Social Media Risks and Rewards

A guide to the steps companies can take to minimize the risks associated with the revolution in the use of social media.

The Social Media Task Force, Reed Smith LLP

Social media usage has revolutionized the way in which companies communicate with consumers. This article provides practical guidance on the potential risks to a company attributable to the use of social media tools by the company and its employees. It explains:

- How companies use social media.
- The main potential risks associated with social media usage.
- The use of social media in employment practices.
- Issues associated with employee use.
- How to create and implement a social media policy.

HOW COMPANIES USE SOCIAL MEDIA

Companies are taking advantage of social media in a variety of ways to promote brand awareness and to interact and communicate with customers. Common practices include:

- Use of branded pages. Branded social media pages created and hosted using a third-party service, such as Facebook or Flickr, allow companies to quickly and easily establish a social media presence. The official Starbucks fan page on Facebook has nearly 5.4 million fans and counting. The Starbucks YouTube channel has nearly 4,800 subscribers and 81 videos. On Flickr, the Starbucks group has 4,880 members and nearly 15,900 photos. And more than 700,000 people are following Starbucks on Twitter. Starbucks' own social network, Starbucks V2V, has more than 22,500 members.
- Promotions and contests. Many companies are using their social media presence as a platform for promotions, by offering sweepstakes and contests within or founded on social media and user networks.
- User-generated content (UGC). Companies frequently and increasingly create promotions centered around UGC, for example by urging consumers to submit content-rich descriptions of why they love a certain product or service.
- Word-of-mouth marketing via blogs. Word-of-mouth marketing typically refers to endorsement messaging. Specifically, an endorsement is "an advertising message" that consumers are likely to believe is a reflection of the opinions and beliefs of the endorser rather than the "sponsoring" advertiser. Examples include providing products to third-party bloggers to create (hopefully favorable) product reviews, offering giveaways on third-party blogs or creating a company-sponsored blog (see below *Customer Service and Feedback*). Many companies are using amplified word-of-mouth marketing by actively engaging in activities designed to accelerate the conversations consumers are having with brands, including the creation of Facebook applications based on a company or its product. In July 2009, for example, Starbucks created a Facebook application where users could share a virtual pint of ice cream with friends.
- Customer service and feedback. Social media can also foster customer feedback and engagement with a brand. General Motors, for example, has at least two blogs: the Fast Lane and the Lab. According to General Motors, the Fast Lane is "a forum for

GM executives to talk about GM's current and future products and services, although non-executives sometimes appear here to discuss the development and design of important products". The Lab lets consumers "get to know the designers, check out some of their projects, and help [the designers] get to know [the consumers]. Like a consumer feedback event without the one-way glass". Companies are also using social media, such as Twitter, to provide nearly instantaneous customer service and receive customer feedback.

- Responding to rumors and negative publicity. Companies can use social media to quickly respond to rumors or other negative publicity. For example, after two employees of Domino's Pizza posted a video on YouTube in which they adulterated the chain's food, the CEO of Domino's Pizza responded by posting his own video, apologizing for what consumers saw and assuring them that such things were not condoned nor practiced at the company. Both traditional media and the blogosphere applauded his open communication and willingness to engage in a conversation about the problem.
- Disclosure of information to the public. Social media can provide companies with the ability to more effectively reach more actual or potential customers, investors and/or shareholders. Notably, the SEC has been moving toward recognizing more channels of distribution for required and other public information disclosures (either to meet regulatory obligations or in connection with individual securities transactions), including a variety of electronic media.
- Employment practices. Human resources departments are increasingly using social media as a research tool to gather information for important staffing decisions, such as hiring new talent and terminating employment.

For a description of popular social media sites and the features that distinguish them from one another, search Social Media: A Quick Guide on our website.

PRACTICE NOTES | DOCUMENTS | CLAUSES | CHECKLISTS | ARTICLES

The following related Practice Notes are available on practicallaw.com

>> Simply search the title OR resource number

Background Checks and References or 6-500-3948

How the Internet Works or 9-107-4439

Online Advertising and Marketing or 4-500-4232

Sales Promotions, Contests and Sweepstakes or 1-500-4243

Website Viruses, Spyware and Attacks or 2-500-6656

IDENTIFYING POTENTIAL RISKS

Although there are many potential benefits of undertaking these and similar activities, before entering the social media arena companies should identify and prepare for the associated risks. Companies should be particularly alert to:

- The terms of use that govern the relationships between the company, the third-party site owners and the end users of branded pages and channels.
- The framework for endorsements and testimonials.
- Securities-related risks.

BRANDED PAGES AND CHANNELS

If a company creates customized pages or media channels on third-party social media sites (for example, the company's fan page on Facebook or channels or communities on YouTube), the company should:

- Review the terms of use and privacy policies the third-party providers have put in place to govern the use of those sites.
- Have effective procedures in place to monitor usage and content, and to respond to negative posts.

Third-party Terms

Company activities must comply with the terms of use of any third-party social media platform. Terms of use can vary significantly from site to site and may include important restrictions. Particular attention should be paid to terms relating to:

- The actions of the users who access, use and interact with the service. Many social networking sites (including Facebook, YouTube and Twitter) prohibit the uploading or posting of content by any user that infringes a third party's rights, including intellectual property, privacy and publicity rights. The company should assess whether such conditions will realistically act as a deterrent and a meaningful enforcement mechanism, and what its liability might be in circumstances where infringing content is posted on its page (see below *Monitoring Usage*).
- "Take down" notices received under the "safe harbor" provisions of the Digital Millennium Copyright Act (DMCA). In practice, the third-party site owner usually bears the responsibility for responding to these notices. The DMCA provides online "service providers" with a safe harbor under certain circumstances for copyright infringement resulting from acts by their users (for example, an infringing video posted by a user on YouTube).
- Age limits for users. The terms of service applicable to Facebook and YouTube specifically prohibit use by children under the age of 13, while Twitter allows access only by individuals who can enter into a binding contract with Twitter. Again, the third-party site owner usually bears the responsibility for establishing age limits for users.
- Prohibitions or restrictions on the use of the social media, including

restrictions on use for advertising or marketing, or for promotions and contests. YouTube's terms of service are generally silent on the issue of sweepstakes and promotions. Facebook's terms of service, however:

- prohibit the offering of contests, giveaways or sweepstakes on Facebook without its prior written consent; and
- require that the sponsor take full responsibility for the promotion and follow Facebook's Promotion Guidelines, as well as applicable laws.

- Ownership of intellectual property used on, or information collected or generated through use of, the site (for example, any of the company's copyrighted material and trademarks that might be posted on the site, or customer information the company collects through the site, or UGC posted to the company's page).
- Recourse available to the company if its rights are violated (such as infringement of its copyrights) by other users.
- Privacy policies. These can vary significantly among sites. Companies should:
  - ensure that the site owner's privacy practices for any data disclosed by the company or collected by the company from users of the site are appropriate and sufficient for the company's intended use of the site; and
  - monitor such privacy policies regularly for updates and changes.

Monitoring Usage

Despite the efforts by social media platforms to impose terms of use prohibiting individuals from posting content that infringes a third-party's rights, a company may nonetheless find that content is posted that:

- Infringes its (or another third party's) intellectual property rights.
- Is defamatory or otherwise damaging to the company's (or another third party's) reputation.
- Contains confidential or proprietary information.

For a discussion of the rights and remedies available to companies when a potential legal claim arises, see the relevant chapters in *Network Interference* on *reedsmith.com* (see *Box, Network Interference*).

It is important to have in place procedures that will bring offensive or infringing postings to the attention of the company. Companies can take the following steps to protect against unwanted posts and mitigate the damage of such posts on their branded pages:

- Institute a monitoring program. The company should monitor social media sites, services and applications (and websites generally) for potentially damaging comments about the company or its products or services and infringement of the company's intellectual property. The company should consider whether to engage a third-party monitoring vendor or use company employees to undertake this activity.
- Put together an internal response team to handle damaging statements or content. Responding appropriately to damaging statements or content posted by third parties may require coordination by multiple individuals across many company areas, and the company should consider creating a response team that includes, for example, members of:
  - senior management;
  - legal;
  - corporate communication/public relations;
  - marketing; and
  - human resources (in case employees are responsible for the damaging activities).
- Do not ignore defamatory comments or misleading information. Companies should not ignore misleading statements being made about the company or its products.

The appropriate response, however, will depend on the type and severity of the conduct at issue and could include, as appropriate, one or more of the following:

- if the offending post appears on a third-party website, requesting that the post be taken down;
- if the offending post appears on the company's own website, including a disclaimer reserving the right to remove content at the employer's discretion and ban abusive users;
- deleting false or misleading postings if possible or replying to the post with correct information;
- responding via other social media outlets, such as a company blog or fan page;
- responding with a press release; and
- taking legal action (for example, sending a cease and desist letter or filing a lawsuit). However, drawbacks to litigation include the potential need to identify an anonymous author, bad publicity and the high cost of litigation.

Companies should enforce their response policy consistently.

For further dos and don'ts, see *Company Use of Social Media: Best Practices Checklist* in this toolkit.

ENDORSEMENTS AND TESTIMONIALS

Companies that use bloggers to advertise their products need to be aware that if bloggers fail to disclose a material connection (such as the provision of free products or other perks to the blogger) between blogger and company, both the blogger and company may face regulatory scrutiny and backlash from consumers who might feel as if they have been duped or that a blog is a glorified advertisement.

The Federal Trade Commission (FTC) recently revised its Guides Concerning the Use of Endorsements and Testimonials in Advertising (FTC Guides). The FTC Guides provide a general principle of liability for

communications made through endorsements and testimonials:

> "Advertisers are subject to liability for false or unsubstantiated statements made through endorsements, or for failing to disclose material connections between themselves and their endorsers. Endorsers also may be liable for statements made in the course of their endorsements."

The FTC has indicated that:

- Endorsers in social media, along with the sponsoring advertisers, are subject to liability for failing to make material disclosures relating to the endorsement relationship (for example, gifts, employment and/or other connections and circumstances).
- The endorsement relationship itself may trigger the obligation to disclose.
- Advertisers need to take reasonable steps to ensure that material disclosures are made.
- Advertisers cannot rely on the "remoteness" of the social media endorsers or on the advertiser's lack of control over them to escape liability.
- Advertisers are technically liable for a remote endorser's failure to disclose. An advertiser's ability

ROLE OF SOCIAL MEDIA USE IN LITIGATION

Lawyers have used social networking sites to gain information about all aspects of a case, including the parties on the other side, how a particular business is conducted, the witnesses and the jurors. Social media sites can contain valuable information such as messages, status updates, photos and times of every posting, all of which can be used to undermine an opponent's case in litigation, and can even negatively affect a company's business and public image.

The following are a few examples of how social media can be used in litigation:

- Impeaching Witnesses. Social media sites may contain contradictory statements, character evidence or other evidence that can be used to impeach witnesses during litigation. Users of social media often fail to consider the consequences of their posted statements and photos prior to such postings. In the corporate world, postings could be made by employees regarding a wide range of work-related issues, including comments concerning layoffs that implicate the Age Discrimination and Employment Act, disclosures of intellectual property and trade secrets in various career-oriented chat rooms or blogs and gossip about a sexual harassment or white collar crime internal investigation.
- Work Product Doctrine and Attorney-Client Privilege. The use of company websites and other social media also provides real opportunity for waiver of the work product doctrine protection and attorney-client privilege through public disclosure of confidential information. It is often sound business strategy for a company to post statements on its website to keep the public informed on various issues, ensure public confidence in the company's product and services, bolster public relations and increase profitability. However, if a company discloses too much, there are instances where it will risk waiving work product and attorney-client communication protections. Managers, supervisors or employees who disclose work-related issues in chat rooms and blogs run the risk of waiving both privileges as well, forcing a company to produce documents they ordinarily would have every right to withhold in litigation.
- Social Media Use by Jurors. In several recent instances, jurors have made inappropriate disclosures concerning corporate and individual litigants during the pendency of a trial. The use of social media by jurors during a trial may impact a company's public image, business and stock price if a juror leaks information about his or her perception of the case prior to the final verdict being rendered by all jurors. The use of social media by a juror may be grounds for a mistrial or an appeal because the social media postings of the juror may indicate that the juror was biased and was making a decision prior to reviewing and considering all evidence.

In light of these concerns:

- A company's managers, supervisors and employees must be educated on the implications and discoverability of site postings so that their use of social media does not undermine legal positions in a future or pending lawsuit against the company.
- All managers, supervisors and employees must be educated about the implications of discussing work-related issues online and to realize that certain postings may come back to haunt the employees and the company for which they work.
- In a jury trial, it is essential that explicit instructions are given to the jury prior to the commencement of trial prohibiting the use of social media.
- Companies and their legal teams should research the social media sites during the trial to ensure that no juror is leaking the jurors' thought process about the case to the public and/or being tainted by other individuals' responses to any postings on the social media sites.

to avoid discretionary regulatory enforcement due to the endorser's failure to disclose will be a function of the quality of the advertiser's policies, practices and policing efforts.

In light of the FTC Guides:

- Companies that provide products to a blogger for purposes of a product review should never instruct the blogger regarding what to say in the review, or ask to review or edit the review prior to posting.
- Companies must disclose material connections with third-party bloggers.
- While companies should provide bloggers with up-to-date, company-approved product information sheets, those information sheets should not reflect the companies' opinions or include prices.
- In the event of a negative review, companies have the option of not providing products to the blogger for future reviews.
- Companies should caution their personnel about engaging in inflammatory disputes with bloggers ("flaming") on any blogs.
- Companies should monitor product reviews made by bloggers to ensure that the claims made are truthful and can be substantiated.

SECURITIES-RELATED RISKS

While social media tools present an attractive channel for public companies to communicate with their investors, market professionals and the public at large, care must be taken to ensure that disclosures are appropriate and conform to a variety of applicable legal standards, and that those standards are understood and adhered to by a company's employees and agents. Some key securities regulations that may be applicable include:

- Regulation FD. Regulation FD governs the public disclosure of material information and requires that such information be disseminated by methods of disclosure "reasonably designed to provide broad, non-exclusionary distribution of information to the public".
- Rule 10b-5. Rule 10b-5 of the Exchange Act prohibits companies from making materially misleading statements or omissions.
- Forward-looking Statements. The Private Securities Litigation Reform Act (PSLRA) contains a safe harbor for certain forward-looking statements made by companies under limited circumstances. In order to benefit from this safe harbor, written statements must be identified as forward-looking statements and be accompanied by meaningful cautionary statements identifying important factors that could cause actual results to differ materially from those in the forward-looking statements.

Before a company decides to adopt social media as a form of communication and disclosure, it must ensure that the proper controls are in place. Practical considerations include the following:

- Companies must be careful not to violate Regulation FD through selective disclosures on social media aimed at market professionals and not the public at large.
- Companies should create programs to educate their employees on the importance of Regulation FD's prohibitions on selective disclosure and keeping the company's most important confidential information internal to the company. Employees need to know what information they can and cannot communicate electronically in order to stay within the limits of compliance. Such programs, together with meaningful and well-circulated corporate policies, will help to prevent violations in the first instance. If a problem should arise, the fact that a company has undertaken these steps may tip the balance in its favor when the SEC decides whether or not to bring an enforcement action.
- Companies should verify that all mandatory disclaimers regarding forward-looking statements and financial measures are included with any electronic disclosure.
- Companies should regularly monitor their websites and social media presence to ensure that the discussion is appropriate, the dispersal of information is compliant with the securities laws and, more simply, that these vehicles are being properly and lawfully used. In addition, it is important to conduct routine searches for the use of the company's name and corporate logo or other image to ensure that false rumors or other manipulations are not occurring.
- Companies that decide to use social media as a tool must carefully plan, execute and periodically revisit a strategy that ensures that its use of social media is compliant with securities laws and that it is protected against its abuse.

THE USE OF SOCIAL MEDIA IN EMPLOYMENT PRACTICES

Companies need to recognize the employment law implications tied to the use of social media during each stage of an employee's tenure with the company. Failure to use social media cautiously and intelligently may create legal exposure. For example:

- Discrimination. If employers make adverse employment decisions based on protected class information learned through social media, they have violated laws prohibiting discrimination. For example, an employer that learns about a candidate's religion or sexual orientation through social media and decides not to hire the individual based on that information has violated anti-discrimination law prohibiting such activity.
- NLRA Violations. The National Labor Relations Act (NLRA) protects the right of employees to act collectively to change their workplaces for the better. An employer that discovers through social media that employees

or applicants for new positions are undertaking these activities and makes adverse employment decisions based on this information has violated the NLRA.

- Background Checks. The Fair Credit Reporting Act (FCRA) and its state equivalents regulate employers' use of consumer reports in conducting background checks. Although an employer's in-house search of online resources is unlikely to fall within the federal FCRA, state requirements may be more stringent. For example, an employer's own search of social media that results in an adverse employment action taken without proper notice and disclosure compliance may create liability under broader state law. In addition, under the federal law, failure to provide required notice for relying on information in a consumer report — such as social media findings — may lead to liability.

Companies using social media in hiring decisions and background checks should:

- Maintain consistent protocols for social media screening of applicants regardless of their race, gender or other protected class status to avoid disparate treatment liability.
- Develop a basic understanding of the activities protected by the National Labor Relations Act (NLRA) to remain compliant and respect the rights it protects.
- Develop a basic understanding of the requirements of the Fair Credit Reporting Act (FCRA) and its state equivalents to promote the lawful use of background checks.
- Access privacy-protected electronic resources only with proper authorization to avoid liability under laws governing electronic resources (such as the Stored Communications Act) and common law privacy rules.
- Comply with the "terms of use" policies of social media websites (see above *Third-party Terms*).
- Check facts and ensure that employment decisions are made using accurate information and account for the prevalence of false or misleading information in social media.

In addition, companies using social media in termination and adverse employment action decisions should:

- Not take retaliatory adverse employment action because of protected activity expressed through social media. It is common for federal and state laws to prohibit retaliation for the exercise of rights protected by statute, and employers considering terminations, demotions or other adverse employment activity should ensure that the reason underlying the decision does not violate employee rights.
- Comply with the NLRA in the use of social media for adverse employment decisions. If employees use social media to communicate about union activities or rights protected under the NLRA (such as conditions of employment), refrain from restricting employee speech or taking adverse employment actions that could violate the statute. Even non-unionized workplaces must respect rights conferred by the NLRA.

EMPLOYEES' USE OF SOCIAL MEDIA

Employee use of social media can be devastating to a company, both legally and from a public relations perspective. Social media may serve as a setting for the type of employee banter that, if used in the workplace, would violate an employer's anti-harassment or other policies. Moreover, social media is an outlet for an employee to "gripe" about his or her employer and possibly damage the employer's reputation. Social media may be used by employees, whether intentionally or not, to divulge trade secrets, or copyright-protected or other confidential company information.

Currently, the law with respect to employment and social media is practically devoid of any useful guidance for companies. Instead, employers must rely on basic principles related to employee privacy, anti-discrimination and harassment law, intellectual property law and other applicable law, in order to discern how to best use (and control the use of) social media in the workplace.

The risks associated with employee use of social media include the following:

- Loss in Productivity. Employees' use of social media sites during working hours can result in a decrease in productivity.
- Promoting Inappropriate Conduct Among Employees. Social media sites can be, and are often used as, communication tools between employees. However, at times, the content of those employee communications may cross the line into harassing, threatening, discriminating or other unlawful conduct that can subject the employer to liability.
- Disclosure of Confidential or Proprietary Information. Employees' disclosure of confidential information could:

PRACTICE NOTES | DOCUMENTS | CLAUSES | CHECKLISTS | ARTICLES

The following related Checklists are available on practicallaw.com
>> Simply search the title OR resource number
Controlling Online Risks and Liability Checklist or 9-500-4362
Federal Employment Anti-Discrimination Laws Checklist or 5-500-4793
Legislation Governing Liability for Website Content Checklist or 3-500-4360
Sales Promotions, Contests and Sweepstakes Checklist or 2-500-9551

CHECKLIST: PURCHASING INSURANCE AGAINST SOCIAL MEDIA CLAIMS

Social media claims or potential claims may arise in almost any context, from branding and advertising issues to defamation and privacy claims, consumer class actions and securities claims. As a result, when considering purchasing or renewing insurance coverage, companies should consider the following steps:

- Inventory Current Policies That May Provide Coverage. Since claims can raise a variety of issues and take different guises—from common law fraud and misrepresentation claims to invasion of privacy and cyber extortion—looking at an inventory of existing policies with a "social media" lens can assist in seeing and seeking potential coverage that may come into play. For example:
  - a comprehensive general liability policy typically provides coverage for bodily injury and property damage, as well as for advertising and personal injury claims. But the language should be examined to determine if there are terms, conditions or exclusions that limit or expand coverage. For example, some definitions of "property damage" may exclude electronic data, while a coverage endorsement may specifically provide some coverage. "Personal Injury" typically includes publication or utterances that are in violation of an individual's right to privacy, defamatory or disparaging. Although whether and how these coverages may apply depends on the provision, facts and applicable law, insurance-policy wording should be negotiated when analyzing the potential "buckets" for coverage, should a claim be made; or
  - a defamation claim may become an employment-related claim and coverage under an employment practices liability policy should be examined to see if there are any obvious exclusions or subtle restrictions that can be addressed when negotiating the coverage. Being proactive in negotiating coverage before a claim arises affords much greater leverage if and when the claim hits.
- Consider New Products and Recognize They Are Negotiable. Cyberliability and internet-related liability policies have improved over the past few years. Policyholders who are willing to invest in reviewing and comparing choices and wording can tailor the coverage to their needs and potential exposures. For example, some technology, media, data privacy breach and professional liability policies provide coverage for first-party loss (damage suffered directly by the company), including internal hacker attacks or business interruption, or expenses to maintain or resurrect data.
- Coverage for Third-Party Loss Is Available. Coverage for third-party loss (claims asserted against the company by third parties) may include reimbursement of defense costs and indemnification for judgments and settlements. The claims may include allegations of violations of privacy rights and personal information, duties to secure confidential personal information under state and federal laws and regulations, breaches by employees or others, infringement of intellectual property rights, unfair competition, defamation and consumer protection and deceptive trade practices statutes. The coverage may include regulatory actions, lawsuits and demands.
- Key Coverage Enhancements to Seek. Policies should cover:
  - A Broad Definition of Claim. Coverage should apply to demands, investigations and requests to toll a statute of limitations, as well as to complaints, civil, criminal, administrative and regulatory proceedings. Keep in mind that a broader definition of Claim also means a corresponding obligation to report what will now be a Claim.
  - A Broad Definition of Loss. Loss should encompass a broad array of relief, including statutory fines and penalties where insurable, as well as defense and investigative costs.
  - Narrowed Exclusions. Exclusions should be narrowly tailored and contain "exceptions" where coverage will be provided. Defense costs should be covered, and the exclusions should be severable, so that one "bad apple" doesn't spoil coverage for others.
  - Defense and Settlement Flexibility. Consider whether the insurer provides a defense or the insured seeks control over the defense. Negotiate "consent to settle" provisions.
  - Seek Coverage Grants via Endorsement. Specialty or tailored endorsements may add coverage and should be requested.

- result in the employee's breach of his or her confidentiality and nondisclosure agreement;
- violate the terms of a confidentiality agreement between the company and a third party, causing the company to be in breach;
- cause the company to lose protections of its proprietary intellectual property rights;
- waive the attorney-client privilege; and
- violate securities laws.

>> For a Practice Note providing more information, search Trade Secrets and Confidential Information on our website.

- Attempts to Discipline Raise Legal Issues. Content posted anonymously is very difficult to police and several states have laws prohibiting employers from taking adverse action against an employee for engaging in lawful off-duty conduct. Employers must also be cautious about taking adverse action against any employee whose social media use could be construed as protected, concerted activity pursuant to the National Labor Relations Act (NLRA), no matter how derogatory the post may be to the company. Finally, government employers have the additional concern of possibly violating their employees' First Amendment rights by disciplining an employee for content he or she posted on a social media site.
- Liability for Employee Content. It is unclear to what extent, if any, an employer may be liable for an employee's statements in social media. However, the FTC Guides suggest that both employers and employees may be liable in certain circumstances, such as when an employee posts messages on a discussion board promoting a company's product without properly disclosing the employee's relationship to the company (see *Example 8 of 16 C.F.R. Part 255.5*). Similarly, laws against harassment, discrimination and other unlawful conduct that can subject an employer to liability apply just as forcefully to social media conduct.

In light of these risks, it is important to send a clear signal about employer expectations for employee use of social media by adopting a Social Media Policy or provision in a company employee handbook. If your company has not developed policies for use of social media by your employees, now is the time to act.

CREATING AND IMPLEMENTING A SOCIAL MEDIA POLICY

A properly drafted policy on the use of social media by employees is an employer's most effective tool in protecting itself against legal liability and harm to its reputation and good will from the use of social media. In most cases, a properly drafted policy pertaining to employee use of social media should assist an employer in protecting its interests.

NETWORK INTERFERENCE

The Social Media Task Force, Reed Smith LLP

This article is based on *Network Interference, A Legal Guide to the Commercial Risks and Rewards of the Social Media Phenomenon*, written by the Reed Smith Social Media Task Force. It includes chapters on the following topics:

Advertising and Marketing
Gregory J. Hessinger, Stacy K. Marcus, Anthony S. Traymore

Commercial Litigation
John L. Hines, Jr., Janice D. Kubow

Data Privacy and Security
Mark S. Melodia, Paul Bond, Amy S. Mushahwar

Employment Practices
Casey S. Ryan, Amber M. Spataro

Government Contracts and Investigations
Andrew L. Hurst, Daniel Z. Herbst

Insurance Recovery
Carolyn H. Rosenberg

Litigation, Evidence and Privilege
Alexander "Sandy" Y. Thomas, Maureen C. Cain

Product Liability
Anthony B. Klapper, Jesse J. Ash

Securities
Christopher P. Bennett, Amy J. Greer, Jacob Thride

Trademarks
Darren B. Cohen, Meredith D. Pikser

Editors
Douglas J. Wood, Stacy K. Marcus, Joseph I. Rosenbaum

Search *Network Interference* on *reedsmith.com*


Douglas J. Wood


Stacy K. Marcus


Joseph I. Rosenbaum

However, policies are not one-size-fits-all. They must be tailored to the culture, needs and realities of your specific workplace.

Some elements to consider in creating and implementing a social media use policy include:

- The company's level of tolerance for personal use of social media.
- Whether the company should permit or even require use of social media for marketing and business development.
- How the company will handle employees who post arguably inappropriate, but not unlawful, posts such as illicit photos, profanity or other potentially derogatory content.
- How the company will comply with laws protecting employees' right to engage in lawful off-duty conduct, but still ensure nothing damaging is posted online.
- The company's strategy to preserve good business relationships and promote a positive corporate image.
- Once the policy is in place, how the company will train employees so they understand what is forbidden (for example, one person's definition of "crude" may vary from another's).
- How the company will monitor compliance with and enforce the policy.
- What the repercussions will be for violations.

Use the policy to remind employees that public or workplace social media activity is not private and that the employer has the right to correct unproductive or harmful employee social media use as necessary. Include (in conjunction with related internet and e-mail use policies) appropriate restrictions covering:

- Employee use of company technology.
- Employee use/misuse of company intellectual property assets, including confidential, proprietary and privileged information.
- Employee use/misuse of third-party intellectual property assets.
- Protection of third-party privacy in the context of employees' personal use.
- Harassment of other employees.
- Discrimination.
- Defamation and disparagement.

For a model social media policy, see the *Social Media Policy* in this toolkit.

It is important to train Human Resources management on appropriate and effective employee monitoring and enforcement of the above policies, restrictions, guidelines and contract provisions, subject to compliance with employees' privacy rights. However, don't impose unnecessary, impractical or intrusive restrictions on employee use of social media. Such disproportionate restrictions might undermine employee morale and invite noncompliance, without real benefit to the company in terms of protecting its property, reputation or employees.

>> For more on employee issues, search Checklist, Employees and Social Media: Company Best Practices on our website.