The 2011 Hospitality Law Conference
Houston, Texas
February 9-11, 2011

You Can't Take It Back: Is Your Company Prepared For Employees Using Social Media?

GRIESING LAW LLC
Francine Friedman Griesing, Esq.
Kathryn Goldstein Legge, Esq.
1717 Arch Street, Suite 3630
Philadelphia, PA 19103
P.: 215.618.3720 / F.: 215.814.9049
fgriesing@griesinglaw.com
klegge@griesinglaw.com
www.griesinglaw.com

FRANCINE FRIEDMAN GRIESING

In January 2010, Fran Griesing founded Griesing Law, LLC, a WBENC-certified firm, recognized as consistently providing personal attention and delivering proven results economically. Fran defends clients and serves as a neutral arbitrator and mediator in complex business transactions, high stakes litigation, and alternate dispute resolution, and she advises clients on reducing legal costs. Her clients, public and closely held companies in the Philadelphia area and beyond, share a desire to succeed in their marketplace, grow revenues and avoid costly legal problems

Fran has successfully represented clients, for almost thirty years, in sophisticated deals, litigation and ADR matters. *Chambers and Partners USA*™, a leading directory of the legal profession, has noted that clients describe her as "intensely detail-focused and a persuasive and energetic litigator" with a "professional and personable manner." *Chambers* has also expressly recognized her for her work in the hospitality industry, and for her "practical and down-to-earth counsel."

Prior to launching Griesing Law, LLC, Fran practiced law at some of the country's top tier firms in New York and Philadelphia and in public service. Earlier in her career, she was appointed by former Philadelphia Mayor Edward G. Rendell, current Governor of the Commonwealth of Pennsylvania, to serve as Chair of Litigation of Philadelphia's City Solicitor's Office. As the City's lead trial lawyer, she handled legal matters involving the City's popular tourist venues, including Veterans Stadium, the Pennsylvania Convention Center, Penn's Landing/Delaware Avenue, Fairmount Park, historic Old City and Main Street Manayunk. She advised the Mayor, ranking administration officials and City Council on cutting-edge legal issues, while managing over 2,000 matters, supervising 75 lawyers plus attendant support staff, and overseeing outside counsel. As the City's lead attorney on several high-profile matters, she is accustomed to working with a diverse constituency and performing under public scrutiny.

An honors graduate of Binghamton University and the University of Pennsylvania Law School, where she was an editor of the *Law Review*, Ms. Griesing has been recognized for her professional and community leadership activities involving bar association and civil projects. She has been acknowledged as a SmartCEO 2010 Legal Elite, Woman to Watch, Pennsylvania Super Lawyer 2004-2010, Governor's Best 50 Women in Business™, and Greater Philadelphia Woman of Distinction™. Demonstrating a longstanding commitment to professionalism, ethics and continuing legal education, Ms. Griesing received the Philadelphia Bar Education Center's *Excellence* in Legal Education Award and the American Bar Association's Excellence in Legal Writing Award. She has taught Business Law, Public Employment Law and Advocacy Skills at Temple University's Beasley School of Law and Fox School of Business & Management and has been a guest lecturer at the University of Pennsylvania's Wharton School. Ms. Griesing is included on the American Arbitration Association Roster of Neutrals for commercial and employment matters, the CPR Dispute Resolution Center list of approved neutrals for commercial, employment and hospitality franchise matters, and the Philadelphia Court of Common Pleas Commerce Court Judge Pro Tempore program.

TABLE OF CONTENTS[1]

[1]Griesing Law, LLC would like to thank its student intern, Jason Kucza (Drexel University, Class of 2012) for his contributions to these materials.

I. SCOPE OF ARTICLE

This program will cover four principal areas related to employee use of social media both at work and offsite. We start with a discussion on social media issues as they relate to defamation, intellectual property infringement, and improper disclosure of confidential information, and liability for personal injury or property damage. We will follow with potential risks of litigation. Next, we will address best practices for human resources use of social media. Finally, we will discuss professional responsibility and ethical issues concerning social media presence.

A. Applicable Legislation and Common Law

The Digital Millennium Copyright Act (DMCA), the Communications Decency Act of 1996 (CDA), and the Stored Communications Act (SCA) provide limited liability under specific circumstances which will be discussed. In addition, there are a wide array of state laws and common law claims that may arise out of improper use of social media.

B. Top Mistakes to Avoid

Specifically, here's how many lawyers find themselves in trouble:

(a) Failing to monitor and enforce copyrights and trademarks.

(b) Failing to protect client confidences, assure preservation of electronic data, and protect privilege in electronic communications.

(c) Neglecting to manage our clients' online presence and social media activity responsibly.

(d) Lacking a proper litigation response plan or failing to implement a litigation response plan.

(e) Not enforcing a company's social media usage policy or failing to establish a comprehensive policy.

C. The Objective of this Program

The purpose of this presentation is to provide guidance for attorneys serving clients or practicing in hospitality, foodservice and franchise industries so they understand the risks involved for clients that either use social media to promote their services or have employees who may use social media in their personal and professional lives. In-house counsel and outside counsel, both have the ethical responsibility to advise clients and assure compliance with the obligations under the applicable rules.

II. HOW SOCIAL MEDIA INTERACTS WITH THE LAW

A. Defamation

1. How It Works In Real Life

Imagine for a moment, that a tenant lives in a rented apartment and discovers that he is cohabitating with roaches. That person airs his grievances through a Twitter account, posting a short phrase stating that "ABC Co. [owner of the apartment] lets rodents infest their buildings." Shortly thereafter, after the roaches are gone, that tenant is served with a complaint filed by ABC Co. alleging that he defamed the company in his Twitter post. If this story sounds familiar, it should, because it recently occurred in Chicago. In that case, it appears that the two parties settled confidentially out of court, but probably with at least some legal expense borne by the individual who posted the statement.

2. The Legal Standard

Simply stated, defamation is a false statement about another that is published to a third party without any privilege to make the statement. In the social media arena, postings made online can give rise to defamation claims just as if they were spoken to another or appeared in traditional media such as newspapers, radio, or television. Courts have recently been analyzing whether a 140-character statement made on Twitter can give rise to a defamation claim. It appears that courts are leaning towards allowing these inherently short statements to be characterized as defamation when the content is false and would be defamatory if printed or communicated by other means. Of course, a blog, which allows an unrestrained flow of thoughts, lends itself, even more, to potential defamatory statements. Blogs are longer statements directed to a certain subject matter, and can have more description and detail about the subject that is allegedly being defamed. This creates complications both for businesses with social media accounts and for individuals with personal accounts if the user posts a misstatement or a statement that is not well thought out. If a company has a social media presence, no matter the type, or if its employees use social media, statements made about a third party that are not carefully crafted could increase the risk that the company could be sued for defamation. While at this time, in the short life of social media, it appears that individuals have been the primary targets of defamation suits, companies can also be sued.

A company can fall into the defamation trap if it does not have, and enforce, clear policies regarding the content employees can post both on behalf of the company and personally. For example, a company policy should clearly state that online postings -- whether for business or personal use -- cannot make any reference to a company competitor. In addition, any postings about a third party should be approved by a supervisor. The company policy should also state, even when employees use a personal account outside the workplace, that all online statements that relate to the company, a supplier, vendor, or competitor, must specifically affirm that the statements are the

employee's personal views and do not reflect the view of the company and are not made at the company's discretion.

3. A Statutory Safe Haven

The Communications Decency Act[1] ("CDA") provides both companies and individuals immunity, "from any cause of action that makes them liable for publishing information by a third-party user of the service." In essence, the CDA protects social media users from being liable for defamatory statements, if the statement is merely quoting a third party. To take advantage of this provision, the statement needs to attribute the statement to the original speaker. For example, if a third party "retweeted" the Twitter statement above, "ABC Co. [owner of the apartment] lets rodents infest their buildings," the third party cannot be liable for defamation to ABC Co., so long as the third party attributed the statement to the original speaker.

4. How To Minimize Risk

With all of this in mind, here are some practical guidelines:

1) Companies should have one designated person to oversee statements made on behalf of the company, even if the statements are published by different company authors.

2) Companies should make sure that the designee to act as the company "voice" is trusted and has good judgment.

3) Companies should have a written policy stating acceptable and unacceptable topics for publication on social media. The policy should also explain potential legal pitfalls, including the definition of defamation with illustrative examples.

4) If a company has its own social media presence, an executive should monitor all posts made in the company name to make sure of compliance with the company policy and message. This applies, for example, to company Facebook pages, LinkedIn, or blogs.

5) Take advantage of statutory protections, such as the CDA, to immunize the company or individual from claims of defamation. Make sure that company policies state that all employees must attribute any quoted statements made by others to the original authors.

[1] 47 U.S.C. § 230

B. Intellectual Property Infringement

1. Avoiding Infringement of the Intellectual Property of Another

The United States government provides certain protections to the authors of "original works of authorship" including but not limited to literary, dramatic, musical, artistic, and certain other intellectual works. Copyright infringement is the violation of the exclusive rights of a copyright holder. Video clips are a common example of copyright material that is consistently posted on social media websites, even when the person posting the material does not own the copyright. Oftentimes, when a company has a site, like a blog where it allows others to post statements and content, it runs a risk of copyright infringement because a third party's posting of someone else's copyrighted material can be an infringement of that material, leaving the company as the liable party. However, the Digital Millennium Copyright Act[2] ("DMCA") exists to help some unwitting IP infringers avoid liability. The DMCA provides a safe harbor from damages for third party copyright infringement. The DMCA requires a company to have a "takedown policy." In essence, a "takedown policy" is a policy that mandates that upon receiving a complaint of copyright infringement, the company will immediately take down the offending material. As part of this "takedown policy," a company must assign a "Designated Agent" who registers with the U.S. Copyright Office and will receive notifications of claimed infringement. Upon proper DMCA notice, that agent will need to remove the offending material quickly or else the company may not be able to take advantage of the safe harbor. This process can help with trademark infringements as well. However, this safe harbor does not apply in situations where a company receives financial benefit from the infringing post and/or there was actual knowledge that the post was infringing on the copyright or trademark of another.

If a company does have a blog or other type of social media that permits third-party comments or posts, the company can further protect itself by taking a few important precautions. First, a company should create privacy and usage policies and a disclaimer for all people who may access its site. Second, the policies should state that it is at the discretion of the company to take down any offensive posts or posts that may infringe on another person's copyright. Third, the policies should be specific about how the company intends to use the posted information in the future. Fourth, the disclaimer should state that any views expressed by third-parties on the site, do not reflect the views or beliefs of the company. Finally, whenever a new user accesses the site for the first time, the user should need to "click" that it accepts the company's usage and privacy policies as well as the disclaimer.

[2] *See* 17 U.S.C. §§ 512, 1201–1205, 1301–1332; 28 U.S.C. § 4001

2. Protecting Your Company From Copyright Infringement

On the other end of the spectrum, a company needs to protect its own copyright and trademarks. Any party can sign up for a Twitter or Facebook account, using any name it wants, including taking the identity of a third party or impersonating the voice of a company. Therefore, one of the best ways to protect a company copyright and trademark is to register accounts using the company's intellectual property before an unauthorized person does so. A company may need to register multiple accounts, but that will not guarantee an imposter cannot confuse customers. Twitter now provides options to verify accounts in the wake of individuals impersonating celebrities. This, however, did not stop a user from establishing a fake public relations account for BP in the wake of the Gulf Oil Spill and gaining more followers than the actual BP account.

Even if a company chooses not to have an online social networking presence, it should continually monitor social media sites to make sure no one is using the company's copyrights or trademarks improperly. A great way for a company to monitor usage of its intellectual property on social media, even when the company does not use social media, is to set up "Google Alerts" that search for online mentions of the company name and key company employees who may have a public face for the company. Failure to monitor and enforce copyrights and trademarks may result in a company losing its IP rights.

3. How To Minimize Risk

With all of this in mind, here are some practical guidelines:

1) Companies should meet the necessary requirements to take advantage of all statutory protections.

2) On a company blog include a usage and privacy policy that all viewers must accept. This can be done with a "click" acceptance.

3) Make sure all blogs and social networking pages include disclaimers that state that comments by third-parties are not the views expressed by the company.

4) If third-parties are posting content on a company blog or page, ensure that policies are specific about how the company intends to use that content in the future.

5) Continue to screen and review all content on blogs and pages. Although postings made by third-parties may not be edited in most cases, a company can enforce restrictions set forth in usage and privacy policies. When enforcing restrictions, companies are permitted to delete posts that violate usage and privacy policies, especially if the policies specifically state that such action may be taken.

6) Set up social media sites promoting your copyright or trademark in your screen name, such as Zappos does by having all of their employees sign up for a Twitter name that includes both the name Zappos and a description of the content for the Twitter feed.

7) If your company does not intend to have a social media presence, you still need to actively monitor social media to make sure no one else is acting as an imposter. Setting up a "Google Alert" will help you monitor that information.

C. Improper Disclosure of Confidential Information

Employees use social networking as a way to express themselves and stay connected to friends and family, regardless of whether their employer wants them to do so or not. A policy simply forbidding the use of social media at all is neither practical nor good for employee morale. Social media has become such an integral part of our culture that employees will inevitably use it. Without proper policies in place, however, a company can be at risk of two serious outcomes relating to confidentiality: (1) their trade secrets may be exposed, or (2) an employee could disclose future company plans that, by law, must remain confidential.

1. Protecting A Company's Trade Secrets

While non-compete agreements are not always enforceable in many jurisdictions, courts will generally protect a company's trade secrets provided certain requirements are met. Many states actually have statutes that govern the protection of trade secrets. Often, the most valuable trade secret a company has is its customer list. To maintain the trade secret status of a customer list, a company must take certain precautions to restrict the access to the list including, but not limited to, putting password protection on the list, and sharing only certain customers with certain employees, while restricting their access to other customers. When employees are on a social network, specifically sites like Facebook or LinkedIn, without a company policy stating otherwise, they may have customers who become their online "friends" or "connections." At that point, the question arises whether the customer list is still confidential because the customer list is now exposed, in whole or in part, to people outside the company. Protection of the customer list may become even more perilous when an employee who has "friended" customers leaves the company and decides to compete against her former employer, contacting customers of her former employer who also happen to be her "friends", or "connections" on social media. As they are the former employee's "friends" on a social networking site, a court may rule that the employer did not closely guard its customer list, allowing it to become public. In that case, the ex-employee will be able to contact customers without any legal consequences as the trade "secret" status of the list was compromised.

Companies also risk that an indiscrete employee could post trade secrets on a social networking site like a recipe for a unique food product, perhaps not realizing that the recipe is indeed confidential. Many restaurants and food purveyors consider their prized recipes to be protected and the recipe loses its value if it becomes publicly available.

2. Insider Trading

A publicly-traded company may be at a greater risk from employees using social networking sites. Under the securities laws, if an employee discloses material nonpublic information or makes forward-looking statements, material misrepresentations, or selective disclosures about their company's financial situation, the company may be liable. In fact, the Securities and Exchange Commission is now monitoring the Twitter activity of publicly-traded companies.

The best way to protect a company from legal exposure is to have a policy that carefully and thoughtfully outlines what types of information may not be posted online. Furthermore, the company must consistently meet with its employees to discuss ways social networking can benefit and/or hurt the company. These policies should be short and clear so as to make them understandable, and they should contain concrete examples that will better illustrate what information must remain confidential. Given the substantial liability associated with securities law violations, this is an area that all public companies need to be attending to.

3. How To Minimize Risk

With all this in mind, here are some practical guidelines:

1) Make sure that all company confidentiality and non-disclosure polices and agreements contain a section on the use of social media including but not limited to, restricting employees from becoming "friends" with customers in their personal capacity, and providing concrete examples of information that must remain confidential.

2) Require that employees who use social networking as part of the employer's business plan maintain separate business and personal accounts.

3) As part of a company's social media policies, prohibit employees from "friending" or otherwise connecting with customers or customer contacts using their personal accounts.

4) If an employee maintains a social networking account for the company, make sure the employee sets the privacy settings to the strictest level possible.

5) Publicly-traded companies should explain to their employees the basics regarding securities laws and the restraints the laws place on them.

6) Publicly-traded companies, companies preparing to become publicly-traded, or companies that may merge into an existing publicly-traded entity should ensure its employees have signed written policies about keeping all company information confidential. One way to accomplish that goal is promulgating a policy mandating that all statements made about company financials or future endeavors can only be made publicly by the company spokesperson or another person expressly designated by the Chief Executive Officer.

D. Avoiding Liability for Personal Injury or Property Damage When Employees are Distracted

1. Please Put Down the Phone

As people are rushing from one place to another the temptation exists to use cell phones and other handheld devices while driving. The distraction caused by doing so – for phoning, texting, friending, searching or posting – is dangerous to drivers, passengers, pedestrians, bikers and others on the road.

2. The Legal Issues

If an employee is using an electronic device for company business while driving (or using a company owned device for personal business) the company may be liable for any injuries caused if the employee is in an accident. Further, the employee may be held liable and even face criminal consequences.

3. How to Minimize Risk

An employer can reduce the risks by promulgating a detailed employee policy relating to the use of cell phones or hand held devices. The policy should emphasize that employers must comply with all applicable laws regarding use of handheld devices and even if not required by law, the employer may require employees to use a hands free device.

III. RISK OF LITIGATION

Litigation is a commonly overlooked risk as many companies think that their existing policies provide them adequate protection.

A. Implementing a Litigation Response Plan

Upon engagement, litigation counsel should prepare a litigation response plan. The first step of the litigation plan is to issue a litigation hold to relevant employees of the company. Litigation counsel and the client should identify relevant employees who may have knowledge of the litigation or may have relevant documents in their possession. Second, litigation counsel should meet with client representatives, especially members of the IT department, and determine where potential responsive documents may

exist. This includes both hard copy documents and electronically stored information. Finally, litigation counsel should develop an understanding of the general document retention practices of different areas of the company. The litigation hold should state the following:

a. no hard copy documents may be destroyed
b. no electronic mail may be permanently deleted
c. all destruction of back-up tapes and other stored electronic data must stop

From the issuance of the litigation hold, all materials as they exist on that day must be maintained until the end of the litigation. The reason for this retention is that if documents are deleted, opposing counsel can reasonably make arguments for spoliation "if the documents were destroyed when the company anticipated, or reasonably should have anticipated, litigation."[3] All documents in existence at the time of the litigation should be considered potentially relevant. By treating them as such, litigation counsel will preserve the available record and have a complete and accurate universe of documents from which they can begin their review for production.

It is of the utmost importance for litigation counsel for both the plaintiffs and defendants to meet and confer to discuss how discovery will unfold in the litigation. FRCP 26(f) provides guidance for the parties to have an initial discovery conference at the beginning of the litigation, directing them to discuss issues regarding electronic data, including preservation, form of production of documents, and privilege. In this conference (and perhaps subsequent ones) it is also very helpful to create a mutually agreed-upon list of search terms and custodians that both parties will use to search the preserved electronically stored information. By agreeing upon search terms in advance of document searching, the parties will have a defined plan to which each must adhere. They have only to adhere to that plan to ensure that their document collection process has been complete. It is also strongly recommended that the parties prepare a joint stipulation outlining the agreed-upon search terms and the requirements of both parties in order to have a formal document binding each side to the discovery plan they have created. Filing with the Court will only make the discovery plan official, thereby binding the parties to a fair and equitable discovery process. In this conference, counsel should also specify in what format they would like to receive documents. Typically documents are produced in single-page image files like PDFs or TIFs accompanied by a file showing where the document breaks exist. Production of the document images is the barest response to document requests. If opposing counsel requests, you must also produce various forms of metadata, the native files of the images, and a special load file so that opposing counsel's vendor can upload the document production into their document review software. By enacting a thorough litigation hold with the client and upholding the terms of the agreed-upon discovery plan with opposing counsel, litigation counsel can avoid proceeding down a road that could lead to the selective and arbitrary searching for documents.

[3] Samsung Elecs. Co. v. Rambus, Inc., No. 3:05cv406, 2006 US Dist Lexis 50074 (E.D. Va., July 18, 2006).

B. Failure to Implement a Litigation Response Plan

When failing to implement a Litigation Response Plan, the following may occur: (1) spoliation of documents; (2) failure to collect responsive documents; and (3) neglecting to meet and confer with opposing counsel as required. The client and counsel may both be sanctioned for spoliation of documents. "Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents."[4] The responsibility lies largely with counsel to ensure that all potentially relevant documents are reviewed for production. It is no longer enough to preserve documents; litigation counsel must "proactively ensure compliance."[5] It is also possible that by failing to acquire a detailed knowledge of the location and status of all potentially relevant documents, the client may not collect all relevant documents. This could lead to missing potentially important evidence that could help the case, or, being held liable for spoliation of documents or the intentional withholding of responsive documents for not searching all files and ESI for relevant documents. By not meeting and conferring with opposing counsel, you lose the opportunity to limit the scope of discovery. Without meeting with opposing counsel to gain their input and to determine appropriate scope and search terms, creates the risk of an extremely costly discovery process and increases the likelihood of neglecting to produce relevant documents.

IV. HUMAN RESOURCES USE OF SOCIAL MEDIA

As social media becomes more prevalent, any human resources director, with help from Google, can research a prospective employee's online presence. Some of the key questions facing companies include: (1) whether a company should do online research of prospective employees; (2) how they can do so legally; and (3) what are the inherent risks of conducting online research of prospective employees.

A. Hiring Decisions Made With Social Media

If you have ever visited social media sites, you probably have encountered inappropriate pictures and postings. Whether it is a picture depicting inebriated people or a comment lambasting work, the *faux pas* made online are rampant. As an employer, a company may have legitimate reasons to want to see these postings as a window into the judgment of a prospective employee. Searching social media, however, will often provide additional information that can lead a company down a slippery slope, because it may reveal the applicant's race, marital status, disability, pregnancy, or sexual preference. Because federal, state, and local laws regulate the process of making employment decisions, employers are restricted on what information they can request on applications and in interviews. How they use such information in evaluating candidates, thus leads to

[4] Zublake v. UBS Warburg LLC, 229 FRD 422, 434 (SDNY 2004).
[5] Best, Richard E., "E-Discovery: What Courts Expect of Counsel," "Judge's Prospective," *California Civil Litigation Reporter*, Vol. 28, No. 5, page 201, Continuing Education of the Bar, October 2006.

a potential conflict when social networking sites reveal protected information. It is unlawful to refuse to hire or to terminate an employee because that person is a member of a protected class based on race, gender, age, disability, and other characteristics. However, on social media sites, this information is obtained easily. For example, a candidate's protected class may appear in the user's social networking profile or in photos and videos. Despite recent efforts to make social networking more private, a user's profile picture is usually available to the general public, often revealing race, sex, and age. If a user has not restricted access through privacy settings, an employer may also see certain traits revealed through postings or what groups the user likes, including political preferences or sexual choice preferences.

Concerns about whether the human resources department could, or even should, access social networking sites has led some companies to create restrictive policies limiting or prohibiting use of these sites for investigating potential employees. For example, one company recently implemented a policy that restricts all use of social networking sites in recruiting and hiring new employees, including by outside recruiters. Information gleaned from social media sites is impossible to filter, and the policy is aimed at preventing its recruiters from coming across information that employers are not legally entitled to consider in making employment decisions.

However, company-wide policies to block the use of social media in the hiring process are not the norm. Instead, the trend among employers is towards increasing reliance on social networking sites to screen job applicants. A January 2010 Microsoft study surveyed recruiters from four countries, including the United States, and concluded that a person's online reputation has become "a significant factor in the making of hiring decisions."[6] The study also showed that 79 percent of the surveyed hiring managers and recruiters in the United States had considered online information about job candidates as part of the hiring process. Of those recruiters, 70 percent said they have rejected applicants because of what they found online.

How does an employer then navigate all the potential issues involving hiring decisions and social media?

Under most anti-discrimination laws, it is not illegal for an employer to learn before an interview that an individual is a member of a legally protected class. However, employment laws mandate that all individuals be provided equal, nondiscriminatory treatment throughout the hiring process. If a representative of the employer surmises certain protected traits through an applicant's social media presence, that knowledge could increase the risk of actual discrimination, or give the appearance that the employer was discriminatory in the hiring process. It may even lead to inadvertent discrimination based on inherent biases. To minimize the risk of exposure to discrimination claims,

[6] Cross-Tab Marketing Services, Online Reputation in a Connected World, 3, available for download at http://go.microsoft.com/?linkid=9709510, last accessed Sept. 14, 2010.

employers should train their HR staff to focus on an applicant's qualifications, which may be difficult to do if an individual's social media profile is particularly revealing.

Another risk of discrimination claims arises if human resources staff look at social networking sites to vet certain candidates but not all candidates. There may be a suspect reason why HR personnel elect to research certain applicants online and not research others. The reasons why this research is conducted selectively may be difficult to defend if challenged in a discrimination suit. Even inadvertently treating members of a protected class differently than others may subject an employer to a disparate treatment claim, which makes it crucial that company personnel follow the same steps and same criteria for hiring. Another potential risk for employers arises if hiring decision makers evaluate information found on social networking sites in a different way for different categories of applicants. All of these concerns are further amplified when some applicants have different privacy settings for their online profiles, preventing potential employers from seeing any information, while granting unfiltered access to others.

Social media information that is reviewed by HR also will become part of an applicant's record that the employer is legally obligated to preserve. Employment laws require employers to maintain applications, resumes, and other records from the hiring process one year from the time the record was created or from the time an employment action associated with that record takes place, whichever is later.[7] Federal contractors are required to maintain additional information for a period of two years.[8] Therefore, if an employer uses social media to evaluate a job seeker's qualifications, that site becomes an employment record, just like a resume or application attached to an e-mail.

Employers can also run the risk of running afoul of the law by improperly accessing social media profiles. Social media sites are regulated on the Internet through the Stored Communications Act ("SCA").[9] Under the SCA, it is a crime to intentionally access a facility through an electronic communication service without authorization or by exceeding an authorization. It is also a crime under the SCA to obtain, alter, or prevent access to electronic communication while it is in electronic storage. The SCA also provides for a private cause of action by an aggrieved plaintiff for injunctive relief, damages, and attorney's fees. Punitive damages are also available. If a company and its representatives are not authorized to view an applicant's or employee's online presence, the company may not resort to alternative means to access that information. However, an online presence is readily available on the internet; a company does not need authorization to access it. Relying upon the information, even if it is accessible, may still give rise to liability.

[7] 29 C.F.R. 1602.14 (1991).
[8] 41 C.F.R. 60-1.12 (2005).
[9] 18 U.S.C. §2701, *et seq*.

1. Current Issues of Social Media and Litigation

Even if you are not a user, company executives need to understand the basics of the popular online social media sites. For example, distinction between Facebook messages and wall posts may trigger different access rights during the discovery phase of civil litigation. In *Crispin v. Christian Audigier, Inc.*, the court grappled with the potential variations in the types of social networking communications.[10] Crispin, an artist, sued apparel manufacturer Christian Audigier for copyright infringement based on an oral license agreement to place Crispin's tattoo-inspired artwork on t-shirts and other street wear. Crispin alleged that Audigier attributed the plaintiff's artwork to a different artist and used the artwork on products like pet accessories and luggage, items purportedly outside the scope of the oral license. During discovery, Audigier issued a subpoena to Facebook and another social networking site seeking Crispin's basic subscriber information, all communication between Crispin and another artist, and all communications that referred to Audigier and the other defendants. The defendants contended these communications were relevant in determining the nature and terms of the oral license if one existed. Crispin's attorneys filed a motion to quash the subpoena, arguing that these Facebook communications were protected from discovery by the Stored Communications Act, which prevents third-party providers of communications services from disclosing electronic communications.

After a federal magistrate judge initially ruled against Crispin, U.S. District Judge Margaret Morrow, on review of the magistrate's order, reversed in part and vacated in part. In a lengthy opinion, Judge Morrow recognized the nuances of social networking communication as it relates to the Stored Communications Act. First, Judge Morrow engaged in an extended analysis of the Stored Communications Act and case law, finding that Facebook and another social networking site provided "electronic communications services" and "remote computing services" under the Act. As such, private communications on Facebook were awarded protection from disclosure. Judge Morrow noted that Facebook Messages were analogous to e-mails and remain "inherently private such that stored messages are not readily accessible to the general public." To that extent, the Judge reversed the magistrate's order and quashed the subpoena. However, since wall posts could be public or private depending on each particular user's privacy settings, the Judge vacated that portion of the magistrate's order and remanded the case to make more evidentiary findings on the level of privacy the plaintiff chose for his wall posts.

Although the issue is far from settled, Judge Morrow's opinion suggests that at least in some courts, user designated Facebook privacy settings play a role in whether wall posts are discoverable under the *Crispin* decision. To the extent that wall posts are accessible to the general public, the information could be discoverable, but wall posts made behind a user-controlled privacy wall would be protected from discovery in civil litigation under the Stored Communications Act.

[10] No. CV 09-09509 MMM (JEMx), --- F.Supp.2d ----, 2010 WL 2293238, (C.D. Cal. May 26, 2010).

Not all courts have followed that approach. For example, state courts in New York and Pennsylvania have been less deferential to a user's self-selected privacy settings in assessing the discoverability of social network postings. In *Romano v. Steelcase, Inc., et al.*,[11] the Supreme Court of New York, Suffolk County held that because public sections of a users social networking site showed information contrary to her claims and deposition testimony in a personal injury case, it was likely the more private portions had relevant information as well. The *Romano* court said any privacy interests were outweighed by the defendants' need for the information. The court, in reaching its decision, concluded that the social networking sites did not guarantee absolute privacy, so there was no reason to expect it.

Similarly, in *McMillan v. Hummingbird Speedway, Inc.,*[12] the trial court in Jefferson County Pennsylvania required a plaintiff in a personal injury case to provide Facebook and MySpace user names and passwords to defendants' attorneys for read-only access, barring counsel from sharing the log-on information. The court determined that again users cannot reasonably expect privacy on social networking sites and that when users post information that is, "pertinent to issues raised in a law suit in which they [are a party] the search for truth should prevail…"

B. Human Resources Review of Current Employees

Social media is a place for individuals to express themselves and oftentimes, vent about their work, employers, customers, or company decisions. Some companies actively review their employees' social media presence on a regular basis. In contrast, sometimes, an employer stumbles upon a comment by an employee that disparages the company or its customers. Either way, a disparaging post may result in the posting employee's dismissal.

In the past few years, there have been several high profile firings occurring after employees made online statements. In one case, Google fired an employee who was keeping a blog chronicling his experiences at Google. Google asked the employee to remove information the company deemed to be sensitive and then discharged him after eleven days of employment. In another case, a part-time Philadelphia Eagles employee who worked at the football stadium, vented on his Facebook page about the decision to let popular player Brian Dawkins sign with another team. The employee's post that he was "[expletive] devastated about Dawkins signing with Denver . . . Dam Eagles R Retarted!!" led to his termination. Similarly, the Pittsburgh Pirates baseball team fired one of its employee mascots who complained on Facebook about the Pirates twenty-year futility, but the Pirates, unlike the Eagles, rehired the employee after public backlash about the decision.

[11] *Romano v. Steelcase, Inc., et al.*, 2010 N.Y. Sup. Op. 20388, 2010 N.Y. Misc. Lexis 4538
[12] *McMillan v. Hummingbird Speedway, Inc.,* 2010 Pa. D&C. Dec. Lexis 270

While there do not appear to be publicly reported legal proceedings flowing from these incidents, the incidents generate publicity that may paint organizations in bad light, and may lower employee morale.

Companies must also be mindful of the SCA when monitoring their current employees. In *Konop v. Hawaiian Airlines*, a company vice president accessed an employee's secure website using the log-in information of another employee who gave it to the vice president for this purpose. The vice president found disparaging comments about the company on the site and threatened to sue the employee for defamation. The employee sued under the SCA and the court found that the company violated the SCA. [13]

A second case of a company improperly accessing employees' social media presence also resulted in a verdict for the employees. In *Pietrylo v. Hillstone Rest. Group*, two plaintiffs sued their ex-employer under the SCA after management accessed a chat group on MySpace where employees of Houston's would vent about the restaurant.[14] A jury found for the employees and awarded punitive damages. The court dismissed the employer's post-verdict motions because a jury could reasonably infer that management coerced a fellow employee into providing access and that the access was not authorized under the circumstances.[15]

1. Developing a Strong Human Resources Policy

With all of this in mind, here are some practical guidelines:

1) Develop a human resources policy on the use of social media in the hiring process. It does not have to be an outright ban on looking at a candidate's internet presence, but it should detail a list of what is appropriate and what is impermissible.

2) Employers need to train human resources staff about applicable local, state, and federal law, including appropriate responses when protected traits are disclosed during recruitment, whether through social media or otherwise. The employer must focus on the person's qualifications for the job.

3) Policies and training measures should be regularly monitored and updated to reflect current law and good practice.

4) If an employer uses social media to evaluate a candidate, it should use similar scrutiny on all candidates for the job to avoid a disparate treatment claim.

5) An employer should establish that it has obtained an applicant pool through a process that includes all qualified applicants.

---

[13] 302 F.3d 868 (9th Cir. 2002)
[14] No. 06- 5754 (FSH), 2008 U.S. Dist. LEXIS 108834 at *1-3 (D.N.J. July 25, 2008), *post-verdict motions denied by,* 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 25, 2009).
[15] 2009 U.S. Dist. LEXIS 88702 at *9.

6) If an employer is using social media in a hiring decision, the version of that page should be saved as a hard or electronic copy for the regulated period in case there is a claim.

7) Information found on a social networking site might not be reliable.

8) Ensure that human resource staff and other employees know that they cannot obtain electronic information that they are not authorized to view.

9) Employment policies should include a paragraph that personal use of social media should uphold the honor and dignity of the company and should not paint the company in bad light.

V. PROFESSIONAL RESPONSIBILITY AND ETHICAL CONSIDERATIONS FOR LAWYERS[16]

A. Ethical Issues Relating to Promoting Yourself or Your Practice

Many lawyers are relying upon social media to promote themselves and their firms. In doing so, it is important not to overlook the ethical obligations relating to self promotion and advertising. Given the often relaxed and spontaneous nature of social networking, it is easy to overstate your expertise or experience because you are not being as thoughtful as you may be in other forms of communications. However, the same standards of accuracy and integrity apply as in any other setting. For example, Model Rules 7.1 and 7.2 provide important guidance.

Information About Legal Services
Rule 7.1 Communications Concerning A Lawyer's Services

A lawyer shall not make a false or misleading communication about the lawyer or the lawyer's services. A communication is false or misleading if it contains a material misrepresentation of fact or law, or omits a fact necessary to make the statement considered as a whole not materially misleading.

Information About Legal Services
Rule 7.2 Advertising

(a) Subject to the requirements of Rules 7.1 and 7.3, a lawyer may advertise services through written, recorded or electronic communication, including public media.

[16] This paper relies principally on the ABA Model Rules of Professional Conduct as a guide (as some jurisdictions follow the Model Rules more closely than others, but the spirit of the Model Rules provides a meaningful yardstick to begin the analysis).

(b) A lawyer shall not give anything of value to a person for recommending the lawyer's services except that a lawyer may

(1) pay the reasonable costs of advertisements or communications permitted by this Rule;

(2) pay the usual charges of a legal service plan or a not-for-profit or qualified lawyer referral service. A qualified lawyer referral service is a lawyer referral service that has been approved by an appropriate regulatory authority;

(3) pay for a law practice in accordance with Rule 1.17; and

(4) refer clients to another lawyer or a nonlawyer professional pursuant to an agreement not otherwise prohibited under these Rules that provides for the other person to refer clients or customers to the lawyer, if

(i) the reciprocal referral agreement is not exclusive, and

(ii) the client is informed of the existence and nature of the agreement.

(c) Any communication made pursuant to this rule shall include the name and office address of at least one lawyer or law firm responsible for its content.

B. Ethical Issues Relating to Communications with Clients

Under the rules of professional conduct, attorneys are expected to keep clients informed and also to maintain client confidences. As explained below, this is not the same as attorney-client privilege. Here is how the Model Rules treats these issues:

Client-Lawyer Relationship
Rule 1.4 Communication

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

Client-Lawyer Relationship
Rule 1.6 Confidentiality Of Information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or

(6) to comply with other law or a court order.

C. Ethical Issues Relating to Communicating with Prospective Clients, Witnesses and Others

Our responsibilities as counsel are not limited to our clients. We have ethical duties to others with whom we have contact in our professional capacity. For example, not all prospective clients with whom we consult initially, actually become our clients. We may elect not to undertake the engagement or the client may elect not to engage us as counsel. However, during that assessment process, we may learn confidential information about the client. Under the Model Rules, we are required to keep those confidences:

Client-Lawyer Relationship
Rule 1.18 Duties To Prospective Client

(a) A person who discusses with a lawyer the possibility of forming a client-lawyer relationship with respect to a matter is a prospective client.

(b) Even when no client-lawyer relationship ensues, a lawyer who has had discussions with a prospective client shall not use or reveal information learned in the consultation, except as Rule 1.9 would permit with respect to information of a former client.

(c) A lawyer subject to paragraph (b) shall not represent a client with interests materially adverse to those of a prospective client in the same or a substantially related matter if the lawyer received information from the prospective client that could be significantly harmful to that person in the matter, except as provided in paragraph (d). If a lawyer is disqualified from representation under this paragraph, no lawyer in a firm with which that lawyer is associated may knowingly undertake or continue representation in such a matter, except as provided in paragraph (d).

(d) When the lawyer has received disqualifying information as defined in paragraph (c), representation is permissible if:

(1) both the affected client and the prospective client have given informed consent, confirmed in writing, or:

(2) the lawyer who received the information took reasonable measures to avoid exposure to more disqualifying information than was reasonably necessary to determine whether to represent the prospective client; and

(i) the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom; and

(ii) written notice is promptly given to the prospective client.

Thus, this rule impacts our use of social media, just as if the confiding party was an actual client. The attorney must exercise the same care not to divulge information via social media and not to assume that self selected privacy designations will be enough to keep information from disclosure.

Another issue relates to social media and witnesses or third parties – namely, being truthful and not deceiving others. For example, unfortunately, some lawyers have posed as someone else or asked an employee or designee to mislead potential witnesses to gain information needed for a case. Plainly, this is improper and an ethical violation.

Transactions With Persons Other Than Clients
Rule 4.1 Truthfulness In Statements To Others

In the course of representing a client a lawyer shall not knowingly:

(a) make a false statement of material fact or law to a third person; or

(b) fail to disclose a material fact to a third person when disclosure is necessary to avoid assisting a criminal or fraudulent act by a client, unless disclosure is prohibited by Rule 1.6.

D. Ethical Issues Relating to Confidentiality and Attorney-Client Privilege

Under the ethical rules governing attorneys' conduct, there is an affirmative obligation to preserve client confidences. That obligation may overlap with, but is not identical to attorney-client privilege, which is an evidentiary rule that generally protects confidential information from compelled disclosure if the information is conveyed to counsel for the purpose of obtaining legal advice and the privilege is not waived. Information may be confidential, but not be protected by privilege if those additional requirements are not met. Further, rules of professional conduct and attorney client privilege do not protect disclosure made for certain improper purposes, such as in furtherance of certain types of crimes. The standards vary from jurisdiction to jurisdiction.

The proliferation of electronic communication methods and the frequency and speed with which we all use e-communications creates greater risk that confidential information from clients will be inadvertently revealed. The Federal Rules of Civil Procedure and the applicable state court rules provide some safe havens for counsel. However, that is beyond the purview of this program. Instead, we focus on how use of social networking increases the risk for counsel. It is not uncommon for social media users to post information on their pages, such as on FaceBook or LinkedIn, with the

expectation that it is private. However, individual privacy designations, can be overcome and when lawyers include client confidences on social media, this amounts to a violation of the duty to retain confidentiality and can expose the posting lawyer to ethical sanctions and malpractice liability if it causes harm to the subject client.

E. Ethical Issues Relating to Airing Your Gripes and Criticism on the Internet

In addition to the risk of being sued for defamation, which applies to lawyers, except for certain immunity for court filings and statements in court, lawyers have to be sensitive to postings even if they are truthful and not defamatory. For example, postings criticizing judges or opposing counsel, even if they are truthful, opinion or otherwise not defamatory under applicable law, can still get a lawyer in trouble. Careful attention should be given to the boundaries of Model Rule 3.6.

Advocate
Rule 3.6 Trial Publicity

(a) A lawyer who is participating or has participated in the investigation or litigation of a matter shall not make an extrajudicial statement that the lawyer knows or reasonably should know will be disseminated by means of public communication and will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter.

(b) Notwithstanding paragraph (a), a lawyer may state:

(1) the claim, offense or defense involved and, except when prohibited by law, the identity of the persons involved;

(2) information contained in a public record;

(3) that an investigation of a matter is in progress;

(4) the scheduling or result of any step in litigation;

(5) a request for assistance in obtaining evidence and information necessary thereto;

(6) a warning of danger concerning the behavior of a person involved, when there is reason to believe that there exists the likelihood of substantial harm to an individual or to the public interest; and

(7) in a criminal case, in addition to subparagraphs (1) through (6):

(i) the identity, residence, occupation and family status of the accused;

(ii) if the accused has not been apprehended, information necessary to aid in apprehension of that person;

(iii) the fact, time and place of arrest; and

(iv) the identity of investigating and arresting officers or agencies and the length of the investigation.

(c) Notwithstanding paragraph (a), a lawyer may make a statement that a reasonable lawyer would believe is required to protect a client from the substantial undue prejudicial effect of recent publicity not initiated by the lawyer or the lawyer's client. A statement made pursuant to this paragraph shall be limited to such information as is necessary to mitigate the recent adverse publicity.

(d) No lawyer associated in a firm or government agency with a lawyer subject to paragraph (a) shall make a statement prohibited by paragraph (a).

In addition, many lawyers have faced disciplinary action and lost their jobs due to intemperate postings about judges before whom they have appeared. Many state disciplinary boards have determined that lawyers, as officers of the court, must sacrifice some free speech protection they might feel they should have. Lawyers need to be especially sensitive to what they post on social media sites. The consequences for going too far can jeopardize professional standing.

F. Professional Responsibility and Malpractice Avoidance When Representing Clients in Litigation or in Anticipation of Litigation

Section III, above, Risk of Litigation, addresses in detail the professional responsibility obligations of counsel representing clients that are in suit or have a reasonable expectation that a potential dispute may escalate to full blown litigation. In these situations, both counsel and the client have an obligation to assure that the documents and information relevant to the matter are properly preserved. Failure to assure that the potentially discoverable information is available later, can limit the client's options – either ability to pursue claims or establish defenses. If counsel fails to advise a client as to these obligations, fails to alert potential adverse parties of a duty to preserve, or fails to advise on a litigation response plan, counsel may face professional malpractice liability for harm to the client flowing from such failure.

VI. CONCLUSION

When representing clients, we have an obligation to be competent and diligent. According to the Model Rules, these are very basic tenets:

> ***Client-Lawyer Relationship***
> **Rule 1.1 Competence**
>
> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
>
> ***Client-Lawyer Relationship***
> **Rule 1.3 Diligence**
>
> A lawyer shall act with reasonable diligence and promptness in representing a client.

As the world is increasingly dominated by social media, effective representation of clients requires at least a working knowledge of these legal issues and the attentiveness to them needed to avoid exposing yourself or your clients to liability. To do so, ensure that key executives understand how and why people and companies use social media. In addition, appreciate that your law firm or legal department is also an employer and has the same obligations, plus additional responsibilities under the rules of professional conduct. Even if your company is not using social media, you may have customers, suppliers, and vendors who are actively participating in social networking websites. Understanding their business plan may create new opportunities for you. For example, a large company recently had an RFP for lawyers, where law firms needed to tweet their proposals using Twitter.

Take the time to explain to all the employees the unique business risks that can occur using social media, including, but not limited to, inadvertent disclosure of highly confidential information, defamation, or risks to intellectual property infringement.

A company including a law firm should have a clear, concise, comprehensive, and reasonable policy regarding social media and social networking. It is impossible for a company to keep its employees away from social media, and in the long run, an austere view toward these websites may shut off new opportunities. The policy should set out the benefits of social media and the associated risks. Providing examples of what is and what is not appropriate will help employees further understand company policies. The company should make clear that all employees, even on their personal social media accounts, are to uphold the integrity and honor of the company and not cast the company in disrepute. This includes not using obscenities, slurs, or insults and refraining from making any negative comments about the company.

Policies are only as good as they are relevant to current standards. Social media and social networking trends evolve quickly. Policies should be consistently reviewed and updated as change occurs. Policies work best when they are proactive and not reactive to these changes.

A company also must ensure that its policies are evenly enforced. A company that does not enforce its policies is in as bad a position, if not worse, than a company without a policy. The same applies to lawyers and their firms. Lawyers are often cavalier about applying the law to themselves or their workplaces. Failure to do so can expose the lawyers and the firm to ethical violations and professional malpractice claims.