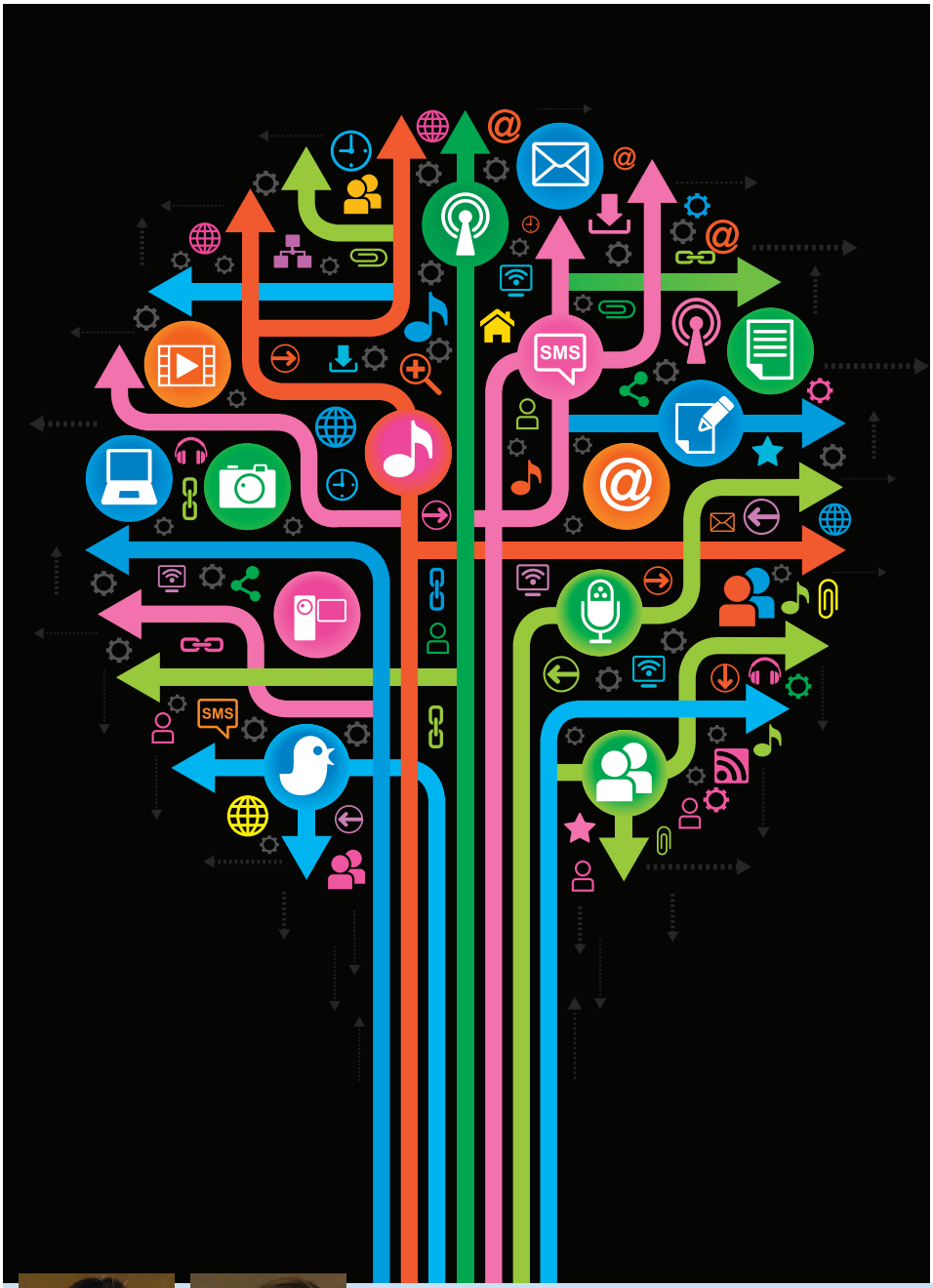
By Christy Mennen and Megan Backer Kelley

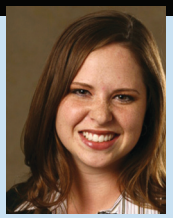
A Social Media Checklist for Your Outside Counsel



The legal world is buzzing about social media's impact on corporate defense strategies. Given the large number of court decisions, ethics opinions, and articles focusing on this area, you likely believe that your outside counsel is tracking the developments and employing the latest and greatest techniques. This article provides a checklist of social media hot topics ranging from employment policies, hiring practices, and handling employee use, to investigating opposing parties and jurors and developing strong trial strategies. It is filled with tips and tricks for social media inquiries and other considerations that outside counsel can and should assist you with today and into the future.

Protecting Your Company Identity

Protecting your corporate name and reputation is always a top priority when defending cases. Now, with the influx of social media, it is extremely important not to underestimate how your corporate online identity can affect the outcome of your case. For example, if your main company witness is posting negative comments about the company on his personal but public Facebook profile, your defense themes could be compromised during his deposition. At the beginning of every case, in-house and outside counsel should discuss the various aspects of the company's online presence and the best tactics for protecting the identity of the company and its



■ Christy Mennen is a shareholder and Megan Backer Kelley is an associate at Nilan Johnson Lewis PA in Minneapolis. Ms. Mennen practices in the areas of product liability, personal injury, and transportation defense, and specializes in social media investigations. She serves on DRI's Young Lawyers Steering Committee and is a member of DRI's Product Liability and Commercial Litigation Committees. Ms. Kelley litigates for and advises clients on a wide variety of labor and employment matters, including social media issues. She is a member of DRI's Employment and Labor Law and Retail and Hospitality Committees.

employees through trial. Counsel should make every effort to identify key company witnesses at the onset and provide advice about their use of corporate and personal social media websites. While it is unlikely that opposing counsel will try to contact them via social media means due to ethical concerns, corporate witnesses and counsel should be advised to consider activating privacy settings and to take caution when communicating with or accepting "friend" requests from unknown individuals. Likewise, key witnesses should be advised not to blog or otherwise discuss court hearings or trials online. Although it may seem obvious that defendants should refrain from discussing their defense strategy online, it can and does happen that corporate defendants are caught posting about their deposition or trial experience on the Internet. In 2007, Boston physician Robert Lindeman offered a play-by-play of his medical malpractice trial on his blog under the pseudonym "Dr. Flea." When plaintiff's counsel caught wind of the website and exposed statements that were inconsistent with his trial testimony, he was forced into a quick settlement. If Lindeman's attorney had advised him of the risks associated with social media use, that situation could likely have been avoided.

In addition, outside counsel can provide a risk-benefit analysis of using social media for marketing purposes, including the potential pitfalls associated with public webpages where consumers can post complaints. This is particularly important for product manufacturers, where public records could be considered evidence of "same or similar claims" in product defect cases.

Understanding Social Media's Relevance to Your Defense Themes

Social media investigations of claimants and plaintiffs are valuable in every case. Given the current 845 million-plus Facebook users alone, the chance that the opposing party to your litigation has posted potentially adverse or incriminating information online is extremely high. A social media inquiry can quickly uncover facts and evidence that would have otherwise taken months to obtain through discovery. In many cases, a Facebook search can tell you the opposing party's birth date, residence, close friends and family members and, if you are lucky, the circumstances leading up to the subject incident, as well as the names of witnesses and related photographs.

Courts across the country agree that social media evidence bears relevance to pending litigation. The key to the relevancy determination appears to be whether the information depicts a snapshot of the user's physical or mental state at the time of the posting. *Bass v. Miss Porter's School*, 2009 WL 3724968, D. Conn. Oct. 27, 2009. While there is continuing debate as to the definition of "relevant" social media evidence, it is common for judges to rule that *any* information related to the physical or mental state of the plaintiff is relevant to the case. Likewise, in many instances, judges have allowed defense counsel to review a plaintiff's entire Facebook profile (in some cases, even private profiles) and make their own determination of what should be deemed relevant.

Outside counsel can provide a risk-benefit analysis of using social media for marketing purposes, including the potential pitfalls associated with public webpages where consumers can post complaints.

Even better, courts have dismissed entire cases or limited select damages claims based, in some instances, on a single posting or photograph of plaintiff. For example, in *In re Welding Fume Products Liability MDL*, No. 03-cv-1700 (D. Ohio Jan. 21, 2010), a federal judge in the District of Ohio dismissed a welder's product liability suit alleging total disability after the defense found Facebook photos of him racing motor boats. In another case, a Los Angeles firefighter was arrested on suspicion of insurance fraud after investigators observed that he competed in seven Mixed Martial Arts bouts—which were uploaded to YouTube and viewable by the public—while he was out of work and receiving workers' compensation benefits.

Conducting Social Media Investigations

At the outset of the claims stage, outside counsel should conduct an efficient, yet thorough inquiry of the opposing parties' social media presence and provide recommendations on how it can be used to strengthen your defense strategy. Counsel can initially conduct searches on Facebook, Twitter, LinkedIn, Yahoo!, Bing and YouTube, for example. Then, depending on the search results, he or she can proceed with a more extensive investigation with advanced searching tools on Google Advanced, Amazon wish list, photo sharing websites and using the Internet Archive Wayback Machine to access archived information. It can take only minutes to determine whether the plaintiff has a profile on one or more of the most popular social media websites and whether his or her personal information is publicly available. In fact, counsel has the ability to determine exactly what the plaintiff did, said, and saw on the date of the incident related to the lawsuit. In addition, outside counsel can conduct social media investigations of other parties, including plaintiff's spouse or family member, witnesses, co-defendants and opposing expert witnesses.

Outside counsel should explain its firm's social media inquiry protocol to in-house counsel so that they understand the parameters of the search and the purpose and goals of the investigation. It is extremely important, for instance, that outside counsel designate an individual with expertise in Internet searches to conduct the investigation. Due to the intricacies of the various social media websites, only a skilled investigator will know how to master the techniques and tricks associated with accessing otherwise hidden data. An untrained investigator may easily overlook the vast amount of information available.

Preserving and Authenticating Social Media Evidence

Social media websites are valuable repositories of potential evidence—snapshots of the past and present—that could be used for impeachment purposes against parties and witnesses. It is imperative that outside counsel are aware of the latest guidelines for preserving, authenticating and admitting social media evidence. It is not enough, for example, to access plaintiff's Facebook page, hit "print" and then offer the printout of the webpage into evidence. Several courts across the country have shown reluctance to admit social media profiles without ample circumstantial evidence attesting to their authenticity and sufficient "distinctive characteristics" to authenticate printouts. Depending on the jurisdiction, some or all of the following avenues for authentication should be used 1) testimony from the creator of the profile and relevant postings; 2) testimony from the person who received the message; 3) testimony or affidavit about the distinctive aspects in the messages revealing the identity of the sender; 4) testimony regarding the account holder's exclusive access to the social media account; or 5) testimony from the social networking website connecting the posting to the person who created it. With respect to number 4, you should expect outside counsel to send preservation requests to Facebook, Twitter, LinkedIn and any other website where the opposing party has an active social media presence. Although these entities take varying positions on their obligation to preserve and produce the evidence, it is advisable to serve these requests at the start of the claims stage or litigation.

In addition to preserving with care any incriminating evidence that is found, outside counsel must be aware of the preservation obligations and potential spoliation considerations related to the handling of social media evidence. Under no circumstances should an attorney instruct a client to spoliate or obstruct the other party's access to documents or information with potential evidentiary value. This rule, of course, applies equally to corporate defendants and their counsel. Your outside counsel should work to ensure that relevant corporate social media, like other electronic evidence, is being properly preserved. You should also expect that your counsel take appropriate measures to protect plaintiff's social media evidence. Counsel should consider sending a specific preservation letter to plaintiff's counsel directing him or her to preserve any potentially relevant social media evidence to avoid spoliation sanctions. Outside counsel should also use written discovery requests to address preservation concerns, including an interrogatory asking whether plaintiff has deleted information or data since the date of the alleged incident giving rise to the claim and if so, the date the information was deleted, the purpose behind the deletion and the nature and substance of the deleted information.

> Counsel has the ability to determine exactly what the plaintiff did, said, and saw on the date of the incident related to the lawsuit.

Judges across the country have shown no reluctance to impose spoliation sanctions, both monetary and by way of dismissal, when parties violate these preservation obligations. In *Torres v. Lexington Ins. Co.*, 237 F.R.D. 533 (D.P.R. 2006), a federal judge in the District of Puerto Rico flatly denied the plaintiff's emotional distress claims after she deleted online postings that defense counsel was aware of and had brought to her attention. In addition, late last year, attorney Matthew Murray of Virginia was ordered to pay a whopping $522,000 after instructing his client to remove photographs from his Facebook profile.

Leveraging Social Media Tactics During Discovery

In addition to knowing where to look, counsel need to be armed with a strategy for using social media evidence once it is found. Outside counsel should propose a plan of action for the discovery phase of the case. This strategy will vary greatly depending on whether the opposing party has activated privacy settings. If so, counsel will have limited access to background information, postings, and photographs. It is common, however, for Facebook users to make their list of Facebook "Friends" publicly available, even where the remaining identifying information is kept private. In this situation, outside counsel should think strategically about using the "Friends" list to his or her tactical advantage. For example, the list can be used to identify fact witnesses and in turn, allow counsel the opportunity to conduct interviews early in the case or send a subpoena *duces tecum* requesting that the individual provide printouts of all information and photographs from the plaintiff's Facebook profile. Additionally, counsel should follow the trail behind the "Interests" tab on Facebook, which, in our experience, has led to evidence that a plaintiff who claimed her injuries kept her from working was profiting from a side business during the course of litigation.

Outside counsel should be strategic in seeking access to protected information through written discovery and depositions. Counsel will need to decide when and how to elicit private information on a case by case basis. Seeking this information too early tips plaintiff off that you are reviewing his or her online presence, while waiting until the deposition runs the risk that opposing counsel will object on relevancy grounds. Again, counsel must be familiar with the laws of the state and views of the assigned judge to avoid any appearance of overreaching. Notably, Facebook recently added a "download profile" feature, which allows counsel to request that plaintiff him- or herself download and provide his or her entire Facebook profile, including Information, Interests, Photographs, and Wall Postings. In situations where plaintiff's Facebook page is marked private and you want to review his or her social media evidence prior to depositions, your outside counsel should consider serving an interrogatory asking plaintiff to run the Facebook download. Another option is to consider seeking limited access to the pri-

vate portion of plaintiff's Facebook page. In an interesting opinion dated February 27, 2012, a Pennsylvania judge ordered defendant to provide his username, email, and password to plaintiff's counsel, yet allowed plaintiff the opportunity to change his Facebook login and password seven days after compliance with the order. *See Gallagher v. Urbanovich et al.*, No. 2010-33148, Court of Common Pleas of Montgomery County, Pennsylvania.

If, on the other hand, plaintiff's social media is public, counsel is free to capture the material and decide the most effective time to produce or reveal it. Where the information is publicly available, it is arguable that it need not be produced. In this situation, defense counsel can use the information through the course of litigation—using the "Friends" list to identify witnesses to the incident or plaintiff's current physical or mental state, for example. It is essential that outside counsel investigate and preserve all relevant publicly available information early as there is always a possibility that plaintiff will activate privacy settings at some point after litigation commences. Likewise, outside counsel should create a specific timeline for periodic review and capture of the evidence throughout the litigation.

In our experience, discoverability of social media evidence through written interrogatories and requests for production varies greatly from case to case. In some instances, plaintiff's counsel will turn over every password, website address and document requested. In others, counsel will require a court order compelling production. Outside counsel should be armed with the strongest language from the most defense-friendly opinions in their state and across the country. For example, in *Zimmerman v. Weis Markets, Inc.*, No. CV-09-1535, May 19, 2011, the court stated: "a social networking site is the interactive sharing of your personal life with others; the recipients are not limited in what they do with such knowledge. With the initiation of litigation to seek a monetary award based upon limitations or harm to one's person, any relevant, non-privileged information about one's life that is shared with others and can be gleaned by defendants from the Internet is fair game in today's society." Similarly, in *McMillen v. Hummingbird Speedway Inc.*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Jefferson Co. Com. Pl. 2010), the Court stated: "Facebook, MySpace, and their ilk are social network computer sites people utilize to connect with friends and meet new people. That is, in fact, their purpose, and they do not bill themselves as anything else. Thus, while it is conceivable that a person could use them as forums to divulge and seek advice on personal and private matters, it would be unrealistic to expect that such disclosures would be considered confidential." These opinions, in which judges have expanded the scope of "relevant" social media evidence, increase the likelihood of success in compelling production.

A jury research team should be put in place prior to trial and be ready to act as soon as the court releases the list of potential jurors.

Keeping Tabs on the Judge and Jury

Outside trial counsel must take advantage of the plethora of information that is publicly available on social media sites to research potential jurors for the purposes of voir dire. It is extremely useful to develop a streamlined system for conducting this research and efficiently managing the information obtained. A jury research team should be put in place prior to trial and be ready to act as soon as the court releases the list of potential jurors and background information on each juror, whether it be days or minutes before voir dire begins. Using a separate jury research team allows the trial team to remain focused on their pretrial responsibilities and preparing to present the best possible defense at trial.

Part of the jury research team should obtain information from public records, including civil and bankruptcy proceedings and judgments, criminal history, vehicle registrations, professional and recreational licenses, household members, neighbors, and relatives. The remainder of the team should comb the Web—including search engines, social media sites, blogs, and news sources—using specific search methods to obtain any relevant information in an efficient manner. As the research team collects relevant data, it should be entered into a live database, which allows the information to be immediately accessible to the trial team for use in conducting voir dire.

The information obtained during the jury research process informs trial counsel's questions during voir dire, and can allow trial counsel to identify a potential juror to strike without giving the potential juror an opportunity to influence the other jurors by voicing unfavorable opinions during voir dire. For example, during a recent pharmaceutical trial, jury research identified a potential juror who made it publicly known in a blog that he did not believe in medicine or trust pharmaceutical companies. We were able to identify this individual as an unfavorable juror without soliciting information about these opinions in the presence of the other potential jurors.

In addition, outside counsel should insist on jury instructions targeted at jurors' social media use. Jurors should be instructed not to use any electronic device or media, cell phone, computer, Internet service, text messaging service, chat room, blog, or website such as Facebook, MySpace, LinkedIn, YouTube, or Twitter to communicate any information or conduct any research about the case. Although whether the court adopts your proposed instructions may depend on whether the particular judge is technologically savvy, your outside counsel should aggressively pursue use of such instructions, not only post-trial but during trial, in addition to requesting that jurors not be allowed to access their cell phones during trial. These instructions will guide your trial counsel's jury research team as they monitor the Internet activity of jurors during trial. In turn, you will be able to identify any potential or real juror misconduct. In the event this misconduct forms the basis of

an appeal, outside counsel should carefully preserve all online materials to ensure that they will be admissible at later proceeding. There is, of course, a balancing act at play, since there is always a possibility that a juror you favor will engage in misconduct or violate the jury instructions.

In addition to researching jurors, your outside counsel should be familiar with the assigned judge's social media activity and specifically whether he or she has an online relationship with opposing counsel or parties. A recent decision by the Pennsylvania Court of Common Pleas suggests a judge who is Facebook friends with a party must recuse him- or herself as a matter of course. In that case, Judge Hayden was Facebook friends with State Representative Cherelle Parker, who was arrested for drunk driving. Judge Hayden's decision to suppress the testimony of the arresting officers was reversed by the Common Pleas Court, on the basis that the judge had abused his discretion by not recusing himself.

Walking the Ethics Tightrope

At all costs, you want to avoid a situation where your outside counsel locates plaintiff's damning social media evidence, yet then concludes it cannot be offered because it was obtained unethically. Although it can be difficult to stay current on the ever-changing social media ethical considerations, it is imperative that your outside counsel makes it a priority to follow the ethical rules, opinions, and guidelines in the states where each case is venued.

There is no question that it is ethical to view opposing party's social media profiles. As the New York State Bar Association Committee on Professional Ethics aptly stated: "[W]e conclude that the lawyer may ethically view and access the Facebook and MySpace profiles of a party other than the lawyer's client in litigation as long as the party's profile is available to all members in the network and the lawyer neither 'friends' the other party nor directs someone else to do so." The real question is—how far can you go to view private information? As you might guess, if your outside counsel (or anyone acting on their behalf) sends a "friend" request to an opposing party, they violate the ethics rule against contact with represented parties. What if the matter is in the claims stage and suit has not yet been initiated? Best practices suggest refraining from contact with unrepresented parties if you anticipate they may seek representation in the future. Ethics committees in Philadelphia and Oregon, among other states, have issued opinions to this effect. The biggest concern appears to be the potentially deceptive conduct, particularly in a situation where the attorney asks his non-attorney assistant to make the friend request. There are also a host of opinions related to social media contact with judges. Ethics committees in Ohio, South Carolina, and North Carolina have issued advisory opinions that permit judges to "friend" attorneys, whereas Florida's committee has concluded such friend requests are not appropriate.

The real question is—how far can you go to view private information?

In addition, your outside counsel should speak openly with you about your role, as well as the role of in-house legal staff and claims adjusters in conducting social media investigations. While adjusters, for example, may not be bound to the same ethical obligations as attorneys, it would be risky to allow them to conduct investigations and furnish the results to your outside counsel if the information was not collected or preserved in a way that ensures its admissibility at trial.

Developing Your Social Media Policy

Even if your company does not intentionally utilize social media sites to further its business or marketing plans, you can be sure that your employees utilize them daily, for better or worse (and sometimes much worse). Your employment policies should ensure—to the extent possible—that your employees' social media use is not detrimental to your business and does not create legal liability for you as the employer. In order to accomplish this, you should develop a social media policy that incorporates at least the following elements.

- Make explicitly clear that your employment policies prohibiting sexual and other forms of unlawful harassment apply with equal force to communications that take place over social media. In addition to this policy, your management-level employees should be trained on the use of social media. The training should include an instruction not to "friend" or accept friend requests from subordinates on social networking sites, as the relationship could lead to interactions that, even if harmless, could look like evidence to support a harassment claim. Management friendships with subordinates could also put the company "on notice" of any communications—including harassment or airing of workplace grievances—that take place on the subordinates' social media pages.
- Expressly prohibit employees from using company property (including computers, company-licensed software, and company facilities) or work time for social networking activities, unless they have a legitimate business reason for logging on to social media sites and have been authorized to do so to perform their job duties.
- Reiterate the company's right to monitor employees' Internet use.
- Prohibit employees from speaking on behalf of the company in any public forum, including social media sites, without prior authorization. It should also provide that when employees engage in authorized use of social media or other forms of web-based communications to speak on behalf of the company, employees must ensure that any communications maintain the company's brand identity, integrity, and reputation. Further, your policy should establish your company's ownership of any postings or tweets that an employee creates in the capacity of their employment.
- Your social media policy should specifically incorporate a number of other employment policies, including but not limited to your policies on harassment, solicitation and distribution, fraternization, and confidential information and trade secrets.

- As with all employment policies, your social media policy should require employees to report any violations of the policy and note that employees who violate the policy will be disciplined, up to and including termination of employment.

Although it may be tempting to prohibit employees from making any disparaging comments about the company via social media, you must ensure that your social media policy does not run afoul of the National Labor Relations Act by prohibiting concerted activity that may be protected by the Act. The National Labor Relations Board has concluded that employment policies that prohibit, for example, "discriminatory, defamatory, or harassing web entries about specific employees, work environment or work-related issues on social media sites," are unlawful, because they sweep too broadly and prohibit discussion of work-related issues.

The elements above are a starting point, but your regulation of your employees' social media use will depend on your business, your workforce, and to what extent your employees have legitimate business reasons for using social media. Because technology is constantly evolving and developing, as is the applicable case law in this area, your company should review its social media policy and procedures on an annual basis to keep current with legal developments.

Responding to Employee Use of Social Media

The use of social media by your employees creates new—and exceptionally visible—avenues for employees to interact with one another and the general public. Due to the public nature of these communications, your company may be put "on notice" of harassment or protected activity under a broader range of circumstances than ever before. Assuming your company has an effective and enforceable social media policy in place, as discussed above, it has taken a big step in the right direction toward responding to employee use of social media. In addition to implementing and enforcing your social media policy, you should be prepared to respond to your employees' use of social media in several specific ways.

Sexual or other unlawful harassment that takes place via social media is different from face-to-face harassment for at least two important reasons. First, depending on the social media practices of your managers, they may witness the harassment, even if it takes place outside the workplace. This puts the company on notice of the unlawful conduct and imposes an obligation to investigate and correct the harassment, as well as prevent further harassment. Your managers should be trained to respond to harassment they witness via social media in the same manner they would respond to harassment in the workplace. And significantly, communications that were at one time "he said/she said" will now be documented and preserved. This can be both a positive and a negative factor, depending on the situation, but it should not be overlooked. If the company receives a report of harassment, the investigation should include an examination of all communications between the alleged harasser and alleged victim on internal and external social networking sites, as well as email and text messaging.

Just as your managers should be trained to respond to any potentially harassing conduct they witness over social media, they should also be trained not to discipline employees for airing grievances about the workplace over social media if those communications could be considered concerted activity under the National Labor Relations Act. Generally, employees engaging in discussion regarding the terms and conditions of their employment with other employees using social media are engaging in protected activity. In contrast, employees airing individual gripes against their employer without any co-worker comments or participation are not protected. The National Labor Relations Board has provided specific guidance on when an employee's social media activities are protected and should not be subject to discipline.

An employee's social media activities may also implicate the Fair Labor Standards Act and state equivalents. To the extent your company encourages employees to engage in social networking to further the company's message or promote its products or services, it should be mindful of wage and hour implications. Time spent posting or tweeting about the company's products or services after work hours may be compensable time if the employee is non-exempt from overtime laws. To avoid liability for unpaid overtime, your employment policies and managers should make clear that engaging in social media activities on behalf of the company outside of work hours is prohibited without prior approval, and when approval for such activities is given, time worked must be recorded and compensated.

Cautioning Against the Use of Social Media in Hiring

Given the wealth of information available on social media sites, it is certainly tempting to search for applicants and even current employees seeking promotion on Facebook, Twitter, or other social networking sites. There is nothing inherently unlawful about searching for applicants on the Internet. However, in doing so, your human resources personnel and recruiters may discover information that exposes you to liability for hiring decisions. Accordingly, social media research on job applicants must be done consistently and according to a policy, or not at all.

If an applicant blogs, tweets, or posts information relating to a protected classification, including gender, race, age, sexual orientation, genetic information, religion, disability, or any other protected classification, and your company declines to hire the applicant after reading the posting or because of the posting, you may be at risk for a discrimination or retaliation claim. Further, if your recruiters gain information about an applicant from a social media site that has a focused audience based on a protected classification, you may be at risk for "disparate impact" discrimination claims (which do not require an applicant to prove intent to discriminate).

The Genetic Information Nondiscrimination Act of 2008 (GINA), gave rise to a new form of discrimination claim and new legal considerations for employers. GINA not only prohibits discrimination based on genetic information, but it also prohibits an employer from acquiring genetic information of an employee or applicant, or the

Social Media › page 60

Social Media ❮ page 13
medical history," which includes information about the manifestation of a genetic disease or disorder in a family member of the employee or applicant. GINA makes it unlawful for an employer to, among other things, conduct an Internet search that is "likely to obtain" genetic information. Accordingly, your recruiters must be cautious about searching for applicants on social media sites and uncovering information about a family member's genetic disorder—for example, an employee's photos of herself with her mother, a breast cancer survivor, at the Race for the Cure; or an applicant's wall post about the news that his child was diagnosed with a genetic disorder. Note, however, that a basic Google search that inadvertently results in the display of publicly available information about a genetic disorder of an individual's family member does not violate GINA.

If your company intends to conduct social media background checks on applicants, you should implement a policy whereby the background checks are conducted by someone—either within your organization or an outside vendor—who is otherwise uninvolved in the recruiting and hiring process. This individual should be trained not to reveal any protected characteristics or other information that cannot lawfully be considered by the hiring decision maker.

Conclusion

There have been dramatic social networking changes over the past few years, making it impossible to ignore social media's influence on corporate business practices and litigation. Because the legal issues associated with social media continue to change as quickly as the technology itself, you and your outside counsel should regularly reevaluate the social media strategies you employ. Although at first glance it may appear costly or time-consuming to track evolving social media considerations, your company will be at a great advantage if you and your outside counsel explore and adopt these techniques. Not only will it lead to better business and litigation results, but it will give you a clear edge over those adversaries who have yet to embrace the true potential of this emerging area. IDQ