

New York Law Journal

GC New York

WWW.NYLJ.COM

©2009 ALM An **ALM** Publication

VOLUME 242—NO. 112

THURSDAY, DECEMBER 10, 2009

FRAUD PREVENTION

Social Networking Changes Approach to Investigations

The increase in the public's use of social networking services, such as MySpace, Facebook, Twitter and LinkedIn significantly impacts general counsel's approach to litigation, investigations, and fraud prevention by providing a new avenue to search for potentially relevant information and evidence.

Social networking can be likened to Webmail on steroids. Social networking allows groups to connect; send and receive communications, pictures and videos; play games; and enjoy other forms of entertainment. Many individuals rely solely on social networking sites for their personal online communication due to the ability to interact with large groups of people. According to "Global Faces and Networked Places: A Nielson Report on Social Networking's New Global Footprint," "Two-thirds of the world's Internet population visit a social network or blogging site and the sector now accounts for almost 10% of all internet time."¹ The authors note that, globally, three out of every 10 people online visit Facebook.²

Evidence in Litigation

Recently, courts have issued rulings establishing that information obtained from social networking sites is admissible at trial and discoverable in pretrial proceedings. For example, on Jan. 27, 2009, the Michigan Court of Appeals upheld the admission at a murder trial of pictures posted on a defendant's MySpace Web page.³ The prosecutor had used the pictures, in conjunction with trial testimony, to establish the defendant's familiarity with the weapon used in the charged offense. Similarly, in February 2009, the Superior Court of Justice, in Ontario, Canada, ruled that a party's postings on Facebook are documents which, if relevant, may be discoverable under Ontario law in a



By
**Stephanie
Giammarco**



And
**Jeffrey
Leap**

civil proceeding.⁴ The court noted that this would be true even if that party had set his Facebook settings to "private."



These cases are just two examples of a growing trend among courts in both criminal and civil cases to utilize evidence obtained from social networking sites. Social networking sites will become an increasingly fruitful source of evidence in the future.

Use in Investigations

As with litigation, the use of social networking sites as a source of evidence in employee investigations is becoming more prevalent. Social networking has changed individuals' communication styles; as a result, social networking has changed employee investigations. Historically, investigations

were performed through the review of books, records, ledgers, journal entries and interviews. In the past, investigators could obtain phone records but, in most cases, were unable to access and review the actual communications engaged in by the subjects of investigations. E-mails, instant messages and text messages, unlike phone records, are capable of leaving a footprint, permitting investigators to review the content of communications. Thus, when corporations began to integrate e-mail and computer use into their operations, they took steps, such as the creation of computer policy statements or the inclusion of language in employees' log-in screens, that preserved management's ability to monitor an employee's communications. As a result, the review of e-mails and other communications conducted through an employer's electronically stored information has become a standard procedure in employee investigations.

Social networking activities have opened an even larger avenue through which investigators can find potentially relevant information. This may include information regarding the dates and times that certain events occurred, locations that an employee has visited, as well as interests, contacts and employment histories of individuals. This information may prove helpful when conducting interviews of an employee suspected of wrongdoing.

Since the evidence to be obtained from social networking sites does not typically reside on corporate servers, investigators must look for this evidence in live and unallocated—or deleted—areas of an individual's desktop or laptop hard drive. This evidence may not be visible to a typical individual; however, a trained computer forensic practitioner will be able to access this information.

Accessing and understanding this evidence is often challenging because a) it may not be easily identifiable, b) it may need to be recovered, c) it may be stored in a format requiring conversion and analysis before it can be read, and d) it may not maintain conveniently or readily available date and time information. For example, searching an

STEPHANIE GIAMMARCO is the national partner in charge of the computer forensics and e-discovery practice at BDO Consulting, a division of BDO Seidman, in New York. JEFFREY LEAP is a manager in that practice in New York.

individual's name or e-mail address may not provide Facebook-related evidence, as the practitioner may first need to identify the individual's unique Facebook ID number to find Facebook-related evidence.

Retrieving evidence may also involve the manual recovery of data or fragments of data, and evidence may not be easy to read because such communications are often surrounded by hypertext markup language (HTML) code; however, a trained practitioner can understand this code. When dates and times are present, they are often stored in a format that requires conversion. Alternatively, if date and time information related to a social networking Web page is not present, the practitioner may corroborate dates and times by analyzing the metadata of pictures or other evidence that previously resided on social networking Web pages but are now stored in unallocated or temporary space on the individual's computer's hard drive. Failure to identify the need to perform these types of conversions, processes, or analyses can lead the practitioner to reach incorrect conclusions or to overlook relevant information altogether.

In addition to preserving evidence residing on a computer system, forensic practitioners should consider preserving and analyzing social networking evidence on handheld devices as people are more frequently accessing social networking sites on such devices. This is especially true for Twitter, which is accessed almost exclusively via handheld devices.

The handheld-device forensics industry is not currently as sophisticated as the computer forensics industry generally. Handheld-device forensic software displays certain information in a less-than-optimal manner, making it more difficult to identify evidence. Also, less evidence is available due to the typically low storage capacity of most handheld devices. Although it is more challenging to access, the evidence created by handheld-device social networking may prove invaluable to the investigator conducting an employee investigation; dismissing this evidence could be costly in an employee investigation.

Due to its potential value, evidence related to social networking can no longer be ignored in investigations. Thus, in-house counsel may find it prudent to create policies that define how social networking evidence may be preserved and analyzed.

Fraud Prevention

Prior to the advent and success of fraud hotlines, fraud prevention in organizations—often the responsibility of in-house counsel—typically relied upon employee tips, audits and internal controls. Social networking provides organizations with an additional means to prevent fraud by examining the social networking activities of employment candidates before they become employees and by monitoring employees' use of social networking sites. Conversely, social networking can negatively impact corporate fraud prevention efforts indirectly by providing fraudsters with

greater access to a corporation's employees, who may become potential fraud victims.

Many organizations today are taking steps to prevent fraud by reviewing social networking sites as part of the background checks conducted during recruitment in an effort to verify a candidate's employment history and to assess whether the candidate is likely to adhere to the prospective employer's core values. Organizations are corroborating this information against resumes and information obtained during interviews, allowing companies to better understand their employment candidates. Moreover, some companies periodically review social networking activity to obtain ongoing information regarding their employees.

One example of an indirect, negative impact of social networking on fraud prevention is that social networking sites provide greater access to victims, making the prevention of fraud perpetrated against employees more difficult. Fraudsters can use these sites to impersonate someone or to make sales pitches to obtain money for fake products, services

As companies utilize social networking to identify new business opportunities, they should not overlook the potential risks associated with reaching out to individuals via social networking sites and should take steps to mitigate these risks.

or investments. Also, to some extent, social networking sites have changed the integrity of communications, since e-mail spoofers and hackers have taken a greater interest in the sites. E-mail spoofing is a method of posing as an individual by sending an e-mail that is displayed as being from that individual but is really from a spoofer or hacker.

Various cases exist where imposters dupe victims into sending money by posing as an individual with whom the victim has a business relationship or some other type of connection. Social networking sites have provided a platform for fraudsters to bring their scams to the masses.

Social networking sites can increase the risk of viruses when employees use company resources to access social networking sites, since viruses can be spread through applications, games, e-mails and instant messages. Many individuals trust the security of social networking sites and are unaware of these risks; however, many sites do not effectively prevent virus spreading, especially if the individual's account does not have the appropriate privacy settings applied. Organizations and their in-house counsel may find it prudent to be aware of these risks and educate their employees accordingly.

Other Risks

Social networking also creates other risks for in-house counsel. These risks include harassment claims related to a social networking communication, decreased employee productivity, and theft or improper transmission of corporate secrets or confidential information. Companies are taking a variety of approaches to reduce these risks.

One approach is to implement social networking training and policies. Employees who understand the consequences of social networking may be more likely to act responsibly, in light of the fact that this activity may be used in litigation or an employee investigation. Methods of educating employees include new-employee orientation, training, departmental meetings and quarterly newsletters or seasonal reminders.

As mentioned previously, companies are now monitoring social networking activity, which can help mitigate risk. Some companies are restricting access to social networking sites on company equipment or during business hours. Such restrictions can help to identify and reduce lack of productivity and other risks, but they typically do not prevent employees from using social networking sites outside of the office or on a handheld device. As companies utilize social networking to identify new business opportunities, they should not overlook the potential risks associated with reaching out to individuals via social networking sites and should take steps to mitigate these risks.

Conclusion

For in-house counsel, the escalating use of social networking sites brings forth both benefits and detriments. On one hand, social networks serve as a source of information which can be used to enhance a position in litigation, develop evidence in an investigation, and reduce instances of fraud. The use of these sites by a company's employees can create significant risks by providing fraudsters new avenues through which frauds can be perpetrated, reduce employee productivity, and place a company's proprietary information at risk. In-house counsel face significant challenges in balancing the benefits of these sites with the risks they present.

.....●●.....

1. Nielsen Company, "Global Faces and Networked Places: A Nielsen Report on Social Networking's New Global Footprint" (March 2009), 1. http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen_globalfaces_mar09.pdf.

2. *Ibid.*, 8.

3. *The People of the State of Michigan v. Liceaga* (No. 280726 Ottawa Circuit Court LC No. 07-031053-FC).

4. *Leduc v. Roman* (06-CV-3054666PD3).