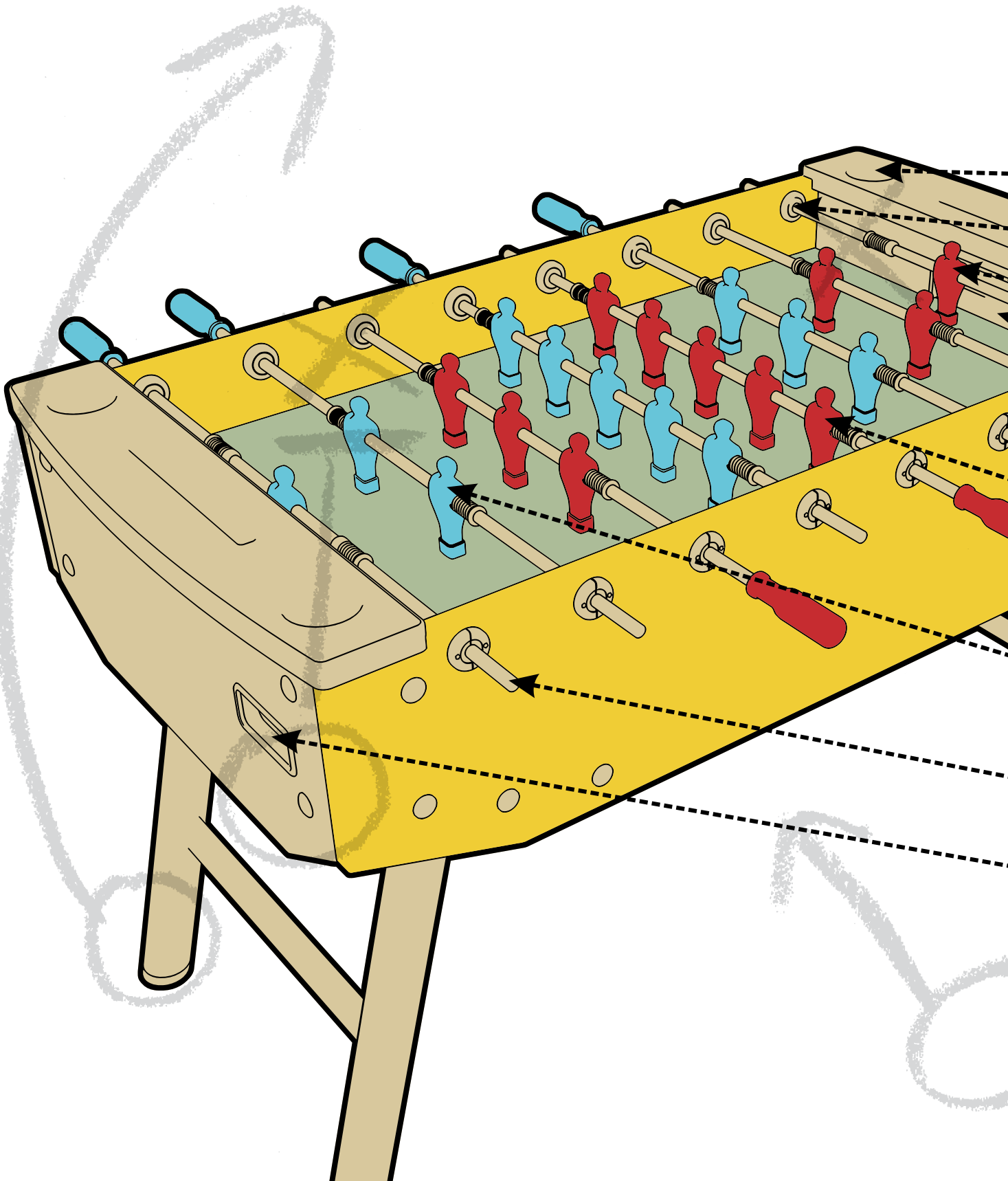


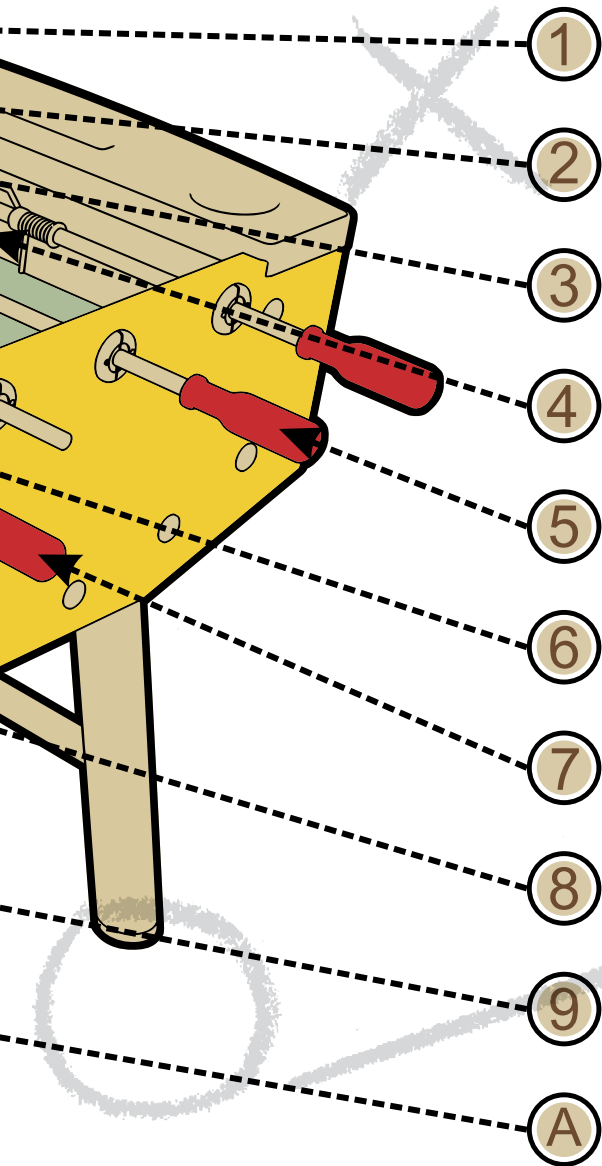
Social Media Game Plan:





IP and Marketing Law Playbook

BY FERAS MOUSILLI AND BARRY M. BENJAMIN



For corporate attorneys who are still waiting for the social media craze to fade away, you can no longer ignore the statistics: Two-thirds of the global internet population visit social media sites. If you believe your company can ignore the Facebook phenomenon, it would be tantamount to ignoring a market bigger than the eighth most populated country in the world. Social networking has exploded in popularity so quickly and become so ingrained in our daily lives that we can no longer think of it as “new media.”

Companies hosting and participating in social media face numerous potential legal minefields — new court decisions come at a dizzying pace, often interpreting relatively new statutes that lack established precedents. Furthermore, as the line between “company time” and “personal time” blurs, companies struggle with the right balance between an employee’s free speech rights and restrictions to protect the company when the employee engages in social media. Protecting company intellectual property is yet another challenge. Whether dealing with “friendly” (fan sites) or “unfriendly” (gripe sites) situations, fashioning appropriate, consistent responses can be an arduous task. There are, however, a number of measures that can minimize risks of engaging in social media.

Hosting social media — legal issues as a publisher

Companies that were long content to publish brochure-type websites now feel compelled to implement social media capabilities on their own websites — giving customers, the general public and employees the ability to interact, post and respond to messages, receive feedback, and even upload pictures and videos. Given the potential legal pitfalls, it is critical to ensure a strong business justification exists before implementing these capabilities — hosting social media by definition means losing some control over published content on your website. Negative comments invariably come with positive ones, and some may believe it is better not to engage with social media at all than publish derogatory comments about your own company. Editing out negative comments is possible, but such editorial control may bring cries of censorship and negative customer backlash. This is the legal, public relations and philosophical minefield to navigate when joining the social media club.

As the website host, your company is the publisher of everything on the site, including user generated content. As the publisher of potentially tortious statements, e.g., from angry consumers, you could be liable (vicariously or as contributors) for defamation. As a publisher, and under traditional theories, your company could also face liability for copyright infringement for works uploaded by someone who does not own all rights to the works.

Fortunately, federal law gives website owners that publish third party content (e.g., user generated content) certain legal “safe harbor” immunities from liability for tort and copyright claims. To gain these immunities, however, the website owner must take certain enumerable steps, based on the particular law at issue. Safe harbor from tort claims is provided by Section 230 of Title 47 of the United States Code,¹ which was passed as part of the Communication Decency Act of 1996 (the CDA), while immunity from copyright claims is provided by Section 512 of the Digital Millennium Copyright Act² (the DMCA).

Section 230 of the CDA

United States common law generally holds the publisher of a tortious statement to the same level of potential liability as the speaker of the tortious statement. The CDA, however, views the website host as merely a distributor of content and not as a traditional publisher, akin to a library providing access to a book, rather than a magazine publisher providing access to articles. The magazine publisher had the chance to review, edit and decide whether to



FERAS MOUSILLI is corporate counsel to Dell Inc., and specializes in intellectual property and technology law. He can be contacted at feras_mousilli@dell.com.



BARRY M. BENJAMIN is a partner in the New York office of Kilpatrick Stockton and chairs the firm's advertising, promotions and media group. He can be contacted at bbenjamin@kilpatrickstockton.com.

publish the problematic content, thus making the problematic content a statement by the magazine itself, as opposed to the library, which merely provides access. Thus, as long as the website host does not actively control tortious statements posted on its site by others, then the safe harbor immunity would apply. Note that this type of immunity applies only to state law civil claims, and does not apply to criminal claims or claims arising out of federal law such as trademark, copyright and patent law.³

Courts have interpreted the scope of the safe harbor immunity under CDA 230 to provide a very strong defense. Decisions consistently hold that websites exercising traditional editorial functions over user generated content, such as deciding whether to publish, remove or even edit material, are generally immunized under Section 230 as long as they do not appear to the reader to transform the statement into their own statement, or otherwise adopt or endorse it. The analysis of particular activities, however, gets more difficult the more the host “interacts” with the user’s statement, such as altering its content,

editing its meaning, or even altering similar statements while not altering others. The broad scope of the safe harbor immunity is such that as long as the website host does not appear to adopt the tortious statement as its own, or change the meaning of a user comment or statement, generally the immunity will apply. Thus, the key to preserving safe harbor immunity is to avoid converting user-generated content into a statement arguably attributable to your company as the website host.

CDA 230 provides safe harbor immunity in any number of situations. Pre-screening content prior to publication, according to court decisions, is immunized activity, even if the content turns out to be defamatory or otherwise tortious. Even after publication, the general rule is that as long as a website host does not change the substance or meaning of a statement, it may actively edit the content and maintain Section 230 immunity. That said, any editing is difficult without risking an accusation that the meaning was changed, or that the comment was adopted by the host via the edit. Thus, editing should be done in limited circumstances only, if at all.

As for soliciting or encouraging users to submit content, there is a difference between providing a forum for consumers to comment and specifically requesting or inviting user comments about a specific topic. Generally, soliciting content or comments from users is acceptable, and a website operator maintains its immunity. Do not, however, solicit the submission of illegal content, or design

the website to require users to input illegal content. The primary example of a website operator that faced liability when soliciting information is where a roommate-finding website service included drop down menus for users to specify characteristics such as race, sex and sexual orientation to assist their users in their search. By providing such drop-down menus, the court found that the website host may have engaged in discriminatory activity.⁴

The immunity provisions of the CDA are quite strong. As long as the website host does not appear to be the speaker of the wrongful statement, the immunities are generally preserved.

Section 512 of the DMCA

The DMCA was enacted to address specific issues created by the internet, namely, that traditional copyright law would render the mere transmission or displaying of a copyrighted work an automatic infringement. Thus, online service providers and website hosts would otherwise be liable for material transmitted through their computers. The DMCA safe harbor immunity, as distinguished from CDA 230, applies in copyright infringement situations, e.g., where a consumer copies and pastes a copyrighted article to the company's website, or where a consumer posts a

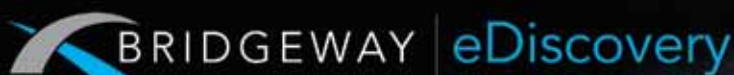
video using a copyrighted popular song, or even simply playing a copyrighted song in the background.

In order to gain and preserve DMCA safe harbor immunities, a website host must take affirmative steps outlined in the statute. Just as with the CDA, the DMCA's safe harbor immunities apply to third party content, not to content posted by the company itself — a company is not protected from claims based on its own infringing actions.

DMCA section 512 outlines the necessary requirements to avoid liability for either permitting access to copyrighted works uploaded by others, or permitting access to copyrighted works by linking or allowing others to link to those works. In order to avoid liability, the website host must:

- designate a copyright agent to receive DMCA take-down notices;
- adopt and implement a copyright infringement policy and "notice and take-down" procedures;
- promptly remove infringing content after notice;
- have no actual or effective knowledge that the material in question is infringing; and
- not directly benefit financially from publishing the material.

It is critical you promptly respond to take-down requests — 48 hours is a good time frame. You should not prevent



eDISCOVERY COMES AT YOU FAST ...
WITH BRIDGEWAY, YOU'RE IN CONTROL

Meet **all the challenges** of electronic discovery
with **one proven vendor**.

Bridgeway eDiscovery supports
in-house legal with :

- Preservation
- Collection
- Process
- Review
- Production

With Bridgeway, you're in Control. Call us today to find out how.

SALES INQUIRIES: 888.272.4699
WWW.BRIDGE-WAY.COM

ACC Extras on... IP and Marketing Law

ACC Docket

- *How You Can Safely Use Social Media with Employees (April 2010)*. This article focuses on using social networking sites at the pre-employment screening stage, and monitoring and regulating their use by current employees. www.acc.com/docket/safeuse-socmed_apr10
- *Trust, but Verify: The Reality of Data Protection in an Information-Driven World (May 2008)*. With eight primary elements, the comprehensive privacy protection and information security program described in this article is centered on people, processes and technical management that is standards-based whenever possible. www.acc.com/docket/dataprot_may08

Education

- Still need clarification on what social media is and how it can affect your company? Join us at ACC's 2010 Annual Meeting, Oct. 24-27 in San Antonio, for a two-part session on social media. Attend session 510 – Social Media for Novices (Part I): Tips for Joining the 21st Century, then apply those skills in with session 610 – Social Media for Novices (Part II): How Do You Protect Your Company from It? Visit www.acc.com/education/am10.

Sample Forms & Policies

- *Social Media Policy (Sept. 2009)*. This brief social media policy discusses respect and privacy rights components, as well as legal liability components. www.acc.com/forms/socmedpol_sep09

- *Social Media Policy Template (Feb. 2010)*. View this draft of a social media policy based upon a review of current best practices. www.acc.com/forms/socmedtemp_feb10

Quick Reference

- *Recommended Practices on Notice of Security Breach Involving Personal Information (May 2008)*. This reference provides safeguard practices to protect personalized information from unauthorized access. Includes a list of practices that should be included in an incident response plan to ensure timely notice to affected individuals. www.acc.com/quickref/secbrea_may08

Program Material

- *Is Privacy the Next Superfund? How to Navigate Privacy & Data Security Issues (Oct. 2007)*. Learn the basic concepts of privacy and data security, understand federal and state authority to regulate privacy practices and more. www.acc.com/navpriv&data_oct07

ACC has more material on this subject on our website. Visit www.acc.com, where you can browse our resources by practice area or use our search to find documents by keyword.

copyright owners from obtaining information for a proper take-down notice. Moreover, do not tolerate repeat offenders — limit or even block their access to your site.

Linking – a hidden source of potential copyright infringement claims

Difficult questions arise when you place links to third party content on your site. If you intentionally use copyrighted content on your website, you subject yourself to potential infringement liability. However, if you simply link to the copyrighted works published elsewhere, the risk is limited, although not quite clear. The question depends, in part, on the type of link used. While the specifics are beyond the scope of this article, the potential for infringement can decrease or increase depending on whether the link is “passive,” meaning one that takes the user to the actual website of a third party, or a link that frames that

information within your website. Furthermore, even if the linked content is framed on your own website, an infringement claim could depend on whether the technology you use retrieves the content from the original publisher each time the link is clicked, or if your site actually caches the content and displays the cached copy. Given the difficulties with determining the answer to this question, it is preferable to use passive links that direct the user away from your site to the original third party site where the content is posted.

Third party social media (e.g., Facebook and Twitter)

All of the above considers your company as the website publisher or host of user generated content. Obviously, other social media providers exist, including the tremendously popular Facebook and Twitter. In the rush to engage with social media, many companies now host their own pages

on various third party sites. All of the advice above also applies to engagement with these third party sites. That said, these third party sites have their own legal ‘Terms of Use,’ ‘Privacy Policies,’ ‘Promotion Guidelines’ and other policies that apply to your pages hosted within their systems. A thorough review of the website policies is necessary to fully understand the ramifications of the relationship.

Employees and social media

Drafting comprehensive policies and practices for employee participation in social media confounds even the savviest of companies. Companies continue to struggle with balancing regulation of an employee’s freedom of expression with protecting the company from employees regardless of their intentions. Obvious and traditional legal risks arising out of employees’ online dealings can range from disclosure of confidential information to the publication of biased statements that may be used as evidence in a discrimination lawsuit.

We will focus here on the recently revised Federal Trade Commission (FTC) guidelines on product endorsements, which reveal an often unforeseen risk: liability under a deceptive trade practice theory arising from false or misleading statements by employees commenting about products or services. With consumers turning more and more to blogs and other social media as sources for reviews and testimonials on products and services, the impact of social media cannot be understated for your brand reputation. Be aware, however, that a host of employment law issues in connection with social media exist that are beyond the scope of this article, including hiring, privacy, harassment, wrongful termination and defamation, among others.

The new FTC guidelines

Section 5 of the FTC Act⁵ prohibits businesses from engaging in unfair or deceptive trade acts or practices. Last updated in 1980, the FTC recently issued revised Guides Concerning the Use of Endorsements and Testimonials in Advertising, which now expressly cover advertising through “new media.” These guidelines define “endorsement” as an advertising message that consumers are likely to believe represents the opinions or experiences of a party other than the sponsoring advertiser. Under the guidelines, a business that pays or has an ongoing relationship with the endorser may be held liable for the endorser’s false or misleading statements about the business’s products or services. The business could also be held liable for the endorser’s failure to disclose the relationship between the endorser and the business, even if the business has no control over the content of the endorser’s statements.

If your employee discusses your company’s products or services on a personal blog or social-networking page,

that could certainly constitute an “endorsement” under the FTC’s guidelines because of the obvious employment relationship. Under the guidelines, even the simple failure to disclose the employment relationship in the endorsement can render an otherwise true and honest statement unlawfully misleading. The rationale is that from the consumer’s perspective, disclosure of the relationship impacts the credibility of the employee’s statement about the company, and the consumer deserves to know about it.

Under the guidelines, even the simple failure to disclose the employment relationship in the endorsement can render an otherwise true and honest statement unlawfully misleading.

Moreover, if the employer is found to be “sponsoring” the employee endorsements, it may be liable for any false or misleading statements in the employee’s message. Determining “sponsorship” can be a tricky undertaking. Of course, it is not so tricky when an employer directs or encourages its employees or contractors to promote the employer’s products or services on their company websites. In other situations, the FTC will consider a number of factors, including whether there is compensation from the business, the length of the relationship, and whether the endorsed products or services are offered to the individual free of charge. In the case of an employer and an employee, compensation could be wages, an employment relationship of significant duration, and, in some cases, the receipt of products or services free or at reduced prices. Thus, an employer could be found to be the sponsor of an employee’s, or even an independent contractor’s, online endorsement, even though the company did not request or direct control over the content.

In comments published with the revised guidelines, the FTC indicated it would consider the existence of the employer’s policies and procedures governing employee postings on blogs and social-networking sites, in determining whether the employer should be held liable for misleading employee endorsements on such sites. The FTC would

generally not pursue an enforcement action against an employer based on the actions of a single employee who violated a company policy that “adequately” covered the employee’s inappropriate endorsement.

Practical implications and corporate social media policy

As discussed, even if an employer did not actively solicit an employee endorsement, the new FTC guidelines suggest that the mere existence of an employment relationship may support a presumption of endorsement. To minimize the risk of liability in this situation, you should be proactive and implement a corporate social media policy that addresses employee statements about your company’s products or services on personal websites. Unfortunately, only about half of employers have a social media policy in place.⁶ A weekly Quick Poll on ACC’s website revealed that 39.8 percent of those who voted said their company has a social media policy for employees.

The social media policy should explicitly detail activities in which employees may not engage, and make it clear that they blog at their own risk and are personally responsible for their content. The policy should inform employees about what constitutes an employee/contractor endorsement, what disclosures must be made in connection with such endorsements, and what statements would be inappropriate. Many require personal activities to include a disclaimer along the lines of: “The views and opinions expressed here are my own personal views and do not necessarily represent the views or opinions of my employer.” In addition, the policy should require employees and contractors to submit proposed endorsements of company products or services to the company’s marketing or legal staff for approval before they are posted on the internet.

A social media policy should also address comments and endorsements of another company’s products or services. You face potential liability for employees’ online endorsements that relate to a third party’s goods and services when the company appears to be the endorser. For example, if the employee generated the content on paid working time, distributed the content through company computers, and the company permits (or does not expressly forbid) such activity, these facts could support an argument that the employee was acting on behalf of the company in issuing the unlawful endorsement. You might also appear to be the endorser if the employee displays the company logo on his or her personal web page. To minimize the risk, a policy on employee endorsements should prohibit employees from using company trademarks on their personal web pages and from using company computer systems to create or contribute content to a personal web page.

The tough question on allowing access to social networking sites will often be decided by your company’s corporate culture. Whichever side of the issue you end up on,

it is important to enforce the policy and punish violators. Finally, designate a contact email address for employees to direct their social media questions, which will be fielded by human resources, legal and public relations.

Although employee endorsements on social media pages can be a valuable marketing tool, having an effective policy in place and exerting an appropriate level of control over such endorsements can mean the difference between a successful marketing campaign and a costly lawsuit.

Protecting intellectual property on social media

With the explosion of social media comes the increased burden of protecting your company’s trademarks, copyrights and related intellectual property. No company can stop all third party uses of company IP — some third party uses are legally protected, even if the use might be viewed as harmful to your company. Conversely, not all unauthorized uses that may be legally stopped should be pursued.

Any legal action against third party use needs to be balanced against the potential impact on your company’s public image. The company’s actions and any communications may well be publicized without your knowledge or consent — your dealings are not subject to any confidentiality. Accordingly, you must evaluate with your public relations department not only the strength of a legal argument against unauthorized third party use of your IP, but also potential public relations costs in taking action.

Your company’s valuable IP rights must be balanced against the costs and expenses involved in taking action against unauthorized third party use. Essentially, you should take action only in situations where:

- you have a sound legal basis for objecting to the third party use;
- the third party use has the genuine potential for doing harm to your company’s reputation, brand, or IP; and
- the costs and expenses of taking action are justifiable based on the potential harm.

Types of unauthorized uses

In analyzing a particular unauthorized use and deciding whether to take action, it is often helpful to categorize the use to formulate a consistent plan of action.

- *Gripe site/page.* Sometimes a dissatisfied customer, consumer advocate or politically motivated person will start a page devoted to bashing the company. In light of the First Amendment, there is often little that a company can do to stop legitimate complaints. Also, lawsuits to stop gripe sites often attract media attention, and civil liberties groups may rush to defend the free speech rights of the “griper,” thus resulting in more undesired publicity.

- *Fan site/page.* Fan sites are often complimentary, but some fan sites may be a commercial entrepreneur that uses company IP to conduct business. A key issue in evaluating any fan site is the potential for false association or sponsorship with your company. You might consider an outreach program with true fan sites, which sets preferred guidelines for their use of your company's IP and which may earn incentives if followed (e.g., product samples or advance product announcements), or warns of potential action if the guidelines are disregarded.
- *"Related use" sites.* Third party companies may be selling products or services related to your company's products or services. You should evaluate each of these businesses and determine whether they present opportunities or liabilities. Among the options to consider: (a) require a clear disclaimer on the site; (b) object to the use of company IP, logo or slogan;

Evaluating whether to take action against unauthorized uses of company intellectual property is a difficult task, but should be coordinated to maintain a uniform and coherent policy response.

(c) roll out a competing offer; or (d) license or certify the third party use.

- *Affirmative statement of affiliation.* If any site advertises that it is an "authorized affiliate" or makes some other affirmative statement of connection with your company, when such a statement is not correct, it is likely problematic.
- *Use of company trademark.* There can be a big difference between a third party's simple, text reference to your company and the use of a company trademark to refer to your company. The use of your trademark can often convey a false sense of affiliation, or may dilute the strength of the trademark used. However, a factual text reference to your company in connection with a political issue will likely not suffer the same problems.

The above list is not intended to be a fully exhaustive recitation of every type of third party use, but rather to assist with evaluating whether or not to take action.


Possible courses of action

Generally, the range of legal actions to consider include:

- File a lawsuit to stop use. This is the most aggressive and costly action, and should only be taken in rare instances.
- Cease and desist letter. Demand the use stop, threatening further action if it does not. Never threaten action you do not intend to follow through with. Follow up to ensure compliance. Note that in this online age, cease and desist letters are often publicized and posted online next to the offending content.
- License the use. If possible, it may be useful to approach the third party to specifically enter into a license agreement to manage the third party's use.
- Do nothing, but maintain vigilance. In certain instances, taking action draws more attention to the unauthorized use. It is often advisable to simply ignore some unauthorized third party uses to avoid attention to your monitoring activities.

Evaluating whether to take action against unauthorized uses of company intellectual property is a difficult task, but should be coordinated to maintain a uniform and coherent policy response. A haphazard, reactive approach is typically both ineffective and expensive. Generally, companies that adopt and abide by a clear, yet flexible, enforcement program not only address the challenges more successfully, but do so more cost effectively.

Reaping benefits with the right policies

In a marketplace that no longer relegates social media participation as an option, and with serious challenges posed in engaging in social media, the lawyer's position is a difficult one. But with the right policies and practices in place, you can reap the tremendous insight and interaction opportunities of engaging in social media, while minimizing your potential exposure. 

Have a comment on this article? Email editorinchief@acc.com.

NOTES

- 1 47 U.S.C. § 230.
- 2 17 U.S.C. § 512.
- 3 47 U.S.C. § 230(e).
- 4 *Fair Housing Council of San Fernando Valley v. Roommates Com, LLC*, 521 F.3d 1157 (9th Cir. 2008).
- 5 15 U.S.C. § 45(a)(1) (2006).
- 6 Source: The Buck Consultants/IABC "2009 Employee Engagement Survey" available at www.iabc.com/rf/pdf/employeeengagement.pdf.

Reprinted with permission of the authors and the Association of Corporate Counsel as it originally appeared: "Social Media Game Plan: IP and Marketing Law Playbook," *ACC Docket* 28, no. 7 (September 2010): 104-112. © 2010 the Association of Corporate Counsel. All rights reserved. If you are interested in joining ACC, please go to www.acc.com, call 202.293.4103, ext. 360, or email membership@acc.com.