March 2010

Online Social Networking: A Brave New World of Liability

An Advisen Special Report

Executive summary

Millions of people across the world now participate on social network websites such as Facebook, LinkedIn and Twitter. Businesses have discovered that social network sites offer new channels to reach customers and prospects, and can be sources of valuable information for evaluating job candidates. But social network sites also can be liability minefields, exposing companies to risks as diverse as copyright infringement, consumer fraud and discrimination. Employers also can be held liable for the unsupervised activities of their employees on social network sites. Risk management practices can help reduce exposures, and various forms of specialized insurance coverage are available.

Introduction

Social network website Facebook now claims more than 350 million active users worldwide, more than the population of the United States. Social network sites in total have now equaled e-mail in terms of usage by computer owners, according to a Nielsen survey. With the explosive growth of social networking comes uncharted liability landscapes for both individuals and businesses. Already, words and phrases like “cyberbullying” and “textual harassment” are creeping into the English vocabulary.

Businesses are recognizing that social network sites present new channels to promote products and services, and venues to cultivate communities of prospects and customers. Many also have discovered they are windows into the personal lives of employees and job candidates. Of growing concern to risk managers and human resource officers is the increasingly blurry line between work activities and personal activities as employees bring their work, their office relationships and their job-related grievances online.

Owners and operators of social network websites are faced with wide-ranging liability concerns including copyright and trademark infringement, privacy and data security issues, and the safety of children and other vulnerable people participating on the websites. Businesses that participate on social network websites have potential liabilities ranging from copyright infringement to trade practice violations to claims of harassment and intimidation. Perhaps the

most vexing exposure for companies is employee participation on social network sites, which can cause liability headaches if employees bring work-related issues into the social networking sphere. Conventional loss control and risk management processes are maddeningly ineffective in the unconstrained virtual world of online social networks, making innovative new strategies essential for keeping a lid on potential liabilities. Additionally, risk managers need to be certain that their insurance programs are fully aligned with the threats posed by the social networking activities of both their companies and the companies' employees.

The online social networking phenomenon

Facebook, MySpace, LinkedIn, Twitter and YouTube now are household names, but they are only a few of the hundreds of social network sites currently operating. Some appeal to diverse audiences, while others target specific groups based on language, nationality or shared racial, sexual or religious identities. What most sites have in common is a system to allow each member to construct a public or semi-public profile of personal information, to create a list of other members with whom they share a connection, and to navigate their list of connections and the connections of others. Members often can post messages, photographs, music or videos to be shared with others either publically or exclusively within their network of contacts.

LinkedIn and MySpace are two of the early social network site success stories. LinkedIn, a business-oriented site used principally for professional networking, has about 50 million users worldwide. MySpace, now owned by Fox Interactive Media, which in turn is owned by Rupert Murdoch's News Corporation, was the largest social network site before being left in the dust by the runaway success of Facebook. Myspace passed 100 million users in 2006, and presently boasts about 125 million active users worldwide. According to web information company Alexa, MySpace.com is the 13th most visited website in the world.

With 350 million users worldwide, Facebook is the 800 pound gorilla of social network sites. Alexa ranks Facebook.com as the second most visited website in the world, trailing only Google. The website initially was launched by Harvard sophomore Mark Zuckerberg for the use of Harvard University students, but soon expanded its user base to encompass any university or high school student before opening its doors to all comers over 13 years old. While 18-25 year olds comprise the largest demographic segment of Facebook users, the site's phenomenal growth has been fueled by users over 35, with women over 55 the fastest growing segment.

Liability issues of social network websites

Social network sites are magnets for copyright violation lawsuits. Millions of users post copyright-protected material lifted from other websites or uploaded from compact discs and

DVDs. The Universal Music Group (UMG) filed a copyright infringement suit against MySpace for allowing users to upload and download songs and music videos. UMG sought damages of $150,000 per song or video posted, claiming that millions of songs and videos on MySpace pages may infringe its copyrights. Media company Viacom filed a copyright infringement suit against YouTube and its parent Google, seeking at least $1 billion in damages. Viacom charged that "YouTube has harnessed technology to willfully infringe copyrights on a huge scale."

Social network sites may be frequently targeted in copyright infringement suits, but they also enjoy certain protections from liability in the US under the Digital Millennium Copyright Act (DMCA). Section 512(c) of the DMCA creates a "safe harbor" against copyright infringement liability for content posted by website users. In order to qualify for protection, mechanisms must in place so that a copyright owner can request the removal of infringing content. The site also must not receive a financial benefit directly attributable to the infringing activity.

Social network sites also enjoy certain immunities from liability for statements posted by users under the Communications Decency Act (CDA). Section 230 of the CDA immunizes websites from liability resulting from the publication of information provided by others. While this typically arises in the context of defamation, some courts have expanded CDA protection to cover other sorts of claims as well. Protections under the DMCA and the CDA, however, have limitations, and social network websites are exposed to a host of other liability exposures not addressed by these acts.

Some social network sites have come under fire over privacy issues. A class action lawsuit filed against social network site Tagged alleges Tagged misappropriated member information by using members' email address books without permission to solicit new members. Facebook paid $9.5 million last year to settle a lawsuit claiming the company's Beacon program, which broadcast members' transactions on affiliated websites on their Facebook pages, violated members' privacy. A recent California lawsuit alleges that Facebook violates state privacy, publicity and consumer protection laws by sharing members' personal information with advertisers and others for commercial purposes. The plaintiffs argue that Facebook misleads users into thinking it provides a secure environment for sharing personal information with friends.

Social network sites also have data security exposures that could trigger lawsuits. In December, for example, an Indiana man filed a lawsuit against RockYou, a provider of social networking applications, alleging that the company failed to secure its network and protect customer data, enabling a hacker to grab passwords of 32 million users. Cybercriminals stalk the social networking landscape, taking advantage of the sense of trust that characterizes exchanges on social network sites. By posing as legitimate users, they entice other users to open messages or launch applications that unleash various types of malware designed to capture sensitive information or give hackers access to – and even control over – victims' computers. Security experts warn that attacks on social network sites and their users have

been increasing in both number and sophistication. Social network sites that fail to take strong steps to protect users are more likely to be targeted in lawsuits.

Protection of children has been a hot button issue for social network sites. According to the US Federal Trade Commission, MySpace and Facebook rank in the top 10 most popular websites for children between 12 and 17. The Federal Trade Commission (FTC) has investigated several social network websites to determine if those sites are in compliance with the Children's Online Privacy Protection Act (COPPA). The New York Attorney General's office stated in 2007 that investigators posing as 12 to 14 year old users of the Facebook were "repeatedly solicited by adult sexual predators." The attorney general's office claimed that Facebook was slow or unresponsive in addressing many of the complaints that were lodged as investigators posed as both minors and parents of minors, and threatened a consumer fraud charge for misrepresenting how safe the site is for minors.

Potential liabilities of other companies arising from online social networking

Businesses have discovered that social network sites are an effective way to reach new customers and to build customer loyalty. Social network sites offer the possibility of not only delivering marketing messages, but also of establishing more direct and personal relationships with individual customers. In the case of Facebook, a member can become a "fan" of a business with a Facebook page. Facebook friends of that member are notified when the member becomes a fan, creating a form of viral marketing complete with an implicit endorsement by the member fan. Businesses can direct messages to their fans, which appear on the fans' "walls" to be read not only by the fans, but also by the fans' friends

Businesses with pages on social network sites have all the potential liabilities of publishers, including copyright infringement, trademark infringement and defamation. Because of the comparatively informal and frequent nature of social networking interactions between businesses and their "fans," the opportunities for stumbling into trouble multiply. The brave new world of doing business on social network sites also can create heighted exposure to claims of consumer fraud and deceptive business practices. The FTC recently stepped up its monitoring of social network sites.

Companies need not maintain pages on social network sites to reap benefits from social networking. Advertisers on some social network sites can take immediate advantage of personal information for millions of potential customers stored in profiles as well as other content on members' pages. Users may disclose age, sex, marital status, where they live, their political and religious affiliations, the movies and music they prefer, and much more. Despite relentless criticism and a few lawsuits, some social network sites use that information to drive targeted advertising to members. To date, the small handful of lawsuits challenging this type of commercial use of personal information have been directed towards the social network sites

themselves, but new theories of liability may someday drag advertisers into this litigation as well.

Companies mine data on social network sites for an array of business purposes. For example, social media monitoring firms such as Trendrr, Trackur, and Sentiment Metrics use algorithms to analyze data disclosed by consumers on social network sites and elsewhere on the Internet to spot trends concerning client companies' brands and reputation. Social media monitoring software also is used by companies to almost instantaneously spot complaints about a product in, for example, a Twitter "tweet," which may trigger an unsolicited and startlingly unexpected response from a customer service representative. One data-mining firm, Rapleaf, claims it can help predict which ads people will pay attention to and whether or not a person is a worthwhile risk for a credit card or a loan by analyzing social networking friends lists. Banks and credit card companies reportedly are evaluating social media data mining tools to aid in credit decisions, thrusting social networking sites and the personal data they contain into the politically sensitive realm of consumer credit.

One well-informed analyst described the future of mining personal data from the Internet as "frighteningly intrusive and scary." Liability issues undoubtedly will emerge as privacy laws catch up with rapidly changing technology and social trends. Privacy advocates and some government agencies have expressed concern about the use of personal information, even if publically accessible. Last year, FTC Commissioner Jon Leibowitz made it clear that regulation may be necessary to protect private information if self-regulation fails. In November, the US Judiciary Committee approved two bills, the Personal Data Privacy and Security Act and the Data Breach Notification Act, which, while not specifically addressing data from social network sites, broaden consumers' privacy rights as concerns information collected and distributed by "commercial data brokers."

A survey of about 350 employers in October 2007 by Vault.com, a media company focused on careers, found that 44 percent of employers use social network sites to examine the profiles of job candidates. Undoubtedly the percentage is higher yet today. Researching job candidates on social network sites is legal, but employers who use the information to make hiring decisions may open themselves to charges of employment discrimination, especially if a candidate's profile reveals sexual orientation, religious or political affiliation, or a disability. On the other hand, some legal experts suggest that an employer who does not search social networks for readily available information may be negligent in their hiring practices.

From a practical standpoint, privacy concerns may subside somewhat in the coming years. The volume of data available for mining and analysis is likely to dwindle as social network sites provide members with controls to limit the amount of personal information that is publically accessible. Facebook, for example, recently introduced new controls that allow users to hide almost all personal information, including friends lists.

Employers' liability for employees' activities on social networking sites

Businesses increasingly forbid access to social network sites from office computers. In addition to concerns about employees tweeting the day away, many firms block access to minimize liability exposures. Hospital personnel, for example, could carelessly violate HIPAA privacy provisions with offhanded remarks about how they are spending their day at work. Law firm employees could inadvertently breach attorney/client confidentiality or disclose the strategy in an active case. Statements about co-workers, vendors and customers could lead to lawsuits alleging defamation, trademark tarnishment or unfair trade practices.

With the proliferation of Internet-enabled "smart" phones, controlling access to the Internet during work hours is becoming increasingly impossible. Additionally, while companies may attempt to limit access to social network sites at work, they have little control over employees' social networking activities away from the workplace. Even during off hours, the activities of an employee can create liability headaches for the employer if the employee is perceived as acting as a representative of the company. This most obviously occurs when an employee airs explicitly job-related issues on a social network site, but it also happens in far more subtle ways. A member of a social network site that merely lists an employer in his or her profile, for example, may create trouble for the employer by criticizing a customer, a vendor or even a competing company's products.

Employers can be held liable for the activities of employees under the common law doctrine of agency – *respondeat superior*. This doctrine states that the superior (or "principal") is held responsible for the acts of its subordinate (or "agent"). A company (the "principal" in this case) can be held liable for the actions of its employees and others deemed agents of the company, even if the agents are acting independently. This is called "vicarious liability."

Employers also can be held liable for an employee's activities on a social network site under claims of negligent training and negligent supervision, especially if the offending activities take place at work. In one Wisconsin case, a manager of a security company copied identification card photos of female employees of a client firm while at work, defaced them in an offensive manner, and published them on several sites. Ten of the women brought suit against the security firm, which was found liable for negligent training and supervision of the manager.

Employee-related liability issues become even more angina-inducing as more people wander about the workplace with cameras and camcorders in their cell phones, and websites such as YouTube provide a very public forum for their handiwork. Domino's Pizza faced a near-disaster last year when two employees filmed a video for YouTube in which an employee stuffed cheese up his nose and then placed the cheese in a sandwich. An employee filming on the job may open a company up to liability for defamation suits or for violation of various privacy laws. Millions of YouTube viewers, for example, have watched a video shot by an airport employee of an irate customer flailing and screaming after missing her flight.

Employers are understandably concerned about employees making unfavorable comments about the employer, as well as its products or services, but employees who use social media to favorably comment on their employers' products or services also subject their employers to potential liability. The FTC recently issued updated guidelines aimed at protecting consumers from misleading endorsements and advertising. The revised Guides Concerning the Use of Endorsements and Testimonials in Advertising suggest that employees endorsing an employer's products or services have a duty to disclose to their audience their relationship to the employer. If employees make misleading statements that result in injury to consumers, the FTC may bring an enforcement action against the employer. Additionally, employers may be vulnerable to class-action lawsuits by consumers and legal action by state attorneys general.

Social network sites create difficult to control harassment, discrimination and retaliation exposures. Employers are only now coming to grips with "textual harassment," where harassment and bullying takes place through inappropriate text messages, emails or internet postings, which the employer usually is not aware of and has little control over. Even if the harassment takes place outside of work in a social networking context, employers can be held liable, especially if the employer becomes aware of the activity and takes inadequate steps to stop it.

A vexing issue for employers is how to respond to inappropriate content on an employee's personal page on a social network site. If the employee attacks or makes inappropriate comments about another employee, the employer's response is clear. Similarly, if an employee makes strongly negative statements about his or her employer, a customer or a business partner in a public forum, the employer probably is safe taking action. Beyond those scenarios, the situation becomes murky. Several laws may restrict an employer's ability to take adverse action based upon an employee's off-duty social networking activities. These laws include the National Labor Relations Act, state laws that prohibit adverse action based on an employee's lawful off-duty activities, and anti-discrimination laws. Also, comments by an employee that constitute whistle-blowing may be protected.

Risk management and insurance

The sprawling and ever-expanding nature of social networking liability exposures demand separate but coordinated risk management programs on a number of different fronts. Companies should have programs in place to minimize their exposure to claims for their own activities on social networking sites, such as copyright and trademark infringement. In addition, companies need a social networking policy that governs not only employee access to and conduct on social networking sites while at work, but also outside the workplace. A social networking policy should:

- Address all publicly accessible communications made via the Internet. This includes not only postings on social network sites, but also communications made on blogs, discussion forums, newsgroups and e-mail distribution lists.

- Define the company's overall attitude toward social networking. Senior managers of some companies see social networking strictly as a threat, or at least as a distraction. At the other end of the spectrum, some companies have integrated aspects of social networking into their business models.

- Clearly state the company's policy concerning access to certain social network sites while at work. This policy is likely to vary according to a company's business model and marketing strategy, as well as by employee roles. Some employers, for example, encourage the use of professional networking sites such as LinkedIn.

- State whether employees are allowed to identify themselves as representatives of the company on social network sites. As a general rule, it is safest to require employees to not name their employer on profiles, though such a prohibition makes little sense if companies encourage social networking for sales and marketing purposes. If employees are allowed to advertise their association with the company, the policy should impress upon them that they have the responsibility to represent the company in a professional manner.

- Make it clear that employees are not to reference any clients, customers or business partners without express permission to do so.

- Prohibit postings that contain defamatory remarks about the company and its policies, business, and management; defamatory, harassing or discriminatory content directed towards co-workers; or proprietary information.

- Require personal blogs to have clear disclaimers that the views expressed by the author in the blog are the author's alone and do not represent the views of the company.

- Prohibit the use of company logos and trademarks without written consent.

Given the evolving nature of online social networking, insuring these risks is a difficult, complicated task requiring careful evaluation of the coverage needed to respond to their unique liability exposures. Many social networking companies may best be insured on a media policy. These policies can be written on a named perils or "open" perils basis (look for the wording in the forms "including but not limited to"), the later preferable as new causes of action may develop during the policy period from innovative attorneys. These media policies should include a broad definition of intellectual property, the most common risk for social media networks as well as broad media coverage including such perils as product disparagement, trade libel, emotional distress or outrage, misappropriation of ideas under contract, invasion of

privacy or publicity, harassment or stalking to name a few. If a firm is involved in providing professional services, such as software development, internet search services, application services, electronic mail, web hosting, marketing, licensing or other business services, these should be scheduled onto the policy with a professional services endorsement or a technology policy with a very broad media services endorsement could be purchased as an alternative to a media policy.

Additional coverage may be needed to address potential exposures, these may include but not limited to:

- Contingent bodily injury and property damage
- Dissemination of a malicious code
- Contextual errors and omissions
- Deceptive trade practices or unfair competition (if alleged with an otherwise covered claim and conduct approved by counsel)
- Privacy/Network Security
- Violation of criminal statues if the underlying act approved by counsel
- Breach of confidentiality arising out of a claim alleging failure to maintain confidentiality of a source
- Subpoena Defense coverage for an insured to object to a subpoena to produce information
- Defense coverage for injunctions
- Breach of indemnification or hold harmless agreements
- Defense for regulatory actions
- Negligent supervision of an employee
- Coverage for independent contractors who provide media material
- Worldwide coverage territory
- Advertising coverage, not only of the insured but on behalf of third parties
- Difference in conditions endorsement to incorporate broader coverage ontained in a predecessor policy
- Defense outside the limits

Online social networking is a phenomenon that lies at the intersection of technology and culture. The enormous number of people sharing personal information on social network websites, the sense of trust that is essential of social networks, the ease with which digitized data can be captured and analyzed, the profit motives of legitimate businesses and the predatory activities of cybercriminals collide in the world of online social networking with a still-evolving legal and regulatory framework providing an often-inadequate guide for lawful conduct. Many companies recognize the business opportunities inherent in social networking, but most companies are only now beginning to wake up to their potential liabilities. These liabilities exist even if a company has no direct involvement in social networking, and often arise in the difficult to control realm of employee activities outside the workplace. Consequently, companies need a well-conceived and well-executed risk management program to minimize exposures, and should have appropriate insurance coverages in place to avoid financial calamity.

If you have any questions about social networking risk management or insurance, you can ask the experts at Swett & Crawford at http://corner.advisen.com/swett_feedback_social.html.

For more information about cyberliability insurance products, visit the Swett & Crawford Professional Services Group website at http://www.swett.com/main.php?page=PracticeGroupView&practiceGroupId=2.

.

This Advisen Special Report was written by David Bradford, Executive Vice President, dbradford@advisen.com. Thanks to Jason White and Mark Smith of Swett &Crawford for their input.

About Swett & Crawford

Swett & Crawford, headquartered in Atlanta, Georgia, is owned by its employees and two private equity firms, HM Capital Partners and Banc of America Capital Investors.

In its national network of offices, Swett & Crawford serves independent agents and brokers through specialized Property, Casualty, Oil & Gas/Energy, Professional Services, Transportation and Underwriting Practice Groups. These groups provide access to commercial insurance products and programs, including property and casualty coverages, products liability, directors & officers and professional liability including cyber/privacy/security, commercial and public auto liability as well as a host of customized binding authorities and exclusive programs tailored to specific industries, businesses and professionals.

About Advisen

Advisen integrates business information and market data for the commercial insurance industry and maintains critical risk analytics and time-saving workflow tools for over 530 industry leading

firms. Through its work for the broadest customer base among information service providers, Advisen delivers actionable information and risk models at a fraction of the cost to have them built internally. Designed and evolved by risk and insurance experts, and used daily by more than 100,000 professionals, Advisen combines the industry's deepest data sets with proprietary analytics and offers insight into risk and insurance that is not available on any other system. Advisen is headquartered in New York. For more information, visit http://www.advisen.com or call +1.212.897.4800 in New York or +44(0)20.7929.5929 in London.