



**CAUTION**



**STUMBLE  
HAZARD**

# Managing the Emerging Business and Legal Realities of Social Media in Corporate America

BY VINCENT M. CATANZARO AND JONATHAN M. REDGRAVE

As you read this article, whether it be in your office, on the subway or walking down the street, stop to look around you. Chances are you will see at least one person engaged in some form of social media, be it Facebook or Twitter, updating an online blog or participating in your company's new internal social media application. This conduit for exchanging facts, opinions and suggestions, ranging from the mundane to the insightful, is clearly here to stay. For example, this past spring, Morgan Stanley announced that they would begin allowing their financial advisors to use social media to interact with their clients.<sup>1</sup> *The Wall Street Journal*, in its April 25, 2011, edition, provided many more examples of how companies are now reaching out through social media tools.<sup>2</sup>

As the availability, functionality and popularity of using social media continues to increase, the lines between our professional and personal lives begin to blur much faster. Today, people are taking their work home and bringing their home life to work, often with encouragement from their employers, leaving legal and IT teams with an entirely new set of data security, information management and compliance challenges.

These challenges present both business and legal risks. On the business side, the *Harvard Business Review* recently conducted a survey that showed that the “stumble rate” — instances of reputation loss due to disdain or ignorance of new media — was an astonishing 50 percent for the world’s most admired companies.<sup>3</sup> Alone, this shows the need for thoughtful management of a company’s social media involvement. On the legal side, social media creates numerous opportunities for potential legal liabilities (see sidebar on p. 65), as well as rich repositories of potential evidence for criminal and civil matters. Indeed, an article in a recent issue of the *United States Attorneys’ Bulletin* highlighted the importance of social media for all government attorneys: “[I]t is good practice for attorneys, whether in civil or criminal cases, to recognize that social networking sites may contain information that could be used as evidence or otherwise have significance in a court proceeding.”<sup>4</sup> Because there is little precedent in the area of social media, courts are still in the process of evaluating and re-evaluating what laws should or should not govern this new world of communication, making it difficult to predict all of the issues that may arise and how they will be resolved.<sup>5</sup>

With these challenges, however, come great opportunities that can, with planning and forethought, help your company effectively navigate this new world. Thinking forward, a number of companies today have already published social media policies, but a policy alone is not enough. A policy is merely a single piece of the larger puzzle whose solution delivers the keys to future success.

Companies should consider these eight steps when addressing the emerging business and legal issues attendant to social media in the workplace:

1. Have a business vision for your company’s involvement in social media;
2. Secure your company’s confidential records, files and information from threats — both internal and external;
3. Designate leaders who will be responsible for and have authority over your company’s involvement in social media platforms;
4. Develop and implement a social media policy (if you have not already done so);
5. Train your employees about the risks and rewards of social media, particularly those who will be officially responsible for your company’s involvement;



VINCENT M. CATANZARO is senior counsel and global discovery manager for E. I. du Pont de Nemours & Company in Wilmington, DE. He is also a member of The Sedona Conference’s® working group on Best Practices for Electronic Document Retention and Production, and the Richard Herrmann Technology Inn of Court. He can be contacted at [vincent.m.catanzaro@usa.dupont.com](mailto:vincent.m.catanzaro@usa.dupont.com).



JONATHAN M. REDGRAVE is a partner with Redgrave LLP in Washington, DC. He has extensive experience in all areas of complex litigation in both state and federal courts, and focuses his practice in the areas of information law, which includes electronic discovery, records and information management, and data protection and privacy issues. He can be contacted at [jredgrave@redgravellp.com](mailto:jredgrave@redgravellp.com).

*\* The views expressed in this article are solely those of the authors and may not be attributed to any other persons or corporate entities. The authors wish to acknowledge and thank the substantial contributions of Benjamin Redgrave, a summer clerk at Redgrave LLP, for the preparation of this article.*

6. Start thinking about the future today, especially regarding records and information retention, and legal discovery;
7. Diligently monitor for compliance and be prepared to enforce your rules; and
8. Adapt to the shifting business and legal landscape, and never become too set in your practices and policies that you are unable to change.

Each of these steps is addressed in this article in greater detail.

**Business vision.** Fundamentally, success requires that your company develop a business plan for your involvement in and use of social media. Chances are your company would never build stores or warehouses, create a new product, or implement a new marketing strategy without first considering long-term goals. Why should your approach to social media be

different? Your company’s overall objectives should drive your social media policy and how you address any problems that may arise out of your social media activities. If you are unsure of the direction your company wants to travel in the vast ocean of social media, or you don’t know what overall plan would benefit your company the most, start by asking yourself a few simple questions:

- What does my company want to accomplish by utilizing the tools social media has to offer?
- Do we want to actively promote our company’s services or products through such sites?
- Would we rather just use social media as an outlet for debunking false or slanderous ideas circulating about the company? Or are we participating in social media simply to build brand awareness?
- How much freedom do we want employees to have? Should they be allowed to post freely about the company to generate more business, or should we restrict them to private comments that do not deal with any of the company’s goals and functions?
- If we are using internal or federated social media platforms, what are our goals and how do we measure success?
- Are we trying to build collaborative workspaces for employees and partners?

Once you answer these types of questions, you can begin to formulate your over-arching plan and address other issues.

## Five Significant Risks to Your Company Posed by Social Media

Among the many potential legal liabilities, we highlight five:

**1. Defamation:** The defamation of your company, or your company's competitors, by your employee(s) can lead to a host of problems. It is all too easy to denounce a company's products or services, often by manipulating facts, when users can create anonymous profiles that mask their true identities. Derogatory comments usually garner attention (mostly negative) in the online community and can often lead to litigation. The risk of defamation to individuals, and resulting legal action against the employer, simply cannot be ignored.

**2. Hijacking of intellectual property:** The use of your company's logo or trademarks by independent third parties for marketing purposes, although potentially harmless, or even seemingly helpful in some situations, poses a substantial threat to brand management and intellectual property rights. The misappropriation or misuse of trademarks, trade names and images, and copyrighted materials can substantially impact direct consumer interactions, as well as impair brand reputation and value depending on the nature of use.

**3. Unauthorized releases of information:** The release of clients' privileged and confidential information and/or

company secrets is one of the worst pitfalls that a company can fall prey to, as incidents related to WikiLeaks has shown repeatedly. Your reputation is often instantaneously tarnished, and depending on the subject of the matter released, substantial efforts may need to be undertaken to contextualize and address the disclosed information and the litigation that oftentimes follows.

**4. Harassment or discrimination:** Few things can create internal discord and cause disruption to a company like an employee or employees who harass or discriminate against other employees (or anyone for that matter). The posting of inappropriate comments that denigrate, show hostility or discriminate against another employee, whether it is on account of race, sex, age, nationality, etc., is a substantial risk in environments where anyone can literally post anything.

**5. Potential liability for deceptive or unfair practices:** In recent years, the Federal Trade Commission has become more aggressive in pursuing deceptive or unfair corporate practice claims, making social media a potential trap for companies. In addition, there is the risk that activity in social media may warrant scrutiny under various state consumer protection laws.

**Security.** Almost as important as your company's business vision are its security protocols. Without a doubt, easy access to social media vehicles that can instantly transmit information around the globe presents a critical threat when it comes to the vulnerability of confidential information. Whether it is a secret formula used in the creation of your products or documents explaining the internal workings of your company, the publication and dissemination of such information could impair your organization. The most obvious example of the peril of widespread and unauthorized/unwanted distribution is seen in the recent phenomena known as WikiLeaks.<sup>6</sup>

As a result, it is imperative that your company address the security issues that impact its most valuable assets, employees and information. Ensure that your information architecture is well-secured and monitored to prevent inadvertent or deliberate loss of confidential information through unauthorized access to company information via social media portals. The range of tools includes physical and logical controls on access to data stores, the training of employees regarding proper use of

information, and monitoring to detect both internal and external threats. This is especially true with the advent of federated systems that allow for trusted collaborative environments (including social interaction spaces) between companies that may seem safer, but in light of potentially deeper access to information, may be a greater risk.

**Authority and responsibilities.** Just as a ship without a captain has trouble navigating the ocean, so, too, will your company have trouble navigating the sea of social media without defined leadership. Once you have decided on a business strategy, it is important to designate an employee or group of employees, depending on the size of your company, who will be responsible for managing social media activity at your company. This person(s) should have the power to implement your business vision, oversee the dissemination and enforcement of your social media policy, direct the training of employees, and keep the company level on the waves of the web. It is crucial that this person(s) be competent and knowledgeable, and able to embrace the high degree

## Top Five Concepts to Address When Creating a Social Media Policy for Your Organization

**1. Transparency:** If and when your employees post comments to social media sites about the company, it is important to use real names and fully disclose their relationship to the business. Not only is it more likely to give your company a better reputation, it can protect against accusations of unfair or deceptive practices under the Federal Trade Commission Act, or other consumer-protection oriented statutes.

**2. Responsibility:** It is imperative to make sure your employees know that what they post online can have far-reaching consequences. Employees need to understand that once you post something to the internet, it is essentially permanent and public, even if you later seek to modify or delete it. This aspect of your policy can also include instructions on using appropriate disclaimers to reflect how an employee's post or account reflects views that are his own, and as such, do not reflect the official position of the company.

**3. Doubt means don't:** One of the easiest ways to prevent social media mishaps is to limit poorly thought-out comments. In your policy, consider including provisions that suggest employees take a moment to think about whether they should post, before posting. Make sure your employees know that, unless they are authorized as an official company representative in the space, they should not post comments

that may be perceived as the authoritative view(s) of your company. In many ways, this advice is similar to all business writing advice and should mirror what your company has said on this subject in the past.

**4. Leave official comments to the officials:** If your employees encounter a comment or situation in social media that they think should be addressed, such as the unlawful use of trademarks or inflammatory remarks against your company, create a process where they can notify an official company representative of the issue, rather than try to resolve the conflict on their own.

**5. Be respectful and use common sense:** All online conversations involve real people. Your policy should encourage employees to remember this fact and treat all participants as people and not anonymous entries. Remind your employees that their actions reflect back on your company, and that if they have a negative reputation, the company will also gain a negative reputation. This aspect of the policy should include reminders about diligently protecting privileged or confidential information from disclosure through postings and discussions, as this is one of the easiest ways to run into legal trouble.

of responsibility such a position demands. Even if the day-to-day involvement in social media is so great that it is necessarily delegated to departments or groups to manage interactions, some level of overall authority and resources is needed to guide such distributed authority. For employees to be able to utilize social media in positive ways, there must be a framework or infrastructure in place to which they can turn when they inevitably have questions.

**Policy.** A major step in the holistic approach to social media is the creation and dissemination of a social media policy. In many instances, your company may already have a social media policy in place. But is it the correct policy? As technology has continued to advance at a breakneck pace, circumstances may have changed since your policy was first implemented. Does your policy still adequately fulfill the goals of your business vision? If your company does not already have some sort of policy, it is doubly important that it creates one in the near future. Without a solid social media policy to fall back

on, your employees will essentially be left to their own devices. Even if all your employees are socially savvy and do not make any blunders, such as posting derogatory comments on Facebook, your company will likely still encounter problems. Without a unifying policy that employees can view and refer to easily, two employees, both with good intentions, might post different comments about the same aspect of your company, causing your company to look poorly managed and impairing corporate efforts to build a consistent brand image.<sup>7</sup>

**Training.** Once you have successfully developed or tweaked your social media policy, you must begin educating your employees about it. Although it is tempting to save time and money by simply sending out your policy to employees via email and/or posting it to your company's intranet, the reality of the corporate workplace today means that some employees may simply brush the policy aside or spend little more than a cursory glance examining it. To integrate your policy within your culture, it is important to consider how to best teach employees about

## ACC Extras on... Social Media in Corporate America



### ACC Docket

- *Are You Building a House of Cards: Social Networking in the Office* (Sept. 2010). [www.acc.com/docket/house-of-cards\\_sep10](http://www.acc.com/docket/house-of-cards_sep10)

### InfoPAK<sup>SM</sup>

- *Workplace Information Risk in the Digital Age: Monitoring Employees, Social Media Challenges, Managing Access to Data and Optimizing Flexibility* (Jan. 2011). [www.acc.com/infopaks/info-risk\\_jan11](http://www.acc.com/infopaks/info-risk_jan11)

### QuickCounsels

- *Blogs and Social Media Marketing: Complying with the FTC's New Endorsement Guides* (March 2011). [www.acc.com/blogs\\_ftc\\_mar11](http://www.acc.com/blogs_ftc_mar11) 
- *Workplace Challenges Associated with Employees' Social Media Use* (March 2011). [www.acc.com/challenges-social-media\\_mar11](http://www.acc.com/challenges-social-media_mar11) 

### Quick References

- *Considerations in Drafting Effective Social Media Policies* (Dec. 2010). [www.acc.com/draft-smp\\_dec10](http://www.acc.com/draft-smp_dec10)
- *All a-Twitter: Drafting Social Media Policies* (July 2009). [www.acc.com/a-twitter-smp\\_jul09](http://www.acc.com/a-twitter-smp_jul09)

### Top Tens

- *Exploring the Risks & Rewards of Social Media: Ten Tips for Success* (Aug. 2011). [www.acc.com/topten/risks&rewards-sm\\_aug11](http://www.acc.com/topten/risks&rewards-sm_aug11)
- *Top Ten Implications of 2011 NLRB Activity on Monitoring Employees' Online Communications* (Aug. 2011). [www.acc.com/topten/nlr-online-comm\\_aug11](http://www.acc.com/topten/nlr-online-comm_aug11)

### Forms & Policies

- *Social Networking and Blogging Policy* (Aug. 2011). [www.acc.com/forms/social&blog\\_aug11](http://www.acc.com/forms/social&blog_aug11)
- *COLEMAN Social Media Policy* (Aug. 2011). [www.acc.com/forms/coleman-smp\\_aug11](http://www.acc.com/forms/coleman-smp_aug11)
- *Sample Blogging and Social Networking Policy* (Nov. 2010). [www.acc.com/forms/blog-networking\\_nov10](http://www.acc.com/forms/blog-networking_nov10)
- *Social Media Guidelines for Marketing Communications and Community Relations* (Oct. 2010). [www.acc.com/forms/smg-mrkt-comm\\_oct10](http://www.acc.com/forms/smg-mrkt-comm_oct10)

ACC has more material on this subject on our website. Visit [www.acc.com](http://www.acc.com), where you can browse our resources by practice area or search by keyword.



The new GLD button lets you click to copy, print or email a checklist from certain ACC online resources.

the risks of social media and the measures your company has adopted to deal with these risks. It may also be beneficial to instruct them about the actual workings of social media that are most pertinent to your company's operation. And it is also important that all levels of employees, from top to bottom, receive instructions and training on the use of social media, including who has the responsibility to manage crisis situations. Of course, the method chosen by corporations can and will vary from the simple to the highly sophisticated. As reflected in the April 25, 2011, edition of *The Wall Street Journal*, on the upper end of the spectrum, Dell has undertaken the ambitious creation of a "social media university" that provides certifications for employees who take all four of the required training courses.

**Forward thinking.** In many ways, a number of the other steps outlined here all involve a good deal of "forward thinking." When creating business plans, policies and training programs for your company, it is important that you start thinking about the future today. This is especially

crucial in the realm of records and information management (RIM), and legal discovery. What will be the "corporate memory" of events, decisions and interactions that happened within social media? Have you thought of what you may need down the road to prove what the company did or did not say or do through social media in the past? This historic information could be germane to antitrust inquiries, Foreign Corrupt Practices Act investigations, consumer-based lawsuits and employment-related suits, just to name a few. Thinking today about what you might need tomorrow will lead to a coherent and defensible approach to what you keep or discard.

**Don't forget compliance.** Even after you have created a business plan, set up a social media policy and trained your employees to follow it — all these measures will be for naught if there is no effort to enforce them. The level of compliance efforts will likely vary among organizations and industries, in light of the nature of regulation and the interactions themselves. Choosing the best approach for your organization




## Once you have successfully developed or tweaked your social media policy, **you must begin educating your employees about it.**

will be important because you do not want to set up a system of “over-policing” that could be ineffective or counterproductive. Some organizations delegate compliance to supervisors, while others engage third-party resources to assist with compliance. For example, the April 25, 2011, *Wall Street Journal* reported that Farmers Insurance Group uses one such resource, Hearsay Social from Hearsay Corporation, to help enable both participation by agents in the field and compliance back at the home office.<sup>8</sup> In the end, be sure to give a significant amount of thought to the level of risk, complexity and value presented by potential compliance approaches, so that you select one that is practical and effectively meets your particular objectives.

**Ability to adapt.** As an old, anonymous quote states, “The mark of genius is the ability to adapt,” and this is certainly true when applied to the legal and business risks associated with social media. The technology and laws are constantly changing, and so business strategies must change as well. In all likelihood, some aspects of your plan will become outdated three years from now — reinforcing the ever-evolving nature of our digital, business and legal worlds. Rather than rendering these recommendations worthless, however, it makes their implementation all the more urgent. The key thing to

bear in mind is the fact that no policy lasts forever and that continual reassessment and revision will be important in this area.

In short, while there is no talismanic plan that all organizations must follow (and it is not realistic to expect that each company will need to address all areas equally), the eight concepts addressed above should help you create a framework that is tailored to your organization, and addresses social media risks and liabilities for years to come. 

Have a comment on this article? Visit ACC’s blog at [www.inhouseaccess.com/articles/acc-docket](http://www.inhouseaccess.com/articles/acc-docket).

### Notes

- 1 Joseph A. Giannone, “Morgan Stanley Allows Broker Use of Social Media,” *Reuters* (May 25, 2011), [www.reuters.com/article/2011/05/25/us-morganstanley-socialmedia-idUSTRE74O4NF20110525](http://www.reuters.com/article/2011/05/25/us-morganstanley-socialmedia-idUSTRE74O4NF20110525).
- 2 Geoffrey A. Fowler, “Are You Talking to Me?” *The Wall Street Journal* (April 25, 2011), [http://online.wsj.com/article/SB10001424052748704116404576265083970961862.html?mod=ITP\\_thejournalreport\\_1](http://online.wsj.com/article/SB10001424052748704116404576265083970961862.html?mod=ITP_thejournalreport_1).
- 3 L. Gaines-Ross, “Reputation Warfare,” “Spotlight on Social Media and the New Rules of Branding,” *Harvard Business Review*, December 2010, p. 76.
- 4 Andrew D. Goldsmith, “Trends – Or Lack Thereof – In Criminal E-Discovery: A Pragmatic Survey of Recent Case Law,” *United States Attorneys’ Bulletin*, Vol. 59, No. 3, p. 6, May 2011, ([www.justice.gov/usao/eousa/foia\\_reading\\_room/usab5905.pdf](http://www.justice.gov/usao/eousa/foia_reading_room/usab5905.pdf)).
- 5 Not surprisingly, the first cases emerging from the dockets address conduct of individuals but reinforce the importance of social media sites from an evidentiary perspective. For example, one notable case, *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965 (C.D. Cal. 2010), illustrates the legal system’s fluctuation in coping with new technology. In an effort to determine the details of the plaintiff’s oral contract with the defendant regarding their trademark and licensing agreement, the defendant issued a subpoena to the plaintiff involving three social networking sites: Facebook, Media Temple, Inc., and MySpace, Inc. In response, the plaintiff argued that such subpoenas were unlawful and violated the privacy rights accorded to the Stored Communications Act (SCA). After reviewing the details of the case, the federal court overturned the original ruling of Judge John E. McDermott and quashed the defendant’s subpoena with regards to all private communications on such sites. At the same time, the court held that the subpoena was lawful with regards to all other information on said sites, including Facebook “wall posts” and MySpace “comments.” Since this information is visible to any visitor to the plaintiff’s site, the court argued that it could not be deemed private and so protected by the SCA. In a similar case, *Romano v.*

## Social Media Governance

[www.socialmediagovernance.com](http://www.socialmediagovernance.com)

This website includes copies of social media policies that have been adopted by a number of large companies and organizations, as well as other resources, and is a good starting point when creating your own social media policy.

*Steelcase, Inc.*, 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010), the court ordered that the user's Facebook and MySpace pages, both past and present, including any deleted material, be given to the defendant. The Court concluded that because of the nature of social networking sites, any posted information could not be considered private, regardless of the "privacy settings" employed by the user.

- Two occasions in particular illustrate the risk. The first incident — the proposed release of secret Bank of America (BOA) documents found on a bank executive's computer hard drive last November (11/29/2010) — caused the bank's stock to drop by more than 3 percent. N. Schwartz, "Facing Threat From WikiLeaks, Bank Plays Defense," *The New York Times* (Jan. 2, 2011), [www.nytimes.com/2011/01/03/business/03wikileaks-bank.html](http://www.nytimes.com/2011/01/03/business/03wikileaks-bank.html), last visited June 6, 2011. Despite the fact that, to date, no actual BOA documents have been published, the mere possibility that "damaging documents" could be released has had a significant impact on the largest bank holding organization in America. The second incident revealed that not even the US government is safe, as the discharge of confidential State Department diplomatic cables last November (11/28/2010) demonstrates. Hundreds of thousands of secret communications (not all of which have been aired to the public) between US embassies and the

State Department, including evaluations of international issues, leaders and countries from around the world, have been opened to public viewing. Instantly, the documents released, many of which did not speak highly of certain leaders, created a foreign relations crisis for the United States, with Secretary of State Hillary Clinton traveling to a number of countries in an attempt to mitigate the damage.

- Sidebar B contains a list, drawn from the common aspects of hundreds of social media policies that were reviewed as part of the preparation of this article, of what the authors submit as five of the most important issues that should be considered for your social media policy. The policies that were reviewed are those available in [www.socialmediagovernance.com](http://www.socialmediagovernance.com), which is an invaluable resource in this regard.
- Geoffrey A. Fowler, "Are You Talking to Me?" *Wall Street Journal* (April 25, 2011), [http://online.wsj.com/article/SB10001424052748704116404576263083970961862.html?mod=ITP\\_thejournalreport\\_1](http://online.wsj.com/article/SB10001424052748704116404576263083970961862.html?mod=ITP_thejournalreport_1).

A tradition as a full-service law firm serving top corporations and emerging companies.

Over 400 lawyers focusing on business transactions and litigation.

A commitment to continuing to invest in the communities in which we work.



Indiana  
Indianapolis

Kentucky  
Florence  
Lexington  
Louisville

Ohio  
Cincinnati  
Columbus  
West Chester

Tennessee  
Nashville

West Virginia  
Charleston

[frostbrowntodd.com](http://frostbrowntodd.com)

**Frost  
Brown Todd** LLC  
ATTORNEYS