The Legal Ramifications of Employee Use of Social Media

Tracy Paul

March 2010

Caveat: Consult legal counsel regarding any questions or actions specific to your company or situation. This white paper is for informational purposes only and should not, in any way, be construed as legal advice.
ABSTRACT

The World Wide Web has seen a dramatic transformation in the past few years with the emergence of Social Media. Social Media allows anyone to post their own words, creations, voice, videos and audio on the internet for potentially the entire world to see. For businesses, social media has turned into a new marketing, sales and customer service venue. To take advantage of the opportunity social media offers, employees now interact with customers about products, the company itself and even the company culture. Employee usage of social media for work purposes is usually defined. However, employees discussing work issues using their private social websites can cause the company concern. The potential liabilities, including loss of reputation, loss of morale, legal actions resulting in fiscal penalties, loss of trade secrets or giving a competitor an advantage are just some of the possible challenges a company can find itself in if it does not address employee use of social media. Personal accountability and responsibility must be conveyed to all employees as well as the potential risks associated with posting to social media sites. To help mitigate this risk, a social media usage policy is recommended for all companies whether or not they actively engage in social media for company purposes.

Keywords: Social Media, Employees, Legal, Productivity, Branding
Introduction

The internet has revolutionized the way society communicates. This revolution is still occurring with the advent of “Web 2.0” and the social media craze. Social media, defined generally as the ability to post your own content for millions to see, has dramatically changed the way businesses market their products to consumers, the way consumers investigate and review products, the control over branding a company has and the interaction companies can expect from their customers. Social media environments, like Facebook, Twitter, LinkedIn, blogs, virtual worlds, online forums and reviewing sites have shifted control of brand perception and information dissemination from the corporate businesses to the individual consumer. This paradigm shift has caused an unsettling realization for businesses that they must monitor and mitigate their own liabilities when it comes to social media communication. One particular liability of concern is that which can occur because of employee interaction with customers in the business environment or even employee discussion of their job during their personal use of social media. Employee indiscretions on the web, to customers or on their own personal sites, may lead to potential loss of competitive advantage or even legal actions filed by regulatory institutions, competitors or company employees themselves. This paper proposes to research and discuss the legal ramifications of employee use of social media for business and personal reasons related to business and the positive and negative affects social media can have on a company.

Overview of Social Media Environment

The use of social media has grown exponentially on a global basis in this past year alone. Facebook increased its growth by more than 111% in 2009. Twitter posted a 14-fold increase globally, ending the year with 65 million visitors. (comScore.com, 2010) Mobile internet usage, amplified by the sale of the Apple iPhone, has seen a boom in services across the board while Social networking on mobile devices increased 106% overall in 2009. The trend shows no sign of slowing down over the next few years.
Social media is still used predominately as a vehicle for personal socialization and communication. For instance, many teenagers today don’t use e-mail at all – they use Facebook. Many people interact on social media sites, keeping their friends and family informed of current events or to let them know what they are thinking. Some people use blogs as their personal soapbox – a place where their own opinions can be heard and shared on the World Wide Web. Anyone and everyone may access to view this blog and comment on what is said for others to read.

For business, this proposes a provocative and intriguing opportunity. Most companies initially slept through social medias’ birth without seeing social medias potential to promote their product. It wasn’t until businesses started reading about their products on consumers’ blogs and social network outlets, and that those opinions shared in those outlets were being read and listened to by more than just a few people, that companies became aware of the potential tremendous power of social media. Businesses were discovering that people wanted to talk about and interact with their products. In response to this realization, some businesses set up corporate social media programs to interact directly with consumers.

For companies reading opinions, savvy marketers realized the value of listening to what these consumers were saying – Clorox found that consumers were suggesting other uses for bleach (off-label) that were intriguing to the manufacturer. Their simple product, bleach, was generating entire discussions on the blogosphere not just on uses, but how consumers liked the product, how they felt about the brand and what consumers didn’t like about it. Clorox also found that they could not only monitor consumer interaction but participate by answering questions, addressing concerns and engaging consumers on a personal level in a large group setting (Neff, 2010).

Social media has become so common-place, government and legal organizations recognize it as a valid source for public information. In July of 2008, the SEC declared that posting updated company
information on a company blog met public disclosure requirements (Solis, 2008). Lawsuits filed citing posts on social media have been held in court. Social media, while being fluid and flexible, is now being held to a standard similar to the fax machine.

For many companies, this means that regulatory (SEC or FDA) requirements now need to be met on company blogs or Facebook pages. Employees of a company must be very careful of what they post to insure compliance with regulations. This, of course, makes sense, but what about an employee who blogs about the company on his/her own personal Facebook page or blog? What if they do this personal blogging while at their workstation?

It would seem if the information is harmless or non-defaming, there should be no concern, correct? Unfortunately, this is not necessarily true. There are many cases (some examples given later) of employees posting seemingly irrelevant and harmless content either about work or about something to do with work that have come back to bite them and the company. Because of this, it may seem obvious that employers should disallow their employees from engaging in social media at work. There are, however, advantages to the employer if employees are allowed to use social media.

**Employee use of Social Media for Work and Personal Business**

Some high profile companies are now actively encouraging their employees to use social media. IBM has a policy available online that encourages employees to blog and participate in social media forums. Macy’s has a Facebook site; Zappos trains their employees on the proper use of twitter accounts to interact with customers. Many more companies are getting their toes wet as they realize the exponential growth of social media usage by the population in general.

For companies who actively participate in social media, employees monitor various networks to see what customers may say about the company or product. Some companies even actively pursue
Customer Relations Management (CRM) strategies by interacting with customers directly through blogs, Facebook pages or online forums. They can even address their customers’ questions and concerns directly on customer network accounts.

Some employees and executives also routinely monitor competitors’ social media sites for trends and intelligence. In fact, many law firms are now diligently monitoring not only their competitors’ websites but the employees of those competitors’ personal websites for any insights or competitive advantage. (Lambert, 2010)

Regarding personal use, Facebook is, by far, the most popular social networking site with an estimated 77% of employees having a personal Facebook account, with 61% accessing their Facebook account from the office. In fact, one in every 33 employees built their profile and check their Facebook account solely at work. (Nucleus Research, 2009).

The average employee who access Facebook at work uses it for about 15 minutes each day. With 61% of the workforce using Facebook, employers can estimate the loss of productivity cost at roughly 1.5% of total employee productivity. (Nucleus Research, 2009)

With these pros and cons in mind, how can a business decide whether to let their workforce use social media during work hours for work or for personal purposes?

To Allow Social Media or Not To Allow....

According to Russell Herder, “...more than eight in 10 executives have real concerns about social media and its implications for both corporate security and reputation management.”(Russell Herder, 2009) Many of these same executives are greatly concerned about the loss of productivity related to using
social media for personal purposes. The dynamic now becomes a tradeoff as to which strategy would be the best to take regarding employee use of social media.

There are three possible scenarios that businesses can adopt (Kelleher, 2009):

1. Completely ban access to social networking sites (and the internet as well)
2. Set limits and restrictions on use of social networking sites
3. Allow unmonitored access to social networking sites

Which strategy is used really depends on the company culture and what the company produces. While many companies are tempted to jump onto the social media bandwagon, it may not necessarily be the right option. For example: A Pittsburgh company received a majority of its revenue from Defense Department contracts. This same company decided to allocate $4 million for social media marketing and branding. After some thought, the company realized the security and privacy-conscious Pentagon might not be happy with them for promoting themselves in such an unpredictable forum. The company subsequently scratched the social media project. (Baker, 2009)

With that being said, if a company is in a position to engage in social media, it becomes a question of how much of a trade-off the company is willing to make regarding interaction in this new medium versus the risks.

The benefits are clear:

- Market research that is interactive and inexpensive with results that are comparable to more expensive research strategies
- Customer interaction and the personal care a customer can feel when their issues are addressed and handled.
• Branding the company to potentially the entire world.
• Solidifying the company reputation by responding quickly to concerns, mitigating negative feedback risk by proactively addressing problems with a product.
• Promoting a corporate and/or product “culture”

The concerns are also clear:

• Loss of productivity due to personal use and time consumed attending to a social network account.
• Bandwidth usage can slow down a company network if social media users are downloading videos from YouTube or using other bandwidth-eating applications.
• Real risk of acquiring a virus or Trojan horse. Twitter and Facebook are common paths hackers use to get access to unsuspecting users who unwittingly download malware.
• The legal liability resulting from employees comments (unintentional or negative) that might harm the company and hold the company accountable. (Kelleher, 2009)

This last concern is of greatest importance as the potential for true monetary and legal harm can be caused by a breach of confidential information by an employee or by a mere comment that can hold the company liable for damages.

Legal Issues Associated with Employee Use of Social Media

Under state and federal law, people who post content on the web (text, audio, artwork and video) are considered publishers and are allotted the same rights and held to the same rules and liabilities as classic published work. (Donovan/Hatem, 2009). Aside from copyright and trademark infringement issues, publishers should be aware that they can be held liable for omissions, breach of confidentiality
(intended or unintended), free speech infringement or hate speech, mistakes, defamation and slander, true but unflattering comments or pictures about a third party, privacy transgressions (public disclosure of private or embarrassing facts, misappropriation of a person’s name and likeness, etc.), causing personal or emotional distress as a result of intrusion, or infringe on a person’s right of “publicity” (that person has exclusive rights to control or exploit their own name and likeness). (Answers.com, 2010)

The legal obligations of an employee using social media for company reasons is far easier to monitor and to understand than social media for private use. Since many companies are now seeing the benefits of using social media to promote their company, brand and messaging, many companies engage in this realm and coach their employees on what to say and how to respond. Employees tend to respond thoughtfully and not impulsively to customers when interacting with them through social media, knowing that their interactions are recorded and can be used as evidence of the discussion. There is no delete button once something is posted and employees representing their companies usually have this in mind. Even if a post is removed, it can be traced through web logs or through previous backups. Anything typed and published on the internet is there to stay in one form or another.

Of course, the marketing and legal departments monitor employee responses to customers to ensure employees are not infringing on legal territory. These departments, ideally, work in conjunction to get the proper messaging out to the customer while insuring legal compliance with regulatory and SEC rules as well as company policies.

When it comes to employees using social media on workplace computers for personal reasons, workers inhibitions tend to go out the window. This is a mistake. Many people who post content on a social network, blog, wiki or forum do so impulsively – they do not think through the ramifications of what they are saying and how what they say or post can be interpreted. While most individuals do not get
into trouble over thoughtless comments on a personal basis, companies, and as an employee of that company are held to a different standard.

The employee does not need to be at work using company computers to still be held responsible for their job-related posts. They can be at home posting comments on private pages and be held accountable for what they publish. For example, a disgruntled employee blogs about his job and his frustration regarding that job – the company doesn’t pay its’ workers overtime yet asks for long hours, the product the company makes is worthless and that he hates his boss. Several problems arise out of this published content. First, a competitor can read this blog and use it as evidence of inferiority of this company and its products. (Make no mistake that savvy competitors are monitoring social networking sites of companies and their employees. A competitive goldmine would be had by reading this employees blog. There is no law to prevent the competitive company from printing the blog and showing it to potential customers.) Second, the company itself and its product are being publically defamed by the employee. This could damage the company’s reputation and potentially hurt future sales. This also hurts morale and causes a PR nightmare for the company to deal with if this post became well known. Third, if the boss reads this post, what is he going to do? Does he speak to the dissatisfied employee? Is there probation or some sort of punitive action taken? Does he have the right to fire the employee?

Some companies have fired employees over blog posts. The company that does fire an employee for this reason, whether they are disgruntled or posting what the company would consider “questionable,” may now be subject to an unlawful termination suit or invasion of privacy filed by the terminated employee.

Take for example the case of Ellen Simonetti, flight attendant for Delta Airlines. In the early days of social media, she posted her “Queen of the Sky” blog about all things related to international travel. She even posted a couple of pictures of herself in uniform posing somewhat provocatively. Delta Airlines
took exception to these pictures as a misrepresentation of Delta Airlines and grounded the flight attendant then fired her one month later. Ms. Simonetti, shocked at this decision filed a sex-discrimination lawsuit for $10 million (Negroni, 2004).

How can employers handle employees who may use social media to threaten, bully or degrade fellow employees? With current safe workplace laws, it is the company’s obligation to take action to stop this form of harassment in order to insure a harassment-free workplace, or else the company may find itself the subject of a lawsuit. (Parker, 2009)

An employee may accidently, unintentionally or purposefully disclose proprietary company information in their blog or social media page. This could lead to serious legal ramifications as this information might divulge trade secrets, negate a competitive advantage, reveal discussions with companies that weren’t public knowledge (a merger or acquisition or partnership), or infringe upon disclosure laws from the SEC (regarding insider trading and other tightly regulated company information).

Sometimes, the problems that arise aren’t necessarily legal but still can negatively impact the company. If an employee tweets “working late- found a bug in software that needs fixing”, it seems innocuous enough. However, if a savvy competitor were monitoring this and other employees’ tweets, and combined it with other information gleaned in context, it could reveal information that may help that competitor. Or, if a customer were to read this tweet, it might concern them that the product they purchased might have a safety issue or malfunction. Do customers really monitor their vendors’ employees’ social media sites? Yes, they do.

For example: an executive at Kechum, New York, having just landed in Memphis tweeted “True confession but I’m in one of those towns where I scratch my head and say ‘I would die if I had to live here!’” Seems harmless enough, but the executive was in town to meet with one of his company’s
largest accounts – FedEx, which is based in Memphis. An employee of FedEx read the tweet and was offended. This employee responded to the executives tweet (and cc’d executives at both Ketchum and FedEx) the following:

“If I interpret your post correctly, these are your comments about Memphis a few hours after arriving in the global headquarters city of one of your key and lucrative clients, and the home of arguably one of the most important entrepreneurs in the history of business, FedEx founder Fred Smith.” (Davis, 2009)

Moral of the story: what an employee says online whether on a work social media site or a private blog, can come back and bite the company.

Another issue that is of concern is the accidental or unintentional downloading of malware or spyware from these varied networks. Many hackers and unethical businesspeople use these spaces to generate mailing lists and send SPAM. Facebook has thousands of third-party applications hosted on its site that are downloadable by employees. Malignant code buried in one of these applications can infect not only an employee’s computer but the entire company network. The virus can possibly collect personal information from all of these computers or slow down the network to a crawl, causing loss of productivity.

Data and identity theft are also concerns. It’s astonishing how an employee will not give out highly personal information to a live person they just met but will publish confidential information on their social network profile without a second thought.

Legal System Ability to Cope

Much of the law regarding social media can be interpreted through current publishing law. (Neff, 2010)

The difference is the new way the technology is used and how it’s used. While the legal system is
comfortable dealing with publishing law, it is notoriously behind the times when it comes to the internet and the ever-changing technology associated with it. It is not clear how a given ethics rule will apply to a new technology and “...the lack of precedent and clear guidance means that each situation may be judged on a case-by-case basis.” (Stine and Poje, 2009)

In other words, social media is so new; the legal system has to play it by ear. With this in mind, many corporate attorneys and HR staff find themselves looking for guidelines on how to mitigate risks and litigation from improper employee use of social media. One answer to this question is to create a social media usage policy.

**New Company Social Media Usage Policies**

More than eight in 10 executives stated they have concerns about social media and what it can do to their company’s reputation; brand and messaging yet only one in three have actually implemented social media usage policies (Russell Herder, 2009). Why so few? Many companies are unsure about what to include in such policies (25%) or the issue hasn’t been addressed (13%) or some companies just don’t think it’s important (9%) (Russell Herder, 2009).

As the high school aged population moves to college or their first jobs, more and more employees will have been using social media since they were children. This means that social media is a natural outlet for their communications to friends, family and other contacts. Companies that do not address the legal concerns of employees using social media will find themselves behind the times when dealing with problems that result from not having any guidelines in place.

Some companies recognized this challenge early and have implemented their own social media usage policies. Intel, a leading chip processors manufacturer, clearly states employees’ responsibility in using social media with company objectives in mind. Intel recognizes that their social media policy must
empower employees to make decisions on what to say and how to say it while acting responsibly in the company’s name. Intel goes so far as to have their very own Social Media Center of Excellence, which trains employees on how to use social media for Intel purposes. Intel will at times moderate its’ publishers until they have been through Intel’s training. Intels’ policy, however, only addresses social media use on behalf of the company and for company purposes and not employee personal use of social media (Intel, 2009).

IBM has one of the most robust social media usage policies. Consequently, many companies have asked IBM for guidance on how to draft their own policies. IBM clearly states ethics guidelines and publishing policies regarding IBM business. IBM also addresses employee use in a private setting by requesting employees use a disclaimer with that post. (IBM, 2010)

FedEx hosts a “Citizenship Blog” in which customers can participate discussing FedEx’s many charity programs around the world. FedEx’s social media policy only addresses this blog, which is moderated for appropriate content. (FedEx, 2010)

GM has a very simple Blog site “GM FastLane Blog” discussing cars, auto shows and more. GM uses this blog as a forum for GM executives to interact with consumers, inform them of future products, designs, etc. They have posted a simple blogger policy regarding their standards and how they will treat their customers. Like FedEx, GM’s policy only covers their specific blog and not social media in general. (GM, 2010)

While researching this paper, I found that technology companies (IBM, Intel) tend to have more robust social media policies. HP, however, is an exception. HP only addresses their blogs. HP’s code of conduct for blogging states what the customer can expect from the blog and how HP will respond to questions and concerns. What HP does that is different than other companies is openly promote its’ employees
individual personal and business blogs – including having a link from the HP site to those blogs directly. HP standard code of conduct and ethics still apply. (HP, 2010)

Jaffe PR, a law firm, has posted a comprehensive policy for Social media and Social networking for employees on behalf of the company. The policy recognizes that employees will use social media for company and personal use and particularly focuses on author responsibility to the company and to the credibility of the author. (Jaffe PR, 2010)

The State of Delawares’ Department of Technology and Information has established a Social Media Policy that covers all state government departments and agencies. Unlike most other companies, the State responds via social media not only on an individual employee basis but as an organization. Any state organization that intends to establish a social media presence will be held to the standard of this policy. (State of Delaware, 2010)

Webtrends policy does not name specific social media venues but simply states what the company expects of itself and its employees when interacting in the social media arena (Webtrends, 2010). In fact, Webtrends uses the same basic standards as GM, both of which obtained their guidelines from Charlene Li’s blogger code of ethics (Li, 2004). While the skeleton of this guideline still holds true, it does not address the current Web 2.0 world with social networking, wikis, YouTube and twitter. Li’s guideline is antiquated.

A noticeable trend for many businesses is that they do have blogging policies in place but these policies do not address social media in its entirety. This is perhaps because social media, with a broader definition than blogging, is still just really starting to be noticed in corporate America at large. For companies that do expand their policies to include social media, they do not seem to address employee use in private matters as much as they probably should. Perhaps this is because discussing what
employees do on private time might be interpreted as an invasion of privacy and frowned upon by employees and HR.

Conclusions and Recommendations

Clearly, a need for corporate protection exists when it comes to company employees interacting with each other, on behalf of the company or in private through social media. The problems that can occur from thoughtless posts or disparaging remarks can cause great harm to a company’s reputation, brand and even make a company legally responsible for a breach of law or open to a lawsuit. Because the technology of social media is relatively new, the legal community has not yet fully developed standards of conduct or rules of thumb to regulate social media usage and responsibility.

Companies have two pieces of guidance they can use to address this situation:

- Companies can rely on the law of publishing to guide them on proper, ethical and legal matters of authors making posts online as a baseline of how to regulate usage in the Web 2.0 world.
- Companies would greatly benefit from a social media policy integrated in an employee handbook as well as posted online for all customers and employees to see.

A social media policy is not just for big companies. Any company that has employees can find themselves in potential hot water over what an employee has said or done on behalf of the company or from using the company’s computer hardware. A thoughtful and respectful social media policy, addressing business and personal use as it pertains to the employees’ job, will help reduce and mitigate potential troubles by making an employee’s responsibility to the company clear and concise.

What should the policy address?
• What is social media? Define social media to employees as broadly as possible to cover potential future technologies and their integration. Do not narrow the discussion to blogs and social networks – wikis, content sharing sites such as YouTube and Yelp also qualify. Tweets, mobile messaging, micro-blogging, online chats, virtual worlds like Second Life and World of Warcraft, and instant messaging are also part of the social media forum.

• How can participating in social media impact the company? Many employees don’t even think about how their posts, tweets or videos may in fact, potentially harm the company. Discuss what employees need to look out for when posting to their private pages regarding their work.

• If employees do reference their employment on private networks, employees need to disclose their relationship with their employer in the post. A disclaimer regarding the opinion of the employee is not meant to portray the opinion of the company can be used such as “The postings on this site are my own and don’t necessarily represent (the company’s) opinions or beliefs” (IBM, 2009).

• Expected privacy? Let employees know that any actions they take on company computers can be monitored. The employee should have no expectation of privacy when using company computer equipment for business or personal reasons.

• How does the company expect its employees to behave when interacting in social media on behalf of the company? Lay out ground rules about how employees respond to customers, including timeliness of response, tone of response and ensure these responses follow corporate ethics and code of conduct guidelines (no political posts, no slander or angry posts, no questionable material, harassing posts or infringing on copyright laws). Employees must also understand the rules of posting to third-party sites for company purposes (clearly identify themselves and who they work for).
• Should employees be allowed to download applications onto corporate computers? Address the concerns of malware, spyware and identity-theft to employees so they are aware that a promising-looking application on Facebook can potentially contain a virus that may infiltrate the company network and cause problems.

• Should employees discuss competitors on company social media venues? Competitors can be discussed but not disparaged. Answers to customer questions with a professional tone and neutral comment regarding competitors are the best policy. Competitors will be reading company social media forums to see what is said about them and will take action if they don’t like what they read.

• What should an employee do if they make a mistake? If an employee accidently discloses non-public information, fights with a customer or posts an unfounded opinion, these mistakes need to be addressed immediately. The employee should not fear severe repercussions as a result of this discretion. This should encourage employees to report their mistake in a timely manner. Removing the false or sensitive posts and calmly concluding arguments must be handled as soon as possible. Also, make any redactions clear to users – don’t hide the fact that redactions were made, rather state some sort of reason for the redaction (example: “information is unverifiable” or “comment not appropriate to guidelines”).

Make sure a lawyer thoroughly reviews the policy for any adjustments due to applicable state and local laws not covered. When the policy is complete, make sure all employees are handed a copy and have them sign a form stating they have read and understand the policy. Include the policy in employee handbooks.
Social media is here to stay and through the nature of technology improvements, the nature of social media will evolve. With forethought and some sound legal advice, companies can mitigate legal issues as well as protect company assets by using a social media policy.
References


Social Media in the Workplace

http://citizenshipblog.fedex.designcdt.com/about_the_blog

http://fastlane.gmblogs.com/about.html

http://www.hp.com/hpinfo/blogs/codeofconduct.html


http://blogs.webtrends.com/about-this-blog/social-media-guidelines/