Social Media: The Business Benefits May Be Enormous, But Can the Risks – Reputational, Legal, Operational – Be Mitigated?

Toby Merrill, Vice President, ACE Professional Risk
Kenneth Latham, Vice President, ACE USA Professional Risk
Richard Santalesa, Esq., Senior Counsel, InfoLawGroup LLP
David Navetta, Esq., CIPP, Partner, InfoLawGroup LLP
focus on:

Social Media: The Business Benefits May Be Enormous, But Can the Risks – Reputational, Legal, Operational – Be Mitigated?

Toby Merrill, Kenneth Latham, Richard Santalesa, David Navetta

Part I: Overview

What Is Social Media and Why Should Your Company Care?

In less than a decade, social media, in many ways, seems to have “taken over the world.”

This statement is not hyperbole. As one of the largest social networking sites in the social media universe, Facebook boasted more than 750 million people actively using its service. If it hasn’t already, Facebook will soon grow twice as large as the population of the United States, which currently hovers at 311 million.

Even so, the vast majority of companies did not immediately join the social media revolution. Instead, they spent varying amounts of time observing from the sidelines. But when the first wave of companies did join, it was because they anticipated the significant business benefits of this “brave new world” – where the personal, the professional, and the commercial combine seamlessly, and in the blink of an eye.

Many others, however, remained unconvinced – often because of a lack of information and an unclear understanding of how social media could be beneficial. “What is this ‘social media’ thing all about?” they wanted to know. “And why should my company care?”

Unlike traditional media, which offers a one-way experience (in which media outlets broadcast information for public consumption), social media offers a two-way interactive experience. Consumers of social media, unlike consumers of traditional media, can interact instantly and directly with either the originators or the authors of the proffered information. They can interact with each other, too. The interaction and cross-communication that social media makes possible is precisely what makes social media so world-changing.

As with any new technology, there is a downside. Social media also creates a whole new world of privacy, security, intellectual property, employment practices, and other legal risks, to name just a few (in Part III of this paper, we will review each risk).

But the opportunity to interact with anyone, anywhere, anytime is too world-changing to ignore. It has altered the traditional media expectation of consumers listening passively to radio and television broadcasts, or reading newspapers and magazines, with no hope of an immediate interaction (and no way, certainly, for customers to converse with companies). With social media, all that changed. Individuals and groups suddenly have a radical new ability to voice opinions through this new media, a channel never before available. Using social media, everyone can become a commenter, editor, content creator, producer, and distributor.

Not only that, but the entire world has become accessible in ways that are disorienting for traditional media and those accustomed to its cultural hierarchy. Consider the popular social networking site, Twitter. This platform allows anyone with an account to post short messages. To tailor the onslaught of messages being broadcast from the “Twitter-sphere” of 200 million current Twitter subscribers, users can create lists of those they wish to “follow” so they only receive Twitter feeds from those they select.

With Twitter, anyone can send a short message of 140 characters – called a “tweet” – about any topic, including the famous and the infamous, the holy and the ethically challenged. Anyone, for instance, can tweet about President Barack Obama and Lady Gaga, or the Dalai Lama and – well, you get the idea. Twitter is just one of the components in a social media portfolio. England’s Queen Elizabeth II, already with a Twitter account, added a Facebook page last year to complement her YouTube channel, Flickr account, and website.
Perhaps most surprising, social media has been an enabler of grassroots revolution in countries where such an event seemed impossible. As a case in point, look at the impact of social media on the governments of Colombia, Egypt, Indonesia, Iran, Libya and Tunisia, to name but a handful. In summing up this trend, author David Kirkpatrick in his book, The Facebook Effect, observed that the “large scale broadcast of information was formerly the province of electronic media – radio and television. But the Facebook Effect – in cases like Colombia or Iran – means ordinary individuals are initiating the broadcast. You don’t have to know anything special or have any particular skills.”

The social media universe encompasses a much broader array of interactions than those that occur on popular and familiar social networking sites like Twitter and Facebook. “Social media” actually refers to a growing galaxy of sites that includes: personal and business blogs, news sites with interactive or comment features, group forums, wikis, social and business networking sites, online community sites, social bookmarking sites, microblogging sites, and gaming as well as virtual world sites. (See the Glossary of Social Media Terms on page 10 for brief definitions of these and related terms that appear in this paper.) Social media embraces a cyber-universe of websites that promise to expand – virtually – forever. (One example: according to WhiteboardAdvisors.com, by the end of 2010, there were 152 million blogs on the Internet.)

In short, like earlier methods of communication that seemed new and a little strange when they first appeared, social media, writes Facebook Effect author Kirkpatrick, “…is a new form of communication, just as was instant messaging, email, the telephone, and the telegraph.”

Part II: How Can Social Media Benefit Business?

“The exponential growth of social media, from blogs, Facebook and Twitter to LinkedIn and YouTube, offers organizations the chance to join a conversation with millions of customers around the globe every day.”


The key word in the quote above is “conversation,” since attracting customers by creating a social network is entirely different than broadcasting ads, or employing marketing strategies to convert targeted groups of consumers into customers. Creating online conversations also requires a whole new approach and skill set.

Social networking sites encourage businesses to change their traditional marketing strategies and focus on talking with – not at – prospects and clients, with the goal of developing and “deepening the relationship” between the company and customer. But what’s the business benefit of that deepened relationship? When prospects grow to “know, like, and trust” a company, through interacting with their representatives on social networking sites, they are much more likely to do business with that company.

“It is well-established that people feel more connected with a company when they have direct communication on an ongoing basis and opportunities to express their opinions,” commented Lisa Brown, in an article about the use of social media risks in business. Indeed, social networking conversations create a level of immediacy and a kind of public intimacy that is impossible with traditional marketing. And since most large or medium-size companies are perceived by the public as relatively “faceless,” social networking gives companies the opportunity to present a human face in the form of a social media spokesperson – an individual who can nurture person-to-person conversations which builds trust in the company’s authenticity as well as its professionalism.

But there is something else that social networking sites offer a business that no other form of public interface does: the ability to monitor public perception of its brand, products, and services in real time. As an accompanying result, companies also have the opportunity as well as the responsibility...
to provide a quick and effective response, if a negative perception goes viral through social media’s worldwide interconnected platforms. Reputation monitoring and repair aside, there are multiple strategies companies can use with social networking sites. As cited in The Harvard Business Review, a large U.S. construction materials company employs a variety of social networking platforms in order to accomplish a handful of business-supporting aims. According to the report, “the company uses Twitter to get news in front of reporters; LinkedIn is where company salespeople post scholarly articles to share with each other and their customers; their Facebook page focuses on the company’s social responsibility efforts, while the company blog is more of an exchange with customers.”

As comprehensive as that may sound, it is in reality just one aspect of how a business can harness the power of social media. Several additional popular strategies companies employ include:

• Branded “Fan” Pages on Social Networking Sites (to establish a social media presence – on Facebook, Twitter, YouTube, and Flickr)
• Quick Online Response to Rumors and Negative Perceptions (social media is ideal for countering negative viral news about a company)
• Information Disclosure – Public Broadcast (social media is an effective way to reach large numbers of people, whether they are actual or potential customers, shareholders, or investors; the U.S. Securities and Exchange Commission (SEC) has been moving in this direction for disclosure of required and public information disclosures)
• Employment Practices (human resources departments increasingly make use of social media – particularly LinkedIn and Facebook – to gather information when making hiring and promotion decisions)
• Customer Service and Feedback (companies set up blogs to communicate product development information and gather comments from consumers; companies also use Twitter for customer service and feedback: for instance, Best Buy’s Twelpforce Twitter account)

• Promotions and Contests (encourage site members to engage with a company’s products or services)
• User-Generated Content Promotions (companies also engage customers on social media platforms by encouraging them, with prize incentives, to write about why they like a particular product; caution must be used with such promotions, however, as Federal Trade Commission (FTC) guidelines regarding paid “endorsements” can lead to legal liability without full public disclosure)
• Word-of-Mouth Marketing via Blogs (companies provide their products to popular bloggers with big reader audiences, hoping for a favorable review; but a number of risks have developed in this area, including FTC disclosure requirements, as in the strategy above)

These diverse forms of social networking may cover a lot of business bases. But how do they translate into business benefits?

For the most part, the business benefit of social media is indirect, in much the same fashion that public relations is, although some companies can point to a measurable relationship between their social networking efforts and sales. If we look at the social networking strategies of a national chain of coffee shops (a well-known chain with 5.4 million fans on Facebook, 4,800 subscribers to the company’s YouTube channel, 4,880 members on Flickr with 15,900 photos, and more than 700,000 followers on Twitter), we see that their overall business benefit comes in the form of customer “identification” with the company and its products. Identification is critical: from it grows online interaction, and from online interaction grows customer loyalty. Being able to claim more than five million loyal customers is a “bankable” social media benefit.
PART III: What Are the Reputational, Legal and Operational Risks of Social Media Participation?

“Social media has changed how people communicate and interact, how marketers sell products, how governments reach out to citizens, [how universities recruit students], even how companies operate. It is altering the character of political activism, and in some countries it is starting to affect the processes of democracy itself.”

David Kirkpatrick, The Facebook Effect

As mentioned earlier, social media makes a whole new world of privacy, security, intellectual property, employment practices, and other legal risks possible. It is important to understand the considerable downside that exists hand-in-hand with the remarkable upside of using social media for a variety of business aims, which can occur in three major areas of risk: reputational, legal, and operational.

Reputational

The reputational risks of social media can easily equal or exceed the reputational benefits, for one simple reason. The vast reach of social media platforms – on which millions, globally, communicate every second of every day and night – offer not only a vast frontier of promotional opportunity, but a vast uncharted “sinkhole” of risk.

In April 2009, two employees of a national pizza delivery chain made a prank video in which one of them tainted a sandwich, ostensibly intended for delivery to customers. When they posted their video on YouTube, it drew over a million viewers. Because of that extreme degree of interest, word of the video trended on Twitter, and within 48 hours, consumer perception of the pizza chain had pivoted 180 degrees – from positive to negative. The company attempted to perform damage control by quickly launching its own Twitter account to counter rumors and answer questions, while its CEO took to YouTube to personally address the public’s concerns. By that time, however, any online search for the pizza chain’s name turned up references to the prank video story on the first page of search results – a true PR nightmare.

But there are less dramatic and drastic ways that employees can harm a company’s image. General “bad behavior” by employees, or the posting of embarrassing information, has the potential to reflect poorly on the company (especially when that behavior is exhibited in a “branded” social media location, for example on a company’s “Fan” page on Facebook). According to the Miami Daily Business Review, “Employees who disparage coworkers, management, clients, vendors or even the company itself, whether intentionally or not, can damage a company’s reputation.”

Ironically, as discussed below, employees who praise their company’s products or services can unintentionally get their employer in hot water, too.

Legal

The legal risks associated with social media should be carefully considered prior to engaging in a social media strategy. The main risks include: employment, privacy, security, intellectual property and media risks. Business managers who want to implement a social media legal strategy should consult with inside and outside counsel who understand information technology law. While these legal risks can be significant, with forethought and planning, they can be managed. In this part of the paper, we will provide an overview of the key risks.

The following are some common situations in which social media can be the occasion for legal action:

Employment Risks:

- The practice of investigating potential and existing employees through social media is widespread. According to The Allentown Morning Call, “Seventy percent of recruiters and hiring managers in the United States have rejected an applicant based on information they found online. In total, nearly one in five companies has disciplined or fired an employee for social media misdeeds.”

Employers who hire outside vendors to investigate either an applicant’s or an employee’s social media activities and content may be required by law to get written consent from those individuals. The information collected from a social media site may constitute a “consumer report” under the Fair Credit Reporting Act (FCRA). If so, the employer seeking to acquire such information must, in some cases, obtain an individual’s consent before the employer may acquire the “consumer report” (e.g., credit report) regarding that individual. In addition, the FCRA would require employers to provide information to individuals as to how they may dispute the accuracy of the report with the company that furnished the report. This requirement, however, applies only when the employer takes an adverse action based on the report (such as not hiring or promoting the person in question). In addition, a number of states, including Illinois, Oregon, Hawaii, and Washington prohibit employers (with certain exceptions) from using consumer reports in the hiring and promotion processes.
• Impermissible discrimination in hiring based on social media research can subject a company to investigation by the EEOC, as well as possible action for alleged violations of the Civil Rights Act of 1964, the Age Discrimination in Employment Act, the Americans with Disabilities Act, and many other federal and state statutes. 17

• Companies whose employees participate in conversations on social media platforms while using company computers may want to monitor their employees’ social media communications. Such monitoring is not without its legal dangers, though, as an employer may then be subject to liability under the Stored Communications Act (part of the larger Electronic Communications Privacy Act), if an employer accesses the content of non-public communications not stored on the company’s own server. In addition, if employees and/or managers engage in unprofessional exchanges online, that can lead to harassment claims against the company.

• Social media legal risks may also be present if an employer decides to fire employees based on their Facebook interactions with other employees in the organization. In one incident, where an employee was fired for negative comments about her supervisor posted on a Facebook page shared with other employees, the National Labor Relations Board (NRLB) said that employer’s action violated the National Labor Relations Act (NLRA). In the NRLB’s view, the firing interfered with employee rights under the NLRA stipulation relating to union organizing – which allows employees to discuss wages, hours, and working conditions with co-workers and others, while not at work. 18 In another case, an employee alleged that a company’s social media policy restrictions on employee communications about the company (on such sites) was a violation of the NLRA. 19 The first case settled and the second complaint was resolved for an undisclosed amount, along with an agreement to revise the company’s social media rules.

• Social media sites pose potentially increased security risks, and if a security breach arises from social media activities, the organization may face liability. Security breaches may occur because of malware downloaded onto an organization’s website through the use of social media. This can happen when an employee downloads an application, or is a victim of “phishing” or “clickjacking” on a social media site while using a company computer. If the organization’s social media-related security policies, procedures, and technical safeguards are inadequate, it may be held liable for a breach arising from the surreptitiously acquired malware. In addition, social engineering within social media sites, as well as “spoofed” social media profiles or pages, provide other points of entry for attackers and pose more legal risks for organizations. A spoofed site is one where criminals have set up profiles or fan pages to look exactly like an organization’s own page. If a customer or employee is tricked into providing company information, personal information, or sensitive information (such as usernames and passwords), it could pose legal liability risks to the organization whose profile or fan page was spoofed, or replicated in a fake version.

• PR News warns, “Make sure your social media team understands what they can and can’t do with the intellectual property of others. If your employees post or re-post information [belonging to others] without permission, this can lead to infringement claims against your company.” 21 It could also result in potential contractual breach claims, if the intellectual property belongs to an existing client. Companies may be held directly liable for hosting material on their website in circumstances where the safe harbor protections of the Digital Millennium Copyright Act may be unavailable – or vicariously liable for employee actions on third-party sites that infringe the copyright, trademark, or other intellectual property rights of others.
• Furthermore, employee discussions on social media sites could disclose third-party trade secrets that the company is legally required to protect, and that can lead to misappropriation and other contractual and tort claims. Companies are generally legally responsible for any financial statements on social media sites made by them, or on their behalf, through the antifraud provisions of securities laws.

• As mentioned earlier, employees who praise or promote their organization’s products and services may create legal liability. The FTC may regard positive statements by employees (when their relationship to the company has not been revealed) as “improper advertising.” For example, if an employee were to publish a fake positive review of its employer’s products or services, or encourage others to do the same, it could violate section 255.5 of the FTC’s Endorsement and Advertising Guidelines.22

Defamation Risks:

• Defamation is yet another common claim that may result from social media activities, and companies need to be aware that they face potential liability for defamatory statements made by their employees about competitors, and for defamatory statements made by the public on the companies’ third-party social networking pages.

Privacy Risks:

• Companies may have an obligation to protect the privacy of members of the public who join their social networking pages on third-party sites, or who provide personal information through social media sites – just as they do, in many cases, when the public provides personal information on the company’s own website. For example, not only do companies need to guard against violating the Children’s Online Privacy Protection Act (COPPA), they need to conform to the privacy regulations and terms of use of those third-party sites. Facebook, for instance, has stringent guidelines surrounding company promotions on their site.22 Finally, companies may run into legal trouble if their social media activities violate their own privacy policies.

• Lastly, there are several ways in which social media activity might compromise or leak sensitive company information (or client information) that could have legal consequences. These are: through crowdsourcing sites (the company posts a problem and asks for solutions from the public, with the unintended consequence that trade secrets are indirectly revealed); through inadvertently compiled client lists (a vice president’s contacts on LinkedIn, say, could equate to a complete client list, visible by competitors); and through the inadvertent disclosure of “competitive intelligence” while discussing products, customers, and strategic decisions on various social networking sites. (Some businesses actively gather information about their competitors through social media sites, and analyze that information to gain a competitive advantage. If trade secrets or other proprietary information has been inadvertently revealed in this way, legal headaches could ensue.)

Operational

When employees access social media platforms at work – even those employees who are designated as social media spokespersons for the organization – they risk endangering the organization’s networked computers by unknowingly acquiring malware, viruses, and spyware. Social networking sites, particularly Facebook and Twitter, are a favorite playground for those with bad intentions. Fraudsters coax unsuspecting users into downloading a free application that covertly delivers spyware, which then infiltrates the company’s entire system of computers. These and “social engineering” scams – in which fraudsters manipulate people into divulging information that either leads to more valuable information, or provides access to a company’s computers for hacking purposes – are common on social networking sites. A related concern, and one that additionally belongs in legal social media risks, occurs when a company’s website and social media pages are spoofed by fraudsters. Visitors are tricked into downloading malware or divulging information, as a result, thinking they are dealing with the actual company. As mentioned above in the legal risk section, some may allege in a lawsuit that a company’s failure to monitor for malware, social engineering scams, and spoofed sites in the social media realm – and the company’s failure to inform visitors as these are discovered – is evidence of potential negligence, breach of contract, or statutory violations.
According to the anti-virus software company, McAfee, “More than six out of 10 organizations have already suffered losses averaging $2 million, for a collective loss of more than $1.1 billion in security related incidents last year [2009].” As a result, in McAfee’s survey of more than 1,000 global business decision-makers in seventeen countries, half of those surveyed “were concerned about the security of Web 2.0 applications such as social media, micro blogging [like Twitter], collaborative platforms, web mail, and content sharing tools.”

Finally, when non-executive (non-exempt) employees communicate during off-hours about work-related issues with supervisors – either through email or social networking sites – that activity can open a company to the so-called “wage and hour” disputes that have recently grown more common. Because non-exempt employees are paid to work certain hours, and their “virtual” work time is not counted nor compensated, it remains unsettled as to whether and how they should be compensated for that additional work.

Five Basic Steps for Addressing Your Company’s Social Media Risks:

1. Conduct a broad assessment of its general social media activities, looking for potential risks. Beyond that general assessment, whenever a social media campaign is contemplated, the organization needs to assess the particular risks of that campaign. Not only should the organization’s contemplated campaign align with the culture of the organization and its current marketing strategy, but the risks should be weighed against the benefits – with both being articulated as clearly as possible.

2. Identify the key players who will be responsible for developing, executing, and monitoring its social media strategy. An active strategy will require a great deal of time and resources – so it’s important to decide which departments will foot the bill for staffing, technology, and other expenses. Also, identify a senior executive or employee with the political wherewithal that can make decisions very quickly and make time-sensitive decisions as necessary.

3. Draft a simple but comprehensive social media policy or set of guidelines tuned to the company, its customers, and its industry (even if a company decides to grant “official” social media access solely to designated spokespersons, separate guidelines are still needed for employees using social media when they’re not at work.) This social media policy should be reviewed by the organization’s human resources, legal, information technology, and communications departments. Also recommended is a review by an independent law firm.

4. Formally address the risks of social media participation with company employees. Since employees actually pose the biggest risk to a company – albeit, usually without meaning to – it is essential to provide regular educational training programs regarding the dangers of damaging the company (reputationally, legally, or operationally) by using social media on the job, or on their own time.

5. Create a social media agreement that employees review and sign annually (as a condition of continued employment, and as part of their employment contract). Such an agreement should be updated annually – or more often, as warranted – to address changes in social media that may impact business in new ways.

Regardless of whether an organization decides to implement an active social media strategy – or not – it must clearly outline how employees are allowed to access social media sites (if they are allowed) and under what guidelines.

Social Media: The Business Benefits May Be Enormous, But Can the Risks – Reputational, Legal, Operational – Be Mitigated?

PART IV: How Can Organizations Mitigate the Social Media Risks They Inevitably Face?

Odd though it may seem, companies that don’t actively participate in social media – to promote their business and build brand awareness – still need to address the reputational, legal, and operational risks that social media can pose. Why? It’s extremely likely that their employees are using social media tools, either at home or during business hours at work, regardless of whether it’s employee- or company-owned equipment. In doing so, such employees may unwittingly put their employer at risk. Even non-participating companies as a result, need to be proactive in creating social media guidelines or policies for their employees.
Here are a few approaches companies have taken:

1.) **No Employee Has Access at Work:** When the company policy is that no employee will have access at work, it is important that training, guidelines, and agreements educate employees about the reason for the no-access policy, while at the same time outlining the company’s at-home social media use concerns, and what is required of employees as a result.

2.) **Designated Individuals Have Access for Work:** When designated individuals within the company have been granted social media access for work – usually for formally approved functions and under specific business guidelines – more formal education should be provided (similar to training for employees expected to act as media spokespersons for the company). This may also require that all content posted on behalf of the company be cleared through the organization’s legal and communications departments.

3.) **Employees Only Have Access to Specific Sites:** When employees are allowed to access LinkedIn, for instance, in order to further the company’s business aims, but are prohibited from accessing other sites – like Facebook and Twitter – social media education and training are crucial. Employees also need to know what they can and cannot do on the allowed site, as well as what the penalties are for migrating to prohibited sites.

4.) **All Employees Have Total Access at Work:** When all employees have total at-work social media access, the same issues need to be clarified and employees need to know when and how long they will be permitted to use social media at work. They need to be instructed on the comments and content they provide as a representative of their employer. They also need to know that their compliance with the company’s written social media policy will be monitored and enforced. Formal education and regular confirmation and acknowledgment of the social media policy is critical to success in this regard.

Here are a few areas that social media education for employees as well as managers should address, in order to mitigate reputational, legal, and operational risks:

- When employees post on their personal blogs, or elsewhere online, they must provide a suitable disclaimer that their opinion on a particular subject does not reflect the views of their employer.
- When communicating a positive opinion about the company or its products, employees must disclose that they are employees; if they post anonymously, the FTC could launch an investigation against the company, generally in response to a complaint.
- When responding to questions and comments about the company or its products on social media platforms, employees must not post in a way that would lead others to reasonably believe they are doing so on behalf of the company (unless as a designated spokesperson – in which case all content should be cleared by the company’s legal department).
- Employees should assume that anything they post online is public information, even if their profile page is only open to their Facebook “friends.” In any case, they should refrain from posting anything online that is derogatory about the company, its products, clients, co-workers, or managers. In the same vein, they would be wise to refrain from the use of profanity, posting compromising photographs, and so forth. (Unfortunately, others may post compromising pictures of them without their knowledge, so it is wise to avoid allowing such photographs to be taken, or to request removal when they are.)
- Employees should be particularly careful about sharing company information through social media; the wise choice is to simply not do it. Even if the information is not a trade secret, it’s best to avoid sharing even trivial facts that are not otherwise expressly and publicly available, unless that employee is the designated social media spokesperson (who has detailed guidelines pertaining to that job and will have reviewed such content with the legal department).
- Employees should be equally careful about protecting the information and privacy of the company’s clients and customers (as well as its co-workers and managers).
- When using social media, employees should carefully avoid a violation of the laws pertaining to human rights (including harassment), defamation, copyright or other intellectual property rights, securities, financial disclosure, and privacy rights.
In a more “open and transparent” world, people will be held to the consequences of their actions and be more likely to behave responsibly.27

PART V: Guidelines for Companies Wishing to Avoid Legal Action

Apart from offering social media guidelines for employees, companies should also follow certain practices to ensure their corporate safety online:28

Engage the Proper Legal Team Early in the Process:
In developing a social media strategy, companies should involve lawyers who understand information technology law, since they can help prevent all the legal pitfalls described above. If lawyers are included early in the planning stage, processes and policies can be developed that are effective for business, while at the same time reflecting the level of risk that the organization is comfortable with. If, however, lawyers are consulted after social media plans have been completed, they may either need to be scrapped or extensively redesigned.

Identify the Laws and Legal Risks That May Apply:
Communication and understanding is crucial to developing a social media strategy that will not pose undue risk to the organization. Lawyers need key information about the organization’s social media activities, including the social media platforms that will be leveraged, the kinds of activities contemplated, the type of information that will be collected, used, and published, and the individuals who will participate on each social media site. With this information, the legal team should determine what legal risks may exist, including applicable regulations, contractual obligations, and common law risks. This analysis will help the organization understand its risk, so it can perform an appropriate cost-benefit analysis concerning its social media activities, and then design mechanisms to mitigate that risk to an acceptable level.

Comply with Third-Party Sites’ Guidelines:
Carefully review the terms of service and the privacy policies for each social media site you have a presence on, and be sure you are in compliance with those social media outlets.

Site Monitoring:
Social media sites may attract postings that infringe upon your company’s intellectual property rights, are defamatory, are damaging to your or another company’s reputation, or contain confidential or proprietary information. It’s important, therefore, to actively monitor social media sites for offensive or infringing posts (via an employee assigned to this task, or through an outside firm).

Create a Response Team: Handling damaging statements or content may require a team of people drawn from senior management, legal, corporate communications/public relations, marketing, and human resources. Appropriate action by the response team will depend upon the actual incident and its severity. But it could include: requesting that a post on a third-party site be removed; removing an offensive post on the company’s own site; replying to misleading posts with the correct information; responding via other social media outlets; responding with a press release; taking legal action; or any combination of the above actions.
PART VI: Making Social Media Work for Your Company

The business benefits of social media participation can be substantial, while the cost of non-participation, or opting out, may mean anything from losing business to losing touch with your customers and important trends in your industry. Of course, as we’ve outlined in this paper, there is also much to lose if your company does not respond proactively to the many risks posed by social media.

To conclude, ensuring your company’s social media safety is a matter of taking the following steps:

- Analyze your company’s unique social media safety needs, create detailed social media guidelines, and educate your employees about safeguarding your company when using social networking sites at work and at home.
- Monitor the social media landscape, including your company’s own sites as well as its third-party pages, for content that is negative, damaging, or that potentially infringes on intellectual property rights – whether your own, or that of your competitors.
- Be sure that you have adequate insurance coverage for your company’s social media activities, and review the coverage parameters and amounts regularly. (Commercial general liability may not cover online content, and your company will need coverage not only for your own website, but for content you’ve placed anywhere on the Internet.)

Once you’ve taken these steps to mitigate the considerable reputational, legal, and operational risks, your company will be in the best possible position to reap the enormous business benefits of social media participation.

A Glossary of Social Media Terms:

- **Crowdsourcing**: Wikipedia, the online encyclopedia (http://www.Wikipedia.org), defines crowdsourcing as “the act of outsourcing tasks, traditionally performed by an employee or contractor, to an undefined, large group of people or community (a ‘crowd’), through an open call.”
- **Microblogging**: The traditional blog (or “web log” journal) features posts by its owner/author that are typically between 400 and 1000 words long, while the typical microblog entry or posting is much shorter – often less than 20 words. The most frequented microblog platforms are Twitter and Facebook’s status updates feature, but there are more than 111 such sites worldwide, according to Wikipedia.
- **Social Bookmarking**: Social bookmarking sites (for example, Delicious, Digg, and Stumbleupon) allow Internet users to store, organize, and share links to web pages that are useful to them. These pages may relate to any number of user interests and are public – so those who share the same interests can find these bookmarked sites as well.
- **Social Engineering**: Social engineering involves online manipulation in order to “con” unsuspecting people into revealing valuable information, or into performing an act that will allow fraudsters access to either computers or information. There are many types of social engineering scams, including phishing, pretexting, diversion theft, and baiting.
- **Spoofed**: This word refers to a victim of “spoofing” as someone who’s been “spoofed,” or has fallen for the online scam of responding to a fake website as if it were the legitimate site it resembles. The spoof site is used to extract valuable information from visitors, such as passwords and user IDs. There are other forms of spoofing as well.
- **Spyware**: This is a type of covertly installed software (a form of malware) that typically infects home computers without the owner’s knowledge, in order to surreptitiously gather information – such as browsing habits. Spyware may also be used to change certain computer settings without the permission of the owner.
- **Tweet**: A short, 140-character message delivered on the microblogging platform, Twitter, by those who have set up a free account on the site.
- **Twitter**: The most famous microblogging site on the Internet, where people can tweet about the things that interest them, as well as retweet – or tweet again – the tweets of others. See: http://www.Twitter.com
- **Wiki**: This Hawaiian word for “fast” has come to mean a collaborative website that enables the creation of content by any number of interested people in an open environment. Examples are: Wikipedia, company intranets, and community sites.
Social Media: The Business Benefits May Be Enormous, But Can the Risks – Reputational, Legal, Operational – Be Mitigated?

About the Authors:

Toby Merrill is Vice President of ACE Professional Risk, where he serves as the national product manager of ACE’s network security, privacy, technology and media liability products. With more than 14 years of insurance experience, he has worked with a number of Fortune 500 companies in reviewing crisis management plans, as well as seeing how well they actually work following a serious data breach. Prior to his tenure with ACE, Mr. Merrill was a Regional Professional Liability Specialist with Chubb Specialty Insurance. He began his career in the Information Technology department at Cozen & O’Connor in Philadelphia. Mr. Merrill has authored numerous articles on network risk management, and frequently serves as a speaker at industry trade conferences on cyber risk and network security topics. He is a graduate of Franklin & Marshall College in Lancaster, Pa., where he received a Bachelor of Arts degree in Business Administration.

Kenneth Latham is Vice President of ACE Professional Risk, and product manager for Employment Liability and Fiduciary Insurance. He is responsible for the underwriting and loss prevention activities within the group and has more than 15 years of management liability insurance experience. Ken is a graduate of Pace University.

Richard Santalesa is Senior Counsel in Information Law Group’s east coast office, based in Fairfield, Connecticut and New York City, where he represents clients on electronic commerce and internet issues, software and content licensing, privacy, data security, outsourcing, website development transactions and other commercial arrangements involving intellectual property and technology-savvy companies. With over 20 years of technology experience, Richard registered his first domain name in 1994 and has authored articles and columns for numerous publications.

David Navetta is a Founding Partner of the Information Law Group. David focuses on technology, privacy, information security and intellectual property law. He is also a Certified Information Privacy Professional through the International Association of Privacy Professionals. David has enjoyed a wide variety of legal experiences, including work at a large international law firm, in-house experience at a multinational financial institution, and an entrepreneurial endeavor running his own law firm. David currently serves as a Co-Chair of the American Bar Association’s Information Security Committee, and is Co-Chair of the PCI Legal Risk and Liability Working Group.

The ACE Group is a global leader in insurance and reinsurance, serving a diverse group of clients. Headed by ACE Limited, a component of the S&P 500 stock index, the ACE Group conducts its business on a worldwide basis with operating subsidiaries in more than 50 countries. Additional information can be found at www.acegroup.com.

The opinions and positions expressed in this paper are the authors’ own and not necessarily of any ACE company or Information Law Group. References to insurance policy contracts are general in nature. Insurance contracts have specific terms, conditions, and limitations that govern the rights and obligations of the parties and the scope of coverage in each case.

© 2011 ACE Limited. All rights reserved. All trademarks and/or servicemarks contained herein are the property of their respective owners.
Social Media: The Business Benefits May Be Enormous, But Can the Risks – Reputational, Legal, Operational – Be Mitigated?

ENDNOTES:

2 http://www.census.gov/population/www/popestclockus.html
3 http://socialtimes.com/200-million-twitter-accounts-but-how-many-are-active-b36952
10 “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,” Practical Law Publishing, PracticalLaw.com, February, 2010, page 38-39. (Additional strategies that companies have employed include: (1) Group pages where social media users gather to discuss particular topics, products, services, and companies. Many organizations actively participate in these forums in order to influence issues important to them; (2) Social Plug-ins: These buttons allow for the instant republication of company content across multiple social media networks. The hope is that the company’s content and message goes “viral” and is viewed by millions; (3) Applications and Login-Connect Interfaces: Some companies create specific applications that can be used on computers and mobile devices. These applications may provide users with access to products and services, as well as provide valuable consumer information to the organization. Login-connection applications allow users to use their login credentials from sites like Facebook to authenticate themselves on the organization’s website. In the process, the organization gains access to the users’ social media information.)
15 “Common Sense Is a Rule When Using Social Media,” The Allentown Morning Call, October 30, 2010.
16 http://www.ncsl.org/?tabid=19825
22 http://www.socialmediaawupdate.com/tags/advertising-law/
23 Facebook Promotion Guidelines are available at: http://www.facebook.com/?ref=home#!/promotions_guidelines.php
24 Facebook Promotion Guidelines are available at: http://www.facebook.com/?ref=home#!/promotions_guidelines.php