Tattletale: Social Media Can Reveal More than You Think

By Lisa A. Myers, CPA, CFE, CGMA

Social media has altered the way employers find new employees. Selecting job candidates based on mailed-in résumés is as outdated as the typewriter. But the Internet not only facilitates finding qualified candidates, it can also be a valuable tool in investigating or monitoring prospective and existing employees. Both employers and employees should understand how social media can reveal insight into an individual's life that may affect employment. The ever-growing number of social media platforms can help identify compromising or inappropriate employee behaviors, networks, and fraud. These platforms, in short, furnish clues to a person's suitability for a job. Regrettably, the majority of social media users are unaware of the ramifications of inappropriate "private" posts, images, and videos. Their postings can affect not only their reputation, but also their employer's. They may even inadvertently compromise sensitive company or client information. Typically, employers will search for information about a prospective new hire that focuses on rooting out lies about a candidate's work history, education, certifications, and more. Other employers may monitor social media for private activities they disapprove of, including employee criticisms directed at individuals or the company. They may then proactively inform or reprimand the employees involved. Considering the easy access and permanent nature of posts, social media policies are a must for all companies. Employees need to understand the procedures and prohibitions in place when company assets (computers, mobile devices, etc.) are used to access, view, collect, use, store, retain, and disseminate information obtained from social media sites. This also includes employees acting on behalf of the company, as is often the case with human resources and marketing.

Social Media Investigation Policy

Spencer Hamer, in "Creating an Effective Workplace Social Media Policy" that ran in Bloomberg Law, wrote that "75 percent of employees access social media daily on the job, with 60 percent doing it multiple times per day." Hamer indicated that "Only 23 percent of the employees, however, have received a social media policy from their employers, and fewer than 10 percent have received social media training."

It is imperative that employers develop and implement a social media investigation policy. If they do it right, they will balance the protection of their interests and their employees' rights. Here are a few useful guidelines for these policies:

- Be consistent with applicable laws, regulations, and other company policies.

- Ensure that information obtained through social media is evaluated for source reliability and content validity.

- Set specific requirements when documenting, storing, and retaining information obtained through social media.

Though individual employees are free to express themselves, their freedom of speech must not impair the work of their employer or expose confidential information.

It's not unusual for employees to include where they work in their personal social media profiles. While this may seem innocent enough, if inappropriate content is included in the employee's activities, his or her company is associated with those messages. Companies may want to include guidelines for social media usage in their code of conduct to ensure personal accounts do not contain obscene or sexually explicit language, images, or acts that ridicule, malign, or otherwise express bias.

If a complaint is lodged or a breach is suspected, a social media investigation is the next step.

When opening an investigation, the first step is to develop a plan. What is the goal of the investigation? What information is being sought? Then identify the inappropriate employee behaviors. These may include some of the following:

- Inappropriate photos taken at the workplace that could expose a company to hackers. For example, an employee may take a "selfie" in the office, where sensitive company or client information is in plain sight.

- Photos of employees playing sports or engaging in other physical activities while on sick leave/workers' compensation.

- Discovery of an employee's separate business that could pose a conflict of interest/noncompete infringement or divert company assets.

- Discovery of photos taken by an employee from locations other than the office during business hours or unauthorized activities during business hours.

You will also want to determine if the company's name is posted on employee Facebook, LinkedIn, or other accounts where inappropriate content may exist.

If you suspect fraud at work, include the following in your investigation plan:

- A network of potential accomplices to the fraudster who may provide relevant investigative information

- Identification of any companies owned by the fraudster where embezzled funds could have been diverted

To be effective in a social media hunt, here are a few search criteria:

- Individual's full name
- His or her nickname, if known
- His or her e-mail address, either work or personal, if known (This search criterion typically provides results, as people generally provide their e-mail when creating user accounts.)
- His or her cell phone number, if known

Hundreds of social media platforms exist, and more seem to emerge every day. What follows are several platforms that are most commonly used in employee investigations.

LinkedIn

According to LinkedIn, the professional network provides access to people, jobs, news, and updates, and has approximately 400 million members in more than 200 countries and territories around the world.

Investigators using LinkedIn must understand how their information and search efforts are being shared with and disclosed to the person being searched. An investigator never wants his or her identity known, and should restrict this within the profile settings. With LinkedIn, people can see your name, photo, and headline when you view other profiles. You can, however, choose to display anonymous profile information or show up as an anonymous member.

These privacy settings are essential to anonymous investigations. The settings restrict Basic LinkedIn users from seeing who has viewed their page. Premium LinkedIn accounts users will see that an anonymous viewer has looked at their profile. Anonymous always looks the same though, and the icon cannot be clicked.

Use in an investigation – LinkedIn can help identify the following types of information about someone under investigation:

- Work history
- Education history
- Organizational memberships

- Relationships/individuals who may provide more information * Possible conflicts of interests or other entities associated with that individual

- Miscellaneous background information, such as birth date, address, phone number, and Twitter handle

Search limitations – LinkedIn subscribers with the Basic membership and anonymous privacy settings are unable to see who has viewed their page and vice versa. According to Linked-In, “Some members choose to remain anonymous when viewing profiles. These members do not choose to be anonymous when only viewing certain profiles. Instead, they choose to be anonymous when viewing all profiles.” Those with a Premium account won’t see the names of viewers who chose to display themselves as anonymous. Be aware that anonymity can be temporary. Say you decide to cloak yourself, so you change the appropriate setting before you go off and browse. However, if you switch back to the nonanonymous setting, make sure you do not visit the same profile within a 90-day period. If you do, LinkedIn will switch all of your previous anonymous footprints back to your name and headline.

Facebook

Facebook bills itself as having the mission to give people the power to “make the world more open and connected.” The platform is primarily used to stay connected with friends and family. Many users receive updates about world events through their Facebook feed.

Investigations using Facebook can be effective, though investigators will obtain the most results if logged on to a Facebook account. Unlike LinkedIn, Facebook users do not have to select preferences for anonymity: users cannot see who has viewed their page.

Use in an investigation – Facebook can be used to identify the following information about an individual:

- Friends and relationships

- Whether activities and posts “liked” are appropriate

- Hate speech or incidences of discrimination

- Posts or photos that identify whether an individual represents the employer well

- Employee activities to see whether he or she has been truthful about leave

Search limitations – Facebook users can block others from viewing their “friends” lists. If an investigator is unable to access this information because of a privacy block, he or she can place the cursor on posted photos and see a drop-down list of individuals who “liked” the photo.

An investigator should never try to contact the individual being investigated or “like” anything posted. If the investigator does contact the person, the investigator’s identity will be disclosed and anonymity will be lost.

Twitter

Users of Twitter send and receive short, 140-character messages, or “tweets.” Investigators using Twitter need not be a registered user to perform searches, but without an account an investigator will not be able to post tweets. Access will be read-only.

Use in an investigation – Twitter can be used to identify the following information about a subject:

- Friends and relationships
- Whether posts “retweeted” by the individual are appropriate or professional
- Use of hate speech
- Posts or photos that identify whether or not the individual represents the employer well
- Recent activities to ascertain whether an employee has been truthful about leave

Searches can be performed through Twitter using the dialogue box on the platform’s website. Remember that usernames, also known as handles, are displayed as “@username.” Phrases can be used to search for an exact name or statement. For best results, the phrase should be enclosed within quotation marks. And don’t forget the hashtags. The # symbol, or hashtag, is used to mark keywords or topics in a tweet. It is how Twitter users categorize messages, such as #offsicktoday.

Search rules – Twitter users performing searches should adhere to five rules:

- Never tweet to the individual being investigated.
- Never mention an individual in a tweet using their handle, nickname, or actual name.
- Never “follow” an individual involved in an investigation.
- Never retweet their messages.
- Never “favorite” their tweets.

Pinterest

“Pinterest is a place to discover ideas for all your projects and interests, hand-picked by people like you,” says Pinterest.com. It is, in essence, a visual bookmarking tool to collect ideas and to follow

other pinners' boards or accounts.

Searches can be made without a Pinterest account, but pins and boards will not be viewable. Without an account, investigators will only be able to view an individual's home page. Investigators can find individuals on Pinterest either by searching on the Pinterest site after logging on or by searching through Google and placing a username directly after www.pinterest.com, such as www.pinterest.com/username.

Use in an investigation – Pinterest can be used to identify the following information about an individual under investigation:

- Activities they like
- A user's correct Facebook account

Google+

Google+ is a platform for sharing digital content with friends, family, and coworkers. Users create a Google+ profile similar to other social media sites, with options to share biographies containing their interests, occupation, contact information, and more.

Photos, blogs, and websites can be shared with other Google+ users. Google+ organizes networks of friends, family, and co-workers into "circles," "communities," and "hangouts."

Use in an investigation – Google+ can be used to identify the following information:

- Biographical information, including interests, occupation, contact information, and more
- Websites and blogs created by the individual
- Posts that can be reviewed for appropriateness
- Networks of friends and family through their communities
- Links to other social media accounts

Search limitations – Investigators using Google+ may encounter the following restrictions:

- The search function is accessible only from registered Google+ user accounts.
- Registered Google+ users can set their account to "private" in the profile settings, allowing the user to choose who has access to their posts.

- Communities and circles can be made private.
- Posts made to private communities will not be viewable on the user's profile.
- Information obtained from private users will be limited.

Instagram

Instagram is a site where users upload photos or videos and share them with their followers or selected friends. Instagram provides various filters and other photo-editing features. Instagram allows users to post and share photos to their registered Facebook, Twitter, and other social media accounts.

Use in an investigation – Instagram can be used to identify the following information:

- Biographical information, including interests, occupation, contact information, and more
- Websites and blogs created by the individual
- Posts of inappropriate photos and videos
- Networks of friends and family that can be identified through the "following" and "followers" lists
- Links to other social media accounts

Searches can be conducted using an individual's name or username. Aside from searching and monitoring accounts directly through Instagram, free Internet services, such as Iconosquare, integrate with Instagram and allow users to grow and measure their social media efforts using certain metrics.

The Instagram mobile app has limitations, but Iconosquare allows users to promote their Instagram accounts over various social media platforms. Additionally, through Iconosquare, investigators are able to select images and identify the exact location that geotagged photos were taken. Geotagged photos are created when location settings are not turned off on a user's cell phone camera.

Search limitations – Investigators may encounter the following restrictions with Instagram:

- Must have an Instagram account to use the search function.
- Users can make their account private, so only followers who have been provided permission can view posted photos.

- Information obtained from private users is limited.

Biznar

Biznar is a public search engine that uses other search engines to gather information. It then collates and ranks the results, dropping any duplication.

Use in an investigation – With Biznar you can search for names or other keywords and create alerts for specific criteria. Biz- nar searches social media, news, published research, and patents to locate specific search criteria. Investigators can use Biznar to assist with investigations and conduct personal brand monitoring.

Conclusion

With these platforms, a social-media-savvy investigator can build a clear online picture of an individual under investigation. Individuals should also be aware of the access social media provides as they build their online profiles.

Lisa A. Myers, CPA, CFE, CGMA, is a principal at Boyer & Ritter LLC, a member of the firm's Forensic, Valuation and Litigation Support Services group, and 2016-2017 president of the PICPA. She can be reached at lmyers@cpabr.com.