follow to clear up potential confusion. For example, “the user name should not include a trademarked name of the subject of the news feed/commentary/fan account.” Additionally, “the profile name should not be the trademarked name of the company or include the trademarked name in a misleading manner.” The account bio should include “a statement that distinguishes it from the real company, such as 'Unofficial Account,' 'Fan Account,' or 'Not affiliated with.'” Lastly, an account “should not use another's trademark, logo or other copyright-protected image without express permission.” ¹⁶⁴

Facebook also has policies to protect “other people’s rights.” Specifically, “Facebook users cannot post content or take any action on Facebook that infringes or violates someone else’s right or otherwise violates the law.” ¹⁶⁵ For non-copyright related infringement such as trademark claims, Facebook provides an automated infringement form that requires personal information such as name, address, telephone and email as well as a description of the alleged infringed rights, the location of the infringing content and how the rights are infringed. The form also requests confirmation that the person filing the complaint is the owner of the rights or authorized to act on behalf of the owner. ¹⁶⁶

Facebook’s recently adopted Community Pages may make it more difficult for brand owners to protect their marks. The Community Pages are dedicated to a community that wants to discuss a particular topic, with background information, user posts and “like” information. These pages may pertain to a particular brand but are not moderated by the brand owner. What recourse the brand owner may have to control use of its mark remains unclear. ¹⁶⁷

**D. Practice Tips**

Trademark owners should include social networking sites in their policing strategy and enforce their brands on social networking sites as they would in other media. Several new online vendor services have become available that search for trademark uses in social media, providing reports to the trademark owner which then can police the infringements with demand letters or infringement litigation where appropriate.

¹⁶⁴ Id.
¹⁶⁵ Facebook Terms of Use, supra note 95.
To assist in this effort, trademark owners should make an effort to cultivate positive relationships with social media sites that are popular among the target market for the owner’s products or services, and where trademark infringement may be likely to arise. This may involve participating in eBay’s Verified Rights Owner (VeRO) program or similar programs on other sites.\footnote{See eBay, VeRO, http://pages.ebay.com/vero/intro/index.html (last visited July 18, 2010).} Where the sites provide procedures for removal of material that infringes trademarks, the trademark owner should follow those procedures in requesting action by the service provider.

Whether or not the trademark owner decides to use social networking as an avenue for marketing its products and services, the owner can reserve for itself the various page, fan site, channel, user accounts and other names using the brand that are available on the social networking site to block possible name squatting. These names and any use of the brand by the trademark owner on social networking sites should meet the same brand standards criteria as in other media. If the trademark owner reserves any names using its trademarks that it plans to leave inactive, it should review the terms of use for each site to check for whether an account may be deactivated if it is inactive for a particular length of time. Based on this activity requirement, a business should plan on making posts to avoid termination of the account.\footnote{Id.}

Trademark owners should consider federal trademark registration for their important brands in the appropriate classes for social media, as well as in the classes for their core products or services. In addition, the terms of use on a trademark owner’s site should expressly claim ownership of its registered and unregistered trademarks, and state that unauthorized use may be a violation of trademark law subject to legal recourse.

**VII. INFORMATION DISCLOSURE THROUGH SOCIAL MEDIA**

**A. Employee Disclosure of Business Secrets**

The frequent posting and updating of social media accounts by authorized employees and others can result in the inadvertent disclosure of proprietary or commercially sensitive information. Unlike in the past when an agency or designated employee was responsible for public relations and media communications, which were vetted carefully before release, a business now may be discussed publicly online by authorized representatives, employees chatting about their day at work, vendors promoting their own businesses, and so forth. A hint of “breaking news” or “inside information” can be tantalizing to followers of the site, since gossip and scoops are a big part of what makes social media interesting to the public.

Businesses with an online presence often understand the importance of frequent, timely postings to enhance the “stickiness” of a social media site, which may cause the business to use a lesser degree of review or clearance before a post is made, or forego clearance altogether. A quick update about what happened during a meeting at work could disclose sensitive information about future business plans. Information about pending cases or personnel issues also could be disclosed with the blogger not recognizing that the information...
could be privileged or confidential. A starting point to address these types of disclosures is adoption of an employee social networking policy.

B. Social Media Sites that Request Disclosure of Proprietary or Commercially Sensitive Information

Some sites are structured to collect information generated by a business without authorization. Theflyonthewall.com ("FOTW") website provided access to financial news, rumors and other information via an online subscription. FOTW openly solicited investment firms’ in-house proprietary and confidential research, analysis and recommendations on investments from the employees and clients of investment firms, and posted those “Recommendations” before the daily opening of the stock market and before other media outlets posted similar information. Several of the investment firms whose reports were posted by FOTW filed suit alleging copyright infringement and misappropriation of their reports. Earlier this year, the FOTW was held liable for both copyright infringement and hot-news misappropriation based on this practice.

Another site seeking disclosures of confidential information is Wikileaks.org, a site “created as a safe haven for anonymous whistleblowers to expose government and corporate secrets.” This site revealed the emails of climate researchers that raised questions about climate change research. In April of 2010, the site posted materials concerning an attack in Iraq for which a United States soldier was charged with allegedly disclosing classified information to an unauthorized source. In July 2010 Wikileaks created national and international anxiety by making public on the internet over 91,000 United States military incident and intelligence reports on the war in Afghanistan from 2004 to 2010. Included in the release were records of military engagements, deadly accidents, enemy intelligence, and meetings with political leaders.

C. Disclosures in Violation of Specific Laws

Social media raise special concerns for companies subject to special regulations concerning disclosure of information. For example, publicly traded companies are governed by Regulation Fair Disclosure ("Regulation FD"). In 2000, the Securities and Exchange Commission (SEC) adopted Regulation FD to address the disclosure of information by publicly


171 Barclays Capital Inc. v. Theflyonthewall.com, 2010 WL 1005160, *9 (S.D.N.Y. 2010). Hot news misappropriation is a concept that originated with the Supreme Court decision in Int’l News Service v. Associated Press, 248 U.S. 215 (1918). The copying of “hot news” may be actionable misappropriation under a five-element test that requires that (1) “the information is gathered or generated at a cost,” (2) “the information is time sensitive,” (3) “defendant’s use of the information is free-riding off of the plaintiff,” (4) “the defendant is in direct competition with the plaintiff,” and (5) “the ability of others to free-ride off of the plaintiff would reduce the incentive to produce the product or service such that its existence or quality would be substantially threatened.” Barclays, 2010 WL 1005160, at *17.


traded companies. The purpose of Regulation FD is to prevent the selective disclosure of material non-public information. Specifically, when material nonpublic information is disclosed to certain individuals or entities such as stock analysts, or holders of a particular security, who may act on the information, the information must be disclosed publicly. In 2008, the SEC addressed appropriate circumstances for public disclosure on a website. The guidelines list several factors that a company should consider, such as whether the website is a recognized channel of distribution and whether posting the information on a company website makes it available to the securities marketplace in general.

An example of a recent SEC investigation of online posts concerns the posts by Whole Foods’ John Mackey. Over a six-year period, while CEO of Whole Foods Market, Mackey posted anonymous comments about rival Wild Oats Markets and its stock value. Some of the posts made under the name “rahodeb” (an anagram of his wife’s name, Deborah) included comments questioning why anyone would buy Wild Oat shares at $8 and stating that the Wild Oats company “clearly doesn’t know what it is doing . . . [and] has no value and no future.”

The source of the anonymous postings came to light when the FTC filed suit against Whole Foods to block its purchase of Wild Oats on antitrust grounds. That case settled in March 2009. As part of the settlement, Whole Foods agreed to divest 32 stores and relinquish and sell its intellectual property rights in Wild Oats, including the rights to “Wild Oats” brand. An additional consequence of the posts, however, was an investigation by the SEC to determine whether Mackey broke any laws as a result of his posts. Eventually, the SEC ended its investigation without pursuing any action against Whole Foods or Mackey.

Other specific laws that may be implicated by social media disclosures include laws concerning products liability, advertising, health care, fair housing, and more.

D. Anonymous Postings

Objectionable material may be posted anonymously to social media sites, which initially may stymie efforts to counter or remove the postings. The terms of use of some social media sites may include language that obligates the ISP to protect the blogger’s anonymity. Other social media sites may provide source information for anonymous posts in response to proper requests or subpoenas.

175 See generally, 17 CFR §§ 240, 243, 249.
176 Id. § 240.10b5-1.
177 Id. § 243.
To reveal the true identity of a blogger, a company may need to subpoena the ISP for information on the identity of the user that posted the objectionable material. Several recent cases have addressed this issue of the standards for forced disclosure, but the results among jurisdictions are inconsistent. For example, a Delaware court held that in order to subpoena information on an anonymous blogger, the “plaintiff must make a prima facie showing sufficient to withstand a motion for summary judgment.” The New Jersey Supreme Court held that a subpoena for anonymous information requires “1) notice to the target and an opportunity for the target to be heard; 2) fact specific pleadings; 3) a hearing to determine whether the plaintiff could survive a motion to dismiss and could set forth a prima facie claim with supporting evidence; and 4) assuming plaintiff survives the third hurdle, balancing the defendant’s First Amendment rights against the strength of plaintiff’s prima facie claim.”

In Illinois, Supreme Court Rule 224 permits the filing of a “John Doe” lawsuit solely for the purpose discovering “the identity of one who may be responsible in damages.” This independent lawsuit is for discovery only of the defendant’s identity. The requirements for the complaint are that it must name the party from whom discovery is sought, the reason why the proposed discovery is sought and the nature of the discovery. New York CPLR Section 3102 similarly permits pre-litigation discovery for the purpose of identifying a defendant. Civil subpoenas to obtain customer records (but not their contents) from ISPs are available under 18 U.S.C. Section 2702.

E. Discoverability of Electronically Stored Information

As amended in 2006, the Federal Rules of Civil Procedure governing discovery now apply to “electronically stored information.” The purpose of including the phrase “electronically stored information” (“ESI”) in the amended Rules was “to be broad enough to cover all current types of computer-based information and flexible enough to encompass future changes and developments.” Although traditionally ESI has been considered to include emails and documents stored on a computer or in a database, courts are increasingly willing to require information in social networking sites to be produced in response to narrowly tailored requests. Notably, the privacy policy of many service providers including Facebook and Twitter allow the disclosure of user information in response to subpoenas and court orders, creating one less obstacle in the discovery request of such information.

However, even if the information on the social media is considered discoverable, admissibility of the evidence and authentication issues may arise in court because website

---

183 Id.
187 FED. R. CIV. P. 26(a)(1), 33 & 34.
188 Id. 34 advisory committee’s note (2006 Amend.).
postings are considered out of court statements. Therefore, the content may be subject to a hearsay exception and its authenticity may need to be proved.\textsuperscript{191}

\section*{F. Practice Tips}

Businesses that are active in social networking should consider creating an internal policy for employees and other designees regarding social networking. The policy may describe the appropriate content for posts, the purpose of the sites, the culture and language of the sites, and topics that should not be discussed. A business may set up a system to quickly vet all or at least questionable comments before they are posted. Some businesses may have one policy applicable to agents or employees who are charged with establishing and maintaining the business’ social networking presence, and a different policy applicable to employees regarding their personal social networking posts. Often such policies are in addition to an employee handbook and/or involves additional training to help focus employees on the issues.

The potential discovery of information posted on social networking sites raises issues for businesses that use social media with respect to the preservation, retrieval and production of information posted on the sites after a discovery requests is made.\textsuperscript{192} To the extent that a business intends to use social media for advertising or other purposes, it should have a plan in place to handle its discovery obligations. The plan at a minimum should address preservation of information on social media, means to retrieve the information, and a plan for producing any relevant information found on the social media. This plan should be implemented when a complaint is filed along with any general document preservation policy in place.

\section*{VIII. EXAMPLES OF INTERNATIONAL CONCERNS}

The internet is borderless, and U.S. companies must be aware that their social media activities can and do attract viewers and participants from other countries. These countries’ laws may differ significantly from U.S. laws, with respect to advertising, intellectual property, defamation, privacy, and other issues. Most importantly, the safe harbors from liability for defamation and infringement, offered by U.S. laws such as the CDA and the DMCA, do not apply in other countries. To avoid the entanglements of the laws of foreign jurisdictions, U.S. businesses may limit participation in social media activities – such as contests and sweepstakes, in particular – to citizens of the United States.

Advertising offers a case in point. Internet advertising through social media reaches a worldwide audience. (Indeed, as Twitter points out to users: “What you say on Twitter may be viewed around the world instantly.”\textsuperscript{193}) Yet the United States regulates advertising differently than other countries do. In the United States, the Federal Trade Commission encourages comparative advertising, deeming it a source of important information for consumers as they make purchasing decisions. But other countries have different views of comparative advertising. Some allow it only in extremely limited circumstances, and some not at all.


A. **How Social Media Platforms Deal with Different Laws**

Social media platforms have dealt with the challenge of complying with different laws and regulations in different jurisdictions in various ways. Facebook, for example, includes in its terms of use “Special Provisions Applicable to Users Outside the United States.” The provisions state that users consent to having their personal data transferred to, and processed in, the United States. They also provide that individuals located in “a country embargoed by the United States” and individuals “on the U.S. Treasury Department’s list of Specially Designated Nationals” will not engage in commercial activities, such as advertising, on Facebook and will not operate a platform application or website. Facebook is available in more than 70 languages, and approximately 70 percent of Facebook’s users are outside the United States.

Twitter, on the other hand, has no special provisions related to use outside the United States, although Twitter claims that approximately 60 percent of its use is outside the United States. YouTube and Foursquare, likewise, do not address international considerations in their terms of use or terms of service.

B. **The European Union: Privacy Is Paramount**

In Europe, the primary law regulating social media is the European Union’s 2005 Directive on Unfair Commercial Practices, a consumer protection statute. In December 2009, the EU issued a new guidance clarifying the 2005 Directive’s application to social media. It is by no means a given, however, that meeting the EU’s requirements for social media will suffice to avoid liability in Europe, because each of the EU’s member states may enforce its own requirements as well.

Google experienced this problem firsthand in February 2010, when an Italian court convicted three of its executives for violating Italian privacy law by failing to block a video showing a group of teenagers bullying an autistic teenager. The criminal convictions occurred even though the EU’s 2000 Directive on e-Commerce provides a safe harbor for ISPs and does not hold them liable for third-party content, provided they take down any offensive content after receiving a complaint about it. Google officials said that although the video had been online

---


200 The EU’s Directive on E-Commerce, Council Directive 2000/31/EC, 2000 O.J. (L 178) 1. at Article 14, on “Hosting,” requires Member States to “ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts
for two months, they removed it within 24 hours after Google received a formal complaint about it, and they helped Italian police identify those responsible. The prosecutors contended that Google should have obtained consent from each party involved before permitting the video to be posted. The court sentenced the Google executives to six-month suspended jail sentences and fines. The Google officials were acquitted of criminal defamation charges. Google is appealing the conviction.

Analysts of European and U.S. laws have stated that the conviction calls attention to the importance European governments attach to privacy rights, explaining that while Americans see privacy as a consumer protection right, Europeans see it as a human dignity right. Google’s counsel has said that the company’s privacy policies, like its policies on hate speech, pornography, and extreme violence, are best applied uniformly around the world, because trying to meet all differing local standards “will make you tear your hair out and be paralyzed.”

The Italian government also is considering legislation requiring that videos uploaded by users to sites such as YouTube be prescreened for pornography or excessive violence. Internet providers would be required to shut down any site that does not comply with the decree or face fines that may exceed $200,000. This requirement would eliminate a fundamental feature of social media sites, which permit users to upload videos without any prior review.

C. Asia: Penalties Stiffer for Online Offenses than for Offline Offenses

In Asia, meanwhile, use of social media has grown exponentially, but traps for the unwary exist there. For example, in Indonesia, which has the world’s third largest number of Facebook users, the punishment for defamation online is more severe than offline. Relying on Indonesia’s 2008 Electronic Information and Transaction Law, authorities jailed a mother who sent an email to friends detailing complaints about the service she received at a Jakarta hospital. After a groundswell of online support, she was found not guilty in December 2009.

An Indonesian legislator, Ramadhan Pohan, explained to a New York Times reporter why the government has reacted so strongly against social media: “The problem is that many officials in government are paranoid about this new online content. They are old-style politicians and bureaucrats who, if you ask them, don’t have a Facebook or Twitter account. They don’t realize that in terms of democracy and freedom of expression, we’ve reached a kind of point of

expeditiously to remove or to disable access to the information.” The Directive, at Article 15, also forbids Member States from imposing on providers a general obligation to monitor the information they transmit or store.


204 Gov’t of the Rep. of Indonesia, Law No. 11 of 2008.

Reflecting this attitude, a conviction for defamation under Indonesia’s new electronic information law can result in up to six years in prison, compared to a maximum sentence of 14 months for defamation in offline media under the criminal code.

D. Practice Tips

The most significant fact to keep in mind is that the safe harbors from liability for defamation and infringement, offered by U.S. laws such as the CDA and the DMCA do not apply in other countries.

And cultural differences, as well as legal differences, must be taken into account. The differing views of privacy and its importance offer but one example.

To help minimize the legal risks involved in international use of social media for activities that are particularly heavily regulated, such as contests and sweepstakes, consider limiting participation, through terms of use, to residents of the United States.

IX. FRANCHISE ISSUES

Franchisors and franchisees alike are under pressure to make sales, maintain volume, and build brand loyalty in an increasingly competitive environment – all while keeping costs to a minimum. More and more, they are enlisting social media in this effort, both to connect with consumers and to recruit franchisees.

In some cases, franchisors are ahead of franchisees in adopting social media, and in some cases the reverse is true. The question of how much control franchisors should exert over the system’s social media presence – or, conversely, how much freedom franchisees should have in exerting a social media presence – is being played out in franchise systems everywhere. No matter how that balance is struck, franchisors and franchisees must coordinate their efforts to ensure that their use of social media is effective and consistent with the system’s overall brand-building efforts. An important tool for ensuring an effective, consistent social media presence is a social media policy and code of online conduct.

A. Establishing a Policy and a Code of Online Conduct

The first source of authority for establishing a social media policy and code of online conduct within a franchise system is the franchise agreement. Although most agreements do not make specific mention of social media, the provisions of the agreement related to advertising, control and use of the system’s trademarks, preserving confidentiality, and termination and post-termination obligations all fit into a social media policy.

Both law and technology are changing almost daily in the realm of social media, and any policies and codes established must be flexible enough to adapt to this dynamic environment. This may argue for keeping the social media policy and code in the operations manual, where changes are easier to make, rather than in the franchise agreement. If a franchise has company stores, it may be worthwhile to test a policy and code of conduct there first. If franchisees are ahead of the franchisor in adopting social media, their experiences can offer valuable guidance, and they can help enlist and engage others in the system to participate.

\[ Id. \]
Key issues to consider when setting a social media policy and code of conduct for a franchise system include the following:

- Maintain brand consistency. When franchisees establish their own web pages for their franchises, for example, the franchisor should control the domain names that they use. The same principle holds true for registering names with social media sites. Thus, for example, a franchisor may prohibit franchisees from using the system’s trademark as part of a Twitter handle. In addition, the franchisor may want to control the uses of trademarks and logos on franchisees’ social media sites and Facebook pages.

- Be transparent. Never assume the identity of a customer to post a comment – on your own site or on a competitor’s site. Never post anonymously when discussing matters related to the franchise system. Franchisees and employees must disclaim any authority to speak for the franchisor or the system, unless expressly given that authority.

- Do not post any content that is false, misleading, defamatory, disparaging, offensive, profane, sexually suggestive, or otherwise objectionable – not only because of the legal implications involved, but also to avoid harming the brand.

- Do not post any content that infringes the privacy rights or intellectual property rights of others.

- Do not discuss other franchisees, customers, vendors, employees, or competitors without authorization to do so.

- Do not post or comment on confidential or proprietary information or pending litigation. Be mindful of how such information can be inadvertently disclosed.

- Do not post any information in violation of securities laws or other laws or regulations.

- Abide by the terms of service and privacy policy of any third-party site you use.

- Think before posting. Every post should build, and not diminish, the goodwill of the brand.

- Hosting a social media site is a long term commitment. Do not start unless you are willing and able to post content and respond to users on a daily basis.

- If you start a social media site for a designated market area, make sure all franchisees in the area are onboard. And when posting offers limited to an individual franchise or group of franchises, make sure that limitation is clear.

- When posting offers, make sure they comply with applicable regulations or guidelines, such as those related to contests, sweepstakes, and giveaways, as well as those related to privacy. Postings and Tweets making such offers should direct consumers to the franchisor’s primary website for the full rules of a contest.
• Respond promptly to complaints and negative posts. Never use sarcasm or show hostility in responding to fans or customers. Some franchisors prefer to take responsibility for handling complaints, given the high visibility that social media can give to complainers. A quick, sincere, effective response to a complaint can transform a vocal complainer into a vocal fan of the brand.

• Every statement on the web is accessible worldwide, so geographic limitations should be stated where applicable, and international sensitivities should always be kept in mind.

Franchisors should provide training for franchisees and company employees on the use of social media, covering topics such as the basics of setting up social media sites, strategies for engaging customers and posting content, strategies for dealing with negative posts and complaints, and guidance on avoiding legal and regulatory pitfalls. With respect to franchisees, however, franchisors must be careful not to be so hands-on that they risk creating vicarious liability problems for themselves. For example, a franchisor can require its own employees to abide by certain policies on the use of social media, but it should merely recommend that franchisees adopt policies for their own employees.

Policies and codes of conduct are appropriate for governing business-related uses of social media, but they may be problematic for addressing personal uses by franchisees and employees. Guidelines may be more appropriate than policies in the personal context. Moreover, even if it were possible, as a practical matter, to monitor what employees and franchisees are saying in personal postings, such monitoring can create privacy and free speech concerns. Franchisors should consider disclosing their monitoring of social media, so that franchisees and others cannot then claim surprise at having their content monitored.

Another privacy concern arises from information gathered through social media about users, which can be beneficial for marketing by the franchisor and specific franchisees, as well as by third parties. Given the obligations to disclose data collection practices in privacy policies, the privacy policies for websites or social media sites should explicitly disclose whether information will be shared between a franchisor and its franchisees, or among franchisees, in addition to disclosing any possible sharing with third party marketers or researchers.

Finally, when a franchise relationship ends, the franchisor must ensure that web pages or social media sites operated by franchisees are terminated or transferred to the franchisor.

B. Using Social Media for Franchise Sales

Just as franchisors are using social media to connect with current and prospective customers, they are also using it to find and recruit prospective franchisees. This occurs in two ways: by using platforms such as blogs, LinkedIn, and Facebook to market a franchise opportunity and by “mining information” from social media sites to find prospects.

Franchisors using social media for franchise sales should develop a policy and code of conduct for employees governing this use and should educate employees on legal traps for the unwary. Because this use of social media can constitute advertising, it may implicate other federal and state regulatory schemes that cover franchise advertising.

One issue to consider is compliance with disclosure requirements. If a franchisor’s social media communications are deemed offers to sell franchises, that triggers certain state
requirements regarding franchise sales, such as mandatory filing and waiting periods, disclaimers, and content restrictions. The North American Securities Administrators Association (“NASAA”) in 2001 adopted a Statement of Policy Regarding Franchise Advertising on the Internet that eliminates some of these restrictions. The NASAA policy provides that communications about a franchise offering posted on a website are exempt from the requirements for filing advertising, as long as the franchisor discloses the URL address for the website where the ad appears on the cover page of its Franchise Disclosure Document (“FDD”) and the ad is not directed to any person in a state requiring prior registration.

Use of social media in connection with franchise sales can also create risks associated with offers of franchises in states where a franchisor is not registered. NASAA’s 1998 Statement of Policy Regarding Offers of Franchises on the Internet addresses this issue. It provides that internet offers do not have to be registered in a state as long as they make certain disclaimers, including that the offer is not directed to residents of that state, and as long as no sales are made in the state until the franchisor’s FDD has been registered there.

Another issue to consider is financial performance representations. With limited exceptions, the FTC Franchise Rule prohibits franchisors from making financial performance representations to prospective franchisees unless the representations are included in the system’s FDD. Neither the FTC Franchise Rule nor the FTC’s guidelines for complying with the rule address how statements made in the context of social media should be treated. But if financial information is mentioned in social media communications intended for prospective franchisees, the franchisor could risk liability unless the required disclosures are made.

Of course, in addition to addressing these franchising-specific issues, franchisors using social media must comply with all other requirements for use of social media in their franchise sales efforts. Thus, for example, if a franchisee’s posted testimonial for a franchisor was solicited by the franchisor, that fact would have to be disclosed in the franchisee’s posting, to comply with the transparency required in the FTC Guides, discussed in Section II above.

X. CONCLUSION

Social media can offer franchisors and franchisees huge rewards and huge risks as well. No matter which way the scales may tip in weighing these rewards and risks, however, one thing is certain: Social media cannot be ignored. Customers expect it. Competitors are heavily involved in it. And franchisees will engage in it with or without their franchisors. By learning to leverage the power of social media and avoid the pitfalls that can come with it, franchise systems can strengthen their brands as never before.

207 For a detailed discussion of franchise sales advertising requirements, see C. Been and S. Yatchak, A Basic Overview of Franchise and Consumer Advertising Standards, ABA 31st Annual Forum on Franchising (Oct. 2008).


APPENDIX A

SOCIAL MEDIA PLATFORMS

The primary forms of social media include:

- **Blogs**, which feature comments in the form of journal-type entries posted on a website, sponsored by a company or by an individual.

- **Microblogs**, which permit users to send brief updates, primarily by text messaging, instant messaging, and emailing. On Twitter, the most popular microblog, with more than 100 million registered users, these updates are limited to 140 characters and are called “Tweets.”

- **Social networking sites**, such as Facebook, LinkedIn, and MySpace, which allow individuals and companies to share information about themselves and connect with others. Facebook, one of the primary social media platforms and arguably one of the internet’s biggest successes ever, announced in July 2010 that it has reached the milestone of having 500 million users. These users spend more than 500 billion minutes a month on the site.

- **Video-sharing and photo-sharing sites**, such as YouTube and Flickr, which provide a distribution platform that allows people to watch and share their own videos and photographs with others.

- **Review sites**, such as Angie’s list and Yelp, which allow people to share their experiences and opinions about local products and services.

- **Marketplace sites**, such as eBay and Craigslist, which connect buyers and sellers of products and services, and matching sites, such as Roommates.com and Match.com, which help people find roommates or other companionship.

- **Wikis**, which are collaborative websites that let users read, write, and edit the articles they contain. Wikipedia, the most popular wiki, bills itself as “the free encyclopedia that anyone can edit.”

- **Chat rooms**, which are websites or server spaces on the internet where live “keyboard conversations” occur, usually organized on the basis of a specific topic. Chatroulette, for example, features live conversations audio and video.

- **Virtual worlds**, such as Second Life, on the internet, where users can customize an avatar and socialize using voice and text chat.

---


• **Crowdsourcing sites**, such as InnoCentive and Helium.com, which outsource tasks to a community. Essentially, a “seeker” organization posts a challenge on the site, “solvers” submit solutions to the challenge, and the seeker pays an award to the solver who best meets the solution requirements.

• **Group activity sites**, such as Foursquare, a site that offers users rewards for visiting certain participating locations and lets users connect with friends while there, and Groupon, a “collective buying power” site that features a different deal each day on products or services and can only offer the deal if a certain number of users sign up for it.
CORBY C. ANDERSON

Corby Anderson is a litigation partner in the Charlotte, North Carolina office of McGuireWoods, LLP. Her practice focuses on intellectual property, franchising, media law, and commercial litigation. She has represented business clients and others, from rap artists to race car drivers, in trial and appellate litigation involving trademark and copyright infringement claims, trade secret and noncompete claims, and other contract and business tort disputes. She has defended clients in nationwide class action litigation over the administration of franchise advertising funds, and in a variety of state class actions. She regularly counsels clients on intellectual property, advertising, Internet and social media issues, as well as franchise and distribution matters.

Corby has co-authored articles for the ABA Franchise Law Journal on Franchise Currents, the Initial Interest Confusion Doctrine, and the Antitrust Risks of Information Sharing, and she is currently a Topic and Article Editor for the Franchise Law Journal. She has written about Right of Publicity for the ABA First Amendment and Media Litigation Newsletter. She is co-author of the Fourth Circuit and North Carolina chapters of the Media Law Resource Center's annual 50-State Survey of Libel Law. She has written and spoken on topics ranging from the basics of franchise litigation to libel and privacy issues, to trademark dilution. In 2010, she was named one of North Carolina's "Legal Elite" and one of the "Best Lawyers in America," by WoodwardWhite, Inc.

Corby worked for 12 years as a reporter, editor, and publisher for a Washington, D.C.-based legal publisher before attending law school. After a clerkship on the U.S. Court of Federal Claims for the Honorable Eric G. Bruggink, she was appointed a special master to resolve discovery disputes in Boeing Co. v. United States, a major government contract case. Corby earned a B.A. magna cum laude from the College of William and Mary and a J.D. from the University of Virginia School of Law.
CAROL ANNE BEEN

Carol Anne Been is a partner in the Chicago office of Sonnenschein Nath & Rosenthal LLC. She leads the firm's Trademark, Copyright, Advertising and Transactional IP practice within the Intellectual Property & Technology group, and is a former chair of the IP&T group. Carol Anne has extensive experience in a wide range of intellectual property matters, with an emphasis on trademark, copyright, advertising, computer, internet, media, entertainment and publishing law, including internet and new media. She handles clearance, prosecution and portfolio management, counseling, transactions, licensing and disputes for intellectual property worldwide.

Carol Anne works with a range of clients that host and use social media, including FreeCreditReport.com. She advises clients on social media policies, terms of use and privacy policies, using the media to generate interest, drive traffic and increase revenues. She also works with clients on setting up and managing multinational and domestic e-commerce businesses. For more than 10 years, she has served as a panelist deciding domain name disputes under the Uniform Domain Name Dispute Resolution Procedures (UDRP) of the Internet Corporation for Assigned Names and Numbers (ICANN), working through the World Intellectual Property Organization (WIPO).

Carol Anne has been featured as a Strategic Lawyer for her work partnering with clients, in an article published in the ABA Journal. Her IP&T work and business counsel has been recognized in her Chambers USA ranking as one of America's Leading Lawyers for Business. She served a two-year term on the Governing Committee of the ABA Forum on Franchising. She served with the judges of the U.S. District Court for the Northern District of Illinois on a committee that developed new trademark and copyright jury instructions for the Seventh Circuit. Before law school, Carol Anne worked as a journalist for a National Public Radio member station, and started her law career as a clerk to the Hon. Harlington Wood, Jr. on the United States' Court of Appeals for the Seventh Circuit.

* On June 9, 2010, the partnerships of both Sonnenschein Nath & Rosenthal LLP and UK-based Denton Wilde Sapte LLP approved a combination to form SNR Denton, to become effective on September 30, 2010.