VENABLE LLP

white paper

MAY 2010

When Marketing Through Social Media, Legal Risks Can Go Viral

VENABLE LLP ON ONLINE MARKETING LAW

VENABLE LLP

white paper

MAY 2010

AUTHORS

Melissa Landau Steinman
Partner
Advertising and Marketing
202.344.4972

Mikhia Hawkins
Associate
Advertising and Marketing
202.344.4573

When Marketing Through Social Media, Legal Risks Can Go Viral

VENABLE LLP ON ONLINE MARKETING LAW

The exponential rise in popularity of social networking websites and other social media outlets such as Facebook, Twitter, LinkedIn, and individual blogs, is due in large part to their viral nature. Social networking sites are essentially self-promoting, in that users spread the word for the sites. The more quickly social networking sites grow, the more quickly they spread. The viral quality of social media makes it an appealing way for businesses to market products and services, and marketers have long recognized and tapped the potential of social media outlets. Many advertisers have conducted consumer promotions involving social media to generate attention to and participation in their promotions, thereby maximizing brand exposure. Incorporating social media into a marketing campaign is not, however, without legal risks. Companies utilizing the power of social media must be cognizant of the relevant legal issues in order to protect themselves from liability risks.

Trademark and Copyright Issues

It is of the utmost importance for companies to protect their own trademarks and copyrights when using social media to promote their brands. A company's brands and other intellectual property are often nearly as valuable as the products or services that they offer. Social media's capacity to facilitate informal and impromptu communication – oftentimes on a real-time basis – can aid companies in promoting their brands and disseminating copyrighted material, but it can also facilitate third-party abuse of a business' trademarks and copyrights.

When using social media, whether via a third party outlet or a company's own social media platforms, marketers should regularly monitor the use of their trademarks and copyrights. Companies should monitor their own social media outlets as well as third-party social media platforms to ensure that their intellectual property is not being misused by those providing content through the media outlets. Internet monitoring and screening services are available to monitor the use of your business' marks and copyrights on third-party sites, including checking social media sites for profile or user names that are identical or substantially similar to your company's name or brands. This form of business impersonation can damage a company's brand and reputation if left unchecked; such monitoring can also serve as a positive indicator of business success. Companies should consider reserving, on various social media sites, user names that match or closely resemble their trade names and marks.

Social networking sites generally have terms and conditions that prohibit trademark and copyright infringement, and many sites, such as Twitter, also have rules regarding business and/or celebrity impersonation. Twitter terms and conditions state, in relevant part:

> Using 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 may be considered a trademark policy violation. Accounts with clear intent to mislead others will be suspended; even if there is not an explicit trademark policy violation, attempts to mislead others may result in suspension.

Twitter has specific provisions governing business or individual impersonation and name squatting. A well-known lawsuit involving allegations of impersonation on Twitter involved Tony La Russa, Manager of the St. Louis Cardinals Major League baseball team. In May 2009, La Russa sued Twitter for trademark infringement for allowing an impersonator to use La Russa's name as a Twitter profile name and post offensive "tweets" under the name. The case was eventually settled. *Anthony La Russa v. Twitter, Inc.*, Case Number CGC-09-488101 (Cal. Super. Ct., San Fran. Co., May 6, 2009).

Many social media outlets have procedures by which entities or individuals can report trademark or copyright abuse to the outlet, which may then take appropriate actions, including suspending the responsible user's account and removing infringing content. In fact, many social media companies, including Facebook, YouTube, and Twitter, provide instructions specifically for submitting a take-down notice relating to allegedly copyright infringing content, a procedure that can afford the social media outlets some immunity under the federal Digital Millennium Copyright Act (which is discussed in detail below).

In addition, companies should have terms and conditions for their own social media outlets, with provisions specifying how to properly use the company's and/or third parties' intellectual property. Marketers conducting certain types of social media marketing campaigns, particularly promotions and user-generated content campaigns, should have rules in place that include specific prohibitions regarding trademark and copyright infringement and impersonation.

General Legal Standards Applicable to Social Media Marketing

The law treats advertising and marketing via social media just as it does similar practices as they are employed in the context of traditional media. The backbone of federal consumer protection law is Section 5 of the Federal Trade Commission Act, which is enforced by the Federal Trade Commission (the "FTC") and declares that unfair or deceptive acts or practices are unlawful. Most states have statutes modeled after the FTC Act, known as "mini-FTC Acts"; many of these laws expressly provide that the mini-FTC Act should be interpreted in accordance with FTC guidance and case law. States may also (or alternatively) have general false advertising laws, or prohibitions of specific types of deceptive and misleading conduct such as advertising misleading price comparisons, rebates or sweepstakes promotions. Social media marketing campaigns must comply with these laws and their implementing regulations.

As with advertising through any channel, marketers using social media must ensure that their advertising claims are truthful and accurate and that they have substantiation for their claims before disseminating them. They must also clearly and conspicuously disclose all material information regarding an offer in their advertisements.

Companies that have relationships with third-party affiliate marketers should ensure that those affiliates comply with advertising and marketing laws in marketing the companies' products or services through social media. Businesses should have agreements with affiliates requiring the affiliates to comply with all applicable federal, state, and local laws and regulations; it may be prudent to include specific representations and warranties by the affiliate with respect to compliance, with specific references to significant laws such as the FTC Act. The agreements should also have a provision whereby the affiliate agrees to indemnify the company (either though a mutual indemnification or otherwise) from liability arising out of the affiliate's conduct – preferably with a provision requiring that the affiliate carry sufficient insurance to fund the indemnification should it be triggered. On a related note, confidentiality provisions and related provisions ensuring data security have become increasingly important in the current legal environment, particularly in agreements involving cross-border activities where consumer personal information is collected online. Additionally, businesses should, to the extent it is feasible, monitor the advertising and marketing practices of affiliates and review their marketing materials before they are disseminated. A company should take similar measures with respect to third parties who market through social media outlets operated by the company.

A recent lawsuit in this area is *Swift v. Zynga Game Network Inc.*, No. CV-09-5443 (N.D. Cal. Nov. 17, 2009). In November 2009, Facebook was named in a federal consumer class action suit alleging that advertisers disseminated deceptive ads through games offered on the social media site, such as *Mafia Wars* and *Farmville*. The company that offers many of the games on Facebook, Zynga Game

Network Inc. ("Zynga"), was also named in the suit. The suit alleges that third party marketers published deceptive advertisements through Zynga-produced games on Facebook, and that Facebook and Zynga received payments for the ads. The suit seeks to hold Facebook and Zynga liable for its alleged involvement in the dissemination of the advertising.

<u>Complying with the Terms and Conditions of Social Media Outlets</u>

Social networking websites generally have terms and conditions in place that govern the use of their sites. Some sites' terms and conditions contain provisions specifically regulating advertising and other commercial practices conducted on the site, including consumer sweepstakes, contests, and giveaways.

LinkedIn, for example, prohibits users from disseminating any unsolicited or unauthorized advertising or promotional materials. Twitter prohibits the use of the site to disseminate mass unsolicited messages (*i.e.*, "spamming"). According to Twitter's rules, what constitutes "spamming" will evolve as the site responds to new tactics used by spammers. Twitter's rules list several factors that the site considers in determining what conduct constitutes spamming, including whether a Twitter user has followed a large number of users in a short amount of time; whether a user's Twitter updates consist mainly of links and not personal updates; and whether a user posts misleading links. Facebook has rules in place (discussed in detail below), which were substantially revised and updated last Fall, that specifically govern the administration and advertisement of promotions on the site.

In addition to complying with the provisions of a social networking site that are directly applicable to advertisers, when designing promotional activities, marketers should *also* take into account any rules that restrict *users'* involvement in advertising and other commercial activities on the site. A marketing campaign that leads consumers to violate a social networking site's terms and conditions could expose the marketer to liability, damage the marketer's standing among consumers, and lead the site to bar the marketer from conducting future marketing campaigns through the site.

Social networking sites frequently impose various other rules that restrict how a marketer can use their sites. For example, Facebook, YouTube and Twitter prohibit the uploading or posting of content that infringes a third party's rights, including intellectual property, privacy and publicity rights.

<u>Implementing Your Own Terms and Conditions</u>

If a marketer creates and/or administers its own social media platform, such as a blog or podcast, it should have in place terms and conditions governing use of the platform and should make the terms and conditions readily available to potential users. By providing guidelines governing the use of the site, carefully crafted terms and conditions can prevent both company employees and third parties from using the social media platform in an unlawful manner. To some extent, such terms and conditions may also shelter companies from liability for the actions of third parties and employees. Comprehensive terms and conditions should reflect a good faith, reasonable effort to control and police third-party and employee conduct with respect to the platform. Such efforts are often taken into consideration by courts and regulators in determining a marketer's level of responsibility for the conduct of third parties and employees.

A site's terms and conditions should prohibit unlawful use of the platform, and ideally should specify particular types of unlawful conduct in addition to a broadly prohibiting illegal activity. For example, the rules should bar use of the site in a manner that is defamatory, libelous, or infringing upon the company's or a third party's intellectual property rights or right of privacy/publicity. The terms and conditions should also expressly state that the company is not responsible for content published through the platform by third parties.

User-Generated Content

Oftentimes marketing campaigns involving social networking sites or other social media incorporate user-generated content into the campaigns. Whether it's a video or photo shared on a site, or messages that site users disseminate to members of network, user-generated content holds much promise as a marketing tool. Consumers who create content in connection with a marketing campaign may develop a strong connection with the promoted brand, and audiences are often drawn to the authenticity of the content and the notion that an everyday Joe may perhaps obtain some degree of fame through low-budget, amateur productions that he or she created. In addition, user-generated content comes with a relatively high degree of credibility in the eyes of consumers, particularly if the content was created by someone the consumer knows (for example, a "Tweet" between friends).

Soliciting user-generated content in connection with a marketing campaign comes with some risk of incurring legal liability for content created by an individual participating in the campaign. Incorporating user-generated content in a marketing campaign could expose the sponsor to liability for libel, copyright infringement, violation of one's right of privacy/publicity, deceptive advertising, trademark infringement, or other violations. The law affords social networking sites and marketers some limited shelter from liability stemming from user-generated content used for limited purposes, but gives marketers minimal protection for user-generated content when it is republished in connection with a promotion or other marketing campaign. Marketers can, however, take certain steps to minimize legal risks associated with campaigns that involve the dissemination of user-generated content through social media.

When conducting marketing campaigns in which participants can publish content that they created through a social media outlet, whether the outlet is administered by the marketer or a third-party, marketers should regularly monitor published content and remove or request removal of any postings that violate the marketer's rules or the third-party's rules, or otherwise pose a legal risk. Alternatively, or pending removal of the content, marketers can post a statement disclaiming any association with the content or the content creator, and perhaps also express disapproval of the content. When practicable, marketers should screen user-generated content before it is disseminated. If, in screening content, a marketer identifies any legal issues, it should promptly take appropriate steps to address each issue.

Marketers should also have in place clear (and easily accessible) terms and conditions governing the marketing campaign, and those rules should include specific provisions addressing user-generated content. Marketers should also adopt disclaimers stating that the company had no hand in producing the user-generated content used or published in connection with the marketing campaign and, where appropriate, stating that the content does not reflect the opinions of the marketer.

To provide protection from intellectual property infringement claims by creators of user-generated content used by a marketer, the marketer should obtain the consent of participating consumers to use such content and the terms and conditions for the campaign should grant the marketer the specific right to use the content without compensating the consumer. Companies can also require that participants execute a release agreement allowing the marketer to use the participant's content. To protect against infringement claims by third parties, companies should consider either: (a) prohibiting the use of third party content altogether; (b) restricting the use of third-party content to only content that is in the public domain; or (c) permitting the use of third-party content only when the participant has provided written releases from each third party permitting the use of such content. Marketers can also find creative ways to reduce legal risks while facilitating the screening process by limiting the content that consumers can create in connection with marketing campaign – for example, by providing consumers with a selection of content that they can choose from that the marketer has previously cleared.

Monitoring and Screening Social Media Content

When conducting marketing campaigns in which participants can post content that they created to a social networking site, marketers should regularly monitor the postings and remove or request removal of any postings that violate the marketer's rules or the site's rules, or otherwise pose a legal risk. Alternatively, pending removal of any content, marketers can post a statement disclaiming any association with the content or the content creator, and perhaps expressing disapproval of the content.

When practicable, marketers should screen user-generated content before it is disseminated. If, in screening content, a marketer identifies any legal issues, it should promptly take appropriate steps to address each issue.

There are companies that provide Internet monitoring and screening services, including companies that provide services focusing on social networking sites. Some of these services allow a marketer to provide certain terms (*e.g.*, company name) that it wants the service to search for on a regular basis, and the service will provide the search results. This allows companies to monitor their social media marketing campaigns and any content that is published regarding the company, thereby protecting its brand and limiting its liability exposure.

Sweepstakes, Contests, and Other Promotions

As with any marketing campaign, conducting a promotion through social media can be an effective means of reaching a broad audience and capturing the attention of consumers through fresh, appealing, and interactive marketing formats. Like social media itself, promotions are by their very nature interactive and can thus be seamlessly integrated with social media outlets in a manner that heightens consumer interest in a marketer's brand. Promotions involving prizes incentivize consumer conduct in a manner that increases exposure to the promoters brand and, as such, are self-promoting – consumers are more likely to inform people they know about a promotion if prizes are offered. Social networking sites and other social media allow consumers to spread the word about a promotion quickly and with ease. Thus, promotions are an optimal means of exploiting the viral nature of social media.

When conducting or publicizing promotions through social media, marketers must not keep in mind both the general legal requirements governing promotions (*e.g.,* the sweepstakes laws, the CAN-SPAM Act applicable to email marketing, privacy laws, etc.) and the applicable terms and conditions of the social media outlet being used to "spread the word" about the promotion.

Facebook's Guidelines for Promotions

On November 4, 2009, Facebook issued new Promotions Guidelines containing specific rules for conducting sweepstakes and contests on its website. These Promotions Guidelines, which supplement the site's existing Advertising Guidelines, set forth separate guidelines for administering a promotion on Facebook and for publicizing a promotion on the Facebook site. Under the rules, "administering a promotion" on Facebook means "operating any element of the promotion on Facebook or [by using] any part of the Facebook Platform" (a program that links Facebook to outside applications and websites). For example, collecting entries, conducting a drawing, judging entries, or notifying winners through Facebook constitutes administering an element of a promotion on the site. Publicizing a promotion, on the other hand, means "promoting, advertising or referencing a promotion in any way on Facebook or [through] any part of the Facebook Platform." This includes, for example, announcing a promotion through a status update or wall post.

Under the new Promotions Guidelines, a company does not have to obtain Facebook's consent merely to publicize a promotion on the site. To *administer* a promotion on Facebook, on the other hand, a company must obtain Facebook's prior written consent and the promotion must be administered through Facebook Platform. A marketer that plans to conduct a promotion on Facebook must submit materials to for the promotion to a Facebook Account Representative at least seven days before the start date of the promotion.

If Facebook users are allowed to enter through the site, then the promotion sponsor may allow entry only through a third-party Facebook Platform application. Entry into a promotion, whether administered or merely publicized on Facebook, cannot be conditioned upon a user providing content on the site, including posting content on a profile page, posting a status update, or uploading a photo onto a Facebook page. In contrast, a promotion sponsor may condition entry upon a user providing content through a third-party application. Further, specific disclosures regarding Facebook's non-affiliation with the promotion and the promotion sponsor's collection of data from entrants must appear adjacent to the entry field. The guidelines also require that the official rules for a promotion administered on Facebook include specific provisions, including an acknowledgment that Facebook is not affiliated with the promotion and a provision releasing the social networking site from liability. Various other requirements apply.

Other social networking sites may follow suit and establish comprehensive policies governing consumer promotions.

Marketers planning to conduct a promotion involving a social networking site should take great care to ensure that they comply with the site's terms and conditions, paying special attention to any advertising and promotion guidelines.

Endorsements and Testimonials in Social Media

The FTC recently amended its *Guides Concerning the Use of Endorsements and Testimonials in Advertising* (the "Guides"), which address endorsements by consumers, experts, organizations, and celebrities in advertising. The amendments, which took effect on December 1, 2009, clarify – among other things – how the Guides apply in the context of social and other "new media".

The amendments to the Guides add examples to illustrate how the longstanding requirements that "material connections" (*e.g.*, compensation arrangements) between advertisers and consumer endorsers must be disclosed. Under the Guides, a material connection is one that consumers generally would not expect and that may affect the credibility or weight of the endorsement.
In determining whether a disclosure is required, the threshold issue is whether an endorsement was made. If a blogger was paid to blog about the marketer's product, the blogger's favorable blog posts concerning the product will likely be considered an endorsement under the Guides. If, on the other hand, a blogger makes favorable comments about a marketer's product, but was in no way incentivized by the marketer to post any blog entry about the product, then the blogger's product review would <u>not</u> be considered an endorsement. Further, if that consumer receives a single free sample from a marketer and writes positively about it on a personal blog or on a public message board, his or her comments are not likely to be deemed an endorsement given the lack of any

continuing relationship with that advertiser that would suggest that the consumer is disseminating a sponsored message. But in some cases, receiving free products may warrant disclosure. The fundamental question with respect to whether an endorsement was made is whether the speaker is (1) acting independently or (2) acting on behalf of the advertiser (or its agent). If the latter, the speaker's statement is an endorsement. This is also important in the expert or celebrity context, where previously compensation or a free gift might not previously have been considered to be a "material connection," but may now warrant disclosure in certain circumstances in the social media context.

A material connection certainly exists between a company and its employees. Thus, when an employee makes favorable comments through social media regarding his or her employer, or its products or services, the employee must disclose the employment relationship. If a company encourages its companies to post blog entries or otherwise make favorable statements regarding the company or its products or services, the company should develop procedures and policies that employees must comply with to avoid violating the standards reflected in the Guides. In relevant situations, employees should generally be advised to disclose their employment relationship with the company and whether they are acting on behalf of the company (or, as if often the case, whether they are simply acting on their own behalf); the company may wish to consider limiting the forums through which employees can make comments or even prohibiting altogether comments about the company or its products or services in any online forum. In short, companies encouraging employees to provide endorsements through social media channels should have adequate controls in place to avoid legal liability for their employees' statements, and even if a company does not encourage employees to make comments about the company or its products or services through social media, it should nonetheless have policies in place concerning such conduct.

The amendments to the Guides also address the issue of who is responsible for a deceptive social media endorsement. The FTC recognizes that because the advertiser does not disseminate the endorsements made in blogs or other consumer-generated media, it does not have complete control over the contents of those statements. Nonetheless, the FTC has taken the position that if the advertiser initiated the process that led to these endorsements being made – *e.g.*, by providing products to well-known bloggers or to endorsers enrolled in word of mouth marketing programs – it is potentially liable for misleading statements made by those consumers. Whether liability will be imposed in these circumstances may turn on a determination that the advertiser chose to sponsor the consumer-generated content and, therefore, established an endorser-sponsor relationship. But in determining whether a marketer should be held responsible for a third party's statements through social media, the FTC will consider the marketer's efforts to advise endorsers of their responsibilities (*e.g.,* adoption of a blogger endorsements policy), monitor bloggers' online behavior, and deal with rogue endorsers (*e.g.,* ceasing providing free product to noncompliant bloggers).

Privacy and Data Security Issues Concerning the Use of Social Media

Using social media to promote one's brand, products, or services can also implicate privacy and data security issues. It is important for companies to be aware of these issues and take appropriate measures to minimize their exposure to liability related to personal data collection, use, and maintenance.

Social media companies like Facebook and Twitter generally have their own privacy policies that govern their use of consumer data and third-party conduct on the social media platform with respect to personal data. Marketers utilizing third-party social media outlets should ensure that their marketing campaigns do not encourage consumers or any other parties to engage practices that would violate the social media company's privacy policy, and marketers should also ensure that they are abiding by the policies as well. Companies that administer their own blogs and/or other social media platforms should also maintain comprehensive policies that disclose the company's data collection, use, and storage practices, and any responsibilities that third parties have as regards privacy and data security.

Operators of social media platforms must fulfill the promises they make in their privacy policies and elsewhere with respect to data security and privacy, and they must maintain reasonable personal data protection procedures. The FTC and states have targeted companies for failing to abide by their privacy policies and/or maintain adequate data security protocols.

Companies using social media in marketing campaigns should also be aware of legal and self-regulatory restrictions on privacy and data security practices as regards minors. The Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6506, and its implementing FTC regulations govern the online collection, use, and disclosure of personal information from children under 13 years of age. COPPA applies to any operator of a website or online service directed to children under 13 who collects personal information from children under 13, or who has actual knowledge that it is collecting or maintaining personal information from a child under 13. If data collection and use practices come within the scope of COPPA, the statute and its implementing regulations require the website operator to include a privacy notice on its site and make available a notice to parents regarding its information collection and use practices relating to children under 13. It also requires that the website operator obtain parental consent before collecting personal information from children under 13.

The Children's Advertising Review Unit ("CARU"), an industry-funded, self-regulatory body that reviews nationally disseminated, children-directed advertising, has guidelines concerning the collection, use, and storage of personal data from children. CARU's guidelines are consistent with COPPA and its implementing FTC regulations.

In addition, after some prodding by the FTC, leading industry associations developed the Self-Regulatory Program for Online

Behavioral Advertising in an effort to set standards for and police online "behavioral advertising," which is the practice of tracking a consumer's activities online (*e.g.*, the searches the consumer has conducted, the web pages visited, and the content viewed) in order to deliver advertising targeted to the consumer's interests. The self-regulatory program consists of seven principles that are aimed at ensuring that consumers have control over the collection of their personal information and that marketers protect consumers' data and privacy when engaging in behavioral advertising. Companies should adhere to these principles when undertaking behavioral advertising activities using social media.

In November 2007, Facebook introduced its Beacon advertisement system, which transmitted data from external websites to Facebook for the purpose of allowing targeted advertising to Facebook users. As part of the system, certain activities on partner websites were published on a Facebook user's news feed. In response to protests by many Facebook users, Beacon amended its user agreement policy. However, a class action lawsuit was filed against Facebook and marketers that used the Beacon service, including Blockbuster, Inc., Fandango, Inc., and Hotwire, Inc., among others, and the lawsuit was settled in September 2009. *Lane v. Facebook, Inc.*, Case No. 5:08-CV-03845-RS (N.D. Cal. Aug. 12, 2008). As part of the settlement, Facebook agreed to provide $9.5 million, minus $3 million for legal fees, to create a "Digital Trust Fund" dedicated to studying online privacy. Ultimately, the Beacon advertisement system was shut down, but Facebook continues to "push" the envelope with its privacy practices.

Legal Protections for Social Media Platforms

There are laws that afford website owners and operators, including social networking sites, some protection against legal liability for third-party content published on the sites. Two federal statutes in particular – the Communications Decency Act ("CDA") and the Digital Millennium Copyright Act ("DMCA") – provide some immunity from such liability. The DMCA's "take-down" procedures may provide a particularly valuable tool for marketers seeking to address copyright infringement without resorting to litigation.

The Communication Decency Act

The federal Communications Decency Act ("CDA") was enacted to provide Internet service providers and website operators broad protection from liability for content created by third parties. Section 230 of the CDA affords immunity to interactive computer service providers, which includes owners of websites such as Facebook, YouTube, and other social networking or user-generated content sites, for content posted by third-party users of the service.

The CDA does not, however, extend immunity to intellectual property laws, criminal laws, or state laws that are consistent with Section 230 of the CDA. In addition, an Internet service provider is not entitled to CDA immunity if it plays some role in the creation of the content, including by editing the content, or gives the appearance that it played such role; for example, by failing to make clear that it is publishing content that was created by a third party. Moreover, CDA does not protect marketers that publish content through a third party's Internet service or website; accordingly, a marketer may not be sheltered from liability arising from user-generated or other content that it disseminates through a third-party social networking site.

The Digital Millennium Copyright Act

The federal Digital Millennium Copyright Act ("DMCA") generally protects Internet "service providers", a term that has been interpreted broadly to include all website owners, from all monetary and most equitable relief for copyright infringement where a third party initiated the delivery of the allegedly infringing content and the service provider did not edit or selectively disseminate the content. The DMCA provides "take down" procedures through which service providers are immune from liability if they remove or disable access to content that allegedly infringes a copyright.

To be eligible for the DMCA "safe harbors," an Internet service provider must (1) establish a policy that provides for termination of a repeat infringer's access to the Internet service; (2) designate an agent registered with the U.S. Copyright Office to receive copyright infringement notices; and (3) promptly remove allegedly infringing content upon receiving notice of the alleged infringement.

Like the CDA, the DMCA does not shield non-ISP marketers from liability for third-party content disseminated through another party's Internet service. Thus, marketers utilizing user-generated content are not protected under the DMCA with respect to copyright-infringement if the content is published through a third party's Internet service (although they may access its protections if they own the website and follow the prescribed procedures). However, even marketers using third-party websites may request that an ISP remove third-party infringing content pursuant to its DMCA takedown procedures; the "accused" party is then given a chance to respond. A judiciously used DMCA takedown request may thus be a cost-effective means of addressing intellectual property infringement issues – particularly those where the infringer is overseas and difficult to reach in the United States courts due to jurisdictional issues.

Employer-Employee Issues

As discussed with respect to endorsements and testimonials above, employers should have reasonable policies and procedures in place with respect to employee use of social media to minimize exposure to liability for the statements of employees. Companies should prohibit employees from making negative comments about a competitor, and should implement controls over employees' use of social media to make favorable statements about the company or its products/services. Companies should also consider adopting policies concerning employee use of internal blogs, online news bulletins, and other internal media channels, in order to prevent internal issues that could potentially arise due to inappropriate, confidential, or other statements or conduct by employees in connection with the use of intra-company social media platforms.

Relevant case law indicates that users of social networking sites do not have a reasonable expectation of privacy from employers with respect to information on the users' profile pages. However, an employee may have a cause of action if an employer pressures an employee to reveal a password to a protected web page. In one case, waiters at a restaurant in New Jersey started a group discussion forum on a social networking site for the purpose of voicing their complaints about the restaurant. A manager of the restaurant discovered the site and demanded the password to the group forum web page, then fired two employees in the group after reviewing the web page. The terminated employees subsequently filed suit against the restaurant. The jury found that the employees did not have a reasonable expectation of privacy in the contents of the web page and that it was reasonable to assume that information on the page would be used by their employer. However, the jury found that the restaurant violated the federal Stored Communications Act by improperly coercing an employee to divulge the password for the web page and then using the password to access the page. *Pietrylo v. Hillstone Restaurant Group*, No. 2:06-cv-05754 (D. N.J. 2008).

Companies should proceed with caution when using information gathered from social media in screening prospective employees, including information on a candidate's profile pages on social networking sites. Such information could include an individual's ethnicity, religion, marital status, or sexual orientation, each of which can form the basis for unlawful discrimination claims.

Retaining Records Related to Use of Social Media

Companies using social media should retain records related to such use for a reasonable period of time in the event the records are needed in connection with a regulatory investigation or other legal proceeding. Information and communications conveyed through social media channels may become relevant to a legal or self-regulatory proceeding, and may ultimately be the subject of a subpoena or other compulsory process. Indeed, the legal action may not directly involve a company that has custody of relevant social media exchanges or information, but a regulatory, court, or other authority may nevertheless compel the company to produce the materials. Further, records related to a company's use of social media may also ultimately prove useful in supporting a company's position in a legal proceeding or in connection with a threatened proceeding.

Recent case law has imposed harsh penalties for spoliation of electronic records evidence and raised the bar for maintenance and production of electronic files such as databases, emails, and even personal data assistants in anticipation of and during litigation. Accordingly, it is important to implement sound records retention policies and procedures with respect to social media projects. Companies should consult with counsel for assistance in designing a sound policy that takes into account business requirements, current case law and relevant statutes of limitation.

*   *   *

Social networking sites can be effective platforms for advertising and marketing endeavors. Increasingly, marketers are using such sites as a vehicle to spread the word about a product or service through advertisements, promotions and other means. But marketing campaigns utilizing social networking sites unavoidably involve various third parties – including consumers, the social media outlets, marketing affiliates and potentially other third parties. Marketers must be aware of the legal issues raised by the involvement of these parties. In particular, campaigns that leave certain components of the campaign in the hands of the sites and/or users – as when users are encouraged to disseminate their own announcements regarding the marketing campaign through a social media outlet – can carry liability risks for marketers. By structuring campaigns properly and taking other steps to minimize legal risks, marketers can cash in on the marketing opportunities that social networking sites and other social media present without leaving themselves vulnerable.

Melissa Landau Steinman is a partner and Mikhia Hawkins is an associate in Venable LLP's Regulatory Group; they focus their practices on advertising, marketing and new media law. Ms. Steinman can be reached at (202) 344-4972 or mlsteinman@venable.com. Mr. Hawkins can be reached at 202-344-4573 or mehawkins@venable.com.