Use of Social Media in Employment: Should I Fire? Should I Hire?

Kellie A. O'Shea
Creative Services Inc.

Follow this and additional works at: https://digitalcommons.ilr.cornell.edu/chrr
Part of the Business and Corporate Communications Commons, and the Human Resources Management Commons
Thank you for downloading an article from DigitalCommons@ILR.
Support this valuable resource today!

This Article is brought to you for free and open access by DigitalCommons@ILR. It has been accepted for inclusion in Cornell HR Review by an authorized administrator of DigitalCommons@ILR. For more information, please contact catherwood-dig@cornell.edu.
Use of Social Media in Employment: Should I Fire? Should I Hire?

Abstract
[Excerpt] It used to be that writing on someone's wall would get you in trouble, tweets were only for the birds, and poking was rude. The advent of social media has revolutionized the way we communicate as a society, and wireless technologies allow us to do so faster than we ever thought possible. The lines between personal and professional personas have merged into an indistinguishable haze of likes, links, and posts, making transparency an everyday issue.

Keywords
HR Review, Human Resources, social media, employment

Disciplines
Business and Corporate Communications | Human Resources Management

Comments
Suggested Citation:
USE OF SOCIAL MEDIA IN EMPLOYMENT: SHOULD I HIRE? SHOULD I FIRE?

Kellie A. O’Shea

Introduction

It used to be that writing on someone’s wall would get you in trouble, tweets were only for the birds, and poking was rude. The advent of social media has revolutionized the way we communicate as a society, and wireless technologies allow us to do so faster than we ever thought possible. The lines between personal and professional personas have merged into an indistinguishable haze of likes, links, and posts, making transparency an everyday issue. Although the recession lingered, employers are starting to show signs of optimism as they begin to hire again. This is good news for job seekers, however, the way employers go about filling these positions is much more selective than was seen in the “war for talent” just a decade ago. In order to make the best hiring decision, employers are looking far beyond the resume to learn more about their applicants and employees—including reviewing their personal social networking sites. This new trend has launched a web of legal issues that the courts have just begun to unravel.

Employers’ review of applicants’ and employees’ social media sites can be an extremely valuable tool, but should be used in a manner consistent with lawful hiring and separation practices. When used properly, social media can be a powerful means of candidate identification, selection, and retention.

However, employers must have comprehensive and compliant social media policies that are not overly broad, and which address privacy, lawful access, accuracy, equal protection, permissible and impermissible activities, and conduct within employment practices.

Background

The explosive growth of social media in the past decade has promoted instant and expansive communication to a broad network of people in a quick and convenient way. According to Facebook, there are 845 million active users of their site.¹ In March of 2011, LinkedIn reached the 100 million user milestone.² Other favorite social media sites with users in the tens of millions include MySpace, Twitter, YouTube, and Flickr.

Social media has pioneered its own path into the cultural stream of consciousness, but has left in its wake a web of questions revolving around the issues of modern expression and privacy. Getting at the center of this web involves untangling multiple layers of complex statutes, case law, and agency guidance in a way which balances the pillars of freedom of speech and the at-will employment doctrine. This article is designed to review relevant aspects employers should consider in using social media as part of the hiring or firing process. Although there is no perfect application of the law to society’s new technologies, Part I of this article provides a list of considerations, as well as a threshold of wrongful use, based on statutes, case law, and agency guidance. Part II introduces privacy considerations and employers’ requirements for legal, permissible access and accuracy. Part III discusses potential disparate impact in the use of social
media in recruiting employment candidates. Part IV explores the use of social media in terminating employment and establishes trends from a number of decisions issued by the National Labor Relations Board (NLRB or “the Board”). Part V discusses how employers’ social media policies relate to those NLRB decisions.

Part I

Privacy

The First Amendment of the Constitution states, “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.” As strict constructionists would promptly point out, absent from the First Amendment is the word “right to privacy.” Although there is no “right” to privacy granted under the First Amendment, there are certain privacy protections afforded. Case law suggests that “specific guarantees of the Bill of Rights have penumbras” of privacy that extend to certain areas and situations. The Court reasons that various guarantees within the amendments create zones of privacy. The question becomes whether an applicant or employee has an expectation of privacy in their personal social media persona.

Privacy settings and controls allow users to reduce exposure; however, certain information is typically always publicly available, such as their name, profile picture, and networks. Even with the utmost precautions in making profiles private (which many would argue defeats the purpose of a networking profile), social media sites often provide notice to users that they do not guarantee the privacy of the information. LinkedIn specifically provides notice in their privacy policy that because the internet is not a “100% secure environment,” the company cannot ensure the security of any information submitted to their website, nor can they guarantee that “information not be accessed, copied, disclosed, altered, or destroyed by breach of any of [their] physical, technical, or managerial safeguards”. Even with limited privacy disclosure, users still maintain an expectation of privacy in certain circumstances.

One trend is for employers to ask applicants or employees for their login credentials so that the employer may access their social networking site directly. This approach has been met with staunch resistance both by application providers, legislators, and privacy rights activists. Facebook has created a new Statement of Rights and Responsibilities which states it is a violation to coerce or force users to share private information contained in a personal, nonpublic Facebook page. Facebook strongly discourages the practice, reserving legal action as a potential remedy if efforts with policy makers and stakeholders prove futile. Legislators are also strongly reacting to the new practice, finding it an objectionable invasion of privacy. Before an employer, or anyone for that matter, accesses a personal social media site, they must have permissible and legal access to the information.

Permissible and Legal Access

Users of social media sites who leave open, unfettered public access to their sites or invite or accept potential employers or companies to “friend” or “connect” grant permission of access and should expect little if any expectation of privacy with that employer or company. There are also less permissive ways of gaining access to personal social media pages such as hacking or using another’s authorized login credentials. Although the court may not apply criminal sanctions in some situations, the courts do not view these tactics favorably.
In terms of hacking, the Computer Fraud and Abuse Act imposes criminal sanctions on unauthorized access by computer.\textsuperscript{14} In order to secure a conviction under the Act, the government must establish that the defendant intentionally obtained information by accessing and/or exceeding authorized use of a computer involving interstate or foreign commerce.\textsuperscript{15}

Additionally, creating alias personas on social media sites to gain access to employee or applicant information poses its own set of potential liabilities. Although courts have held that the Void-for-Vagueness Doctrine may minimally protect employers against criminal convictions for violations of social media providers’ terms of service, employers could face criminal penalties for unauthorized or exceeding authorized access to social media provider computers.\textsuperscript{16}

Lastly, courts have reviewed the employer practice of “borrowing” authorized login credentials and have decided that employers are subject to criminal sanctions if they gain unlawful access to stored communications.\textsuperscript{17} Gaining access to a personal social media site through utilizing another user’s username and password will not skirt the authorized user requirement.\textsuperscript{18}

Training talent acquisition representatives on the importance of voluntary, non-coercive permission and legal access to view personal social media pages will reduce the risk of criminal liability. Although it is recommended to devise a recruiting strategy that distinguishes the recruiting function from the hiring decision function, outsourcing recruiting efforts which include the review of social networking sites, will not necessarily alleviate the vicarious liability of that employer under the theory of respondeat superior.\textsuperscript{19} An employer can be liable in tort for the acts of its employees as well as independent contractors if the employer controls certain activities.\textsuperscript{20}

Accuracy

Once an employer has permissibly and legally accessed information in a personal social networking site they should ensure the information is both accurate and related to the person for whom they are searching. For example, is this the same John Smith who applied for a position? It is also worth considering whether the person described on the social media site established the account themselves, or if someone else created their page without their permission or knowledge.

To address some of these challenges, employers will sometimes outsource the social media site review to a third party Consumer Reporting Agency (CRA). If a CRA is engaged in a search for information regarding personal character or reputation on an applicant or employee’s social media site, the employer is required under the Federal Fair Credit Reporting Act (FCRA) to ensure accuracy of the information.\textsuperscript{21} The FCRA requires, in part, that the employer have a clear and conspicuous written disclosure from the applicant or employee in order to procure a consumer report which may include information from a social media site.\textsuperscript{22} The FTC announced in an opinion letter that in certain circumstances in which a CRA has investigated an applicant or employee’s social media sites in compliance with applicable provisions of the FCRA, the Bureau of Consumer Protection Division of Privacy and Identity Protection found no FCRA violations. “The FTC has, however, made note that although a CRA may comply with FCRA provisions by conducting social media site searches, they may still be in violation of other laws, such as equal employment opportunity violations.”\textsuperscript{23}

There is another cause for concern if an employer is receiving consumer reports containing social media or other information via mobile apps. The Division of Privacy and Identity Protection of the FTC recently announced that these mobile apps may violate the FCRA.\textsuperscript{24} Several companies received directed letters of the warning.\textsuperscript{25} Employers should not rely on disclaimers provided by
Part II - Recruiting Candidates – Should I Hire?

Employers face two major questions when they decide to use social media in recruitment. Firstly, how does social media impact candidate sourcing and statistics? Secondly, what is the impact of viewing candidate information on a social networking site?

To answer the first question, it is important to understand that although the fastest growing segment of the population adopting social networking is over the age of 35, a disconnect in demographics still remains. While 32% of the population between the ages of 23 to 35 participated in social networking, only 20% of the population between the ages of 50 to 65 participated—with a mere 5% participating aged 65 and up. In addition, statistics show that race and gender also play a role in social networking site demographics. On MySpace 70% of users are white, and on LinkedIn there are nearly twice as many men (63%) as women (37%). Studies also show that some social networking sites attract users that hold less formal education than others. This is important because it could potentially fuel disparate impact cases of discrimination even when the employers had no subjective intent to discriminate when they decided to use social media outlets. To avoid pitfalls of potential statistical traps using social media for recruiting, employers are urged to use a variety of sourcing strategies across multiple social media sites in addition to traditional avenues to attract a diverse applicant pool.

Concerning the second question on the impact of viewing candidate information via social networking sites, employers should be forewarned that information on these sites often includes a plethora of statistical characterizations about the applicant including those protected by Title VII and ADEA. Employers with permissible, non-coercive, legal access to social networking profiles who take reasonable steps to ascertain accuracy need to be aware that a picture can be worth a thousand demographic words.

According to a recent social recruiting survey by Jobvite, eighty-nine percent of companies said they were using or planned to use social media in hiring. There is evidence that demographic data thrives in cyberspace. Consider, for instance, that there are over sixty million status updates posted to Facebook daily and three billion photos uploaded each month. In today’s world of electronic storage and internet protocol (IP) address tracking, proving an employer was a visitor to a personal social networking site is easier than ever before. Simply viewing demographic data on an applicant or employee’s social networking site may be enough to flag a particular hiring practice that would survive a motion for summary judgment and begin the costly course of litigation.

Part III – Current Employees – Can I Fire?

Equal protection violations are not limited to applicants for employment. Terminated employees can also file Title VII or state claims when demographic data gleaned from a social networking site proves to be the catalyst for termination.

In situations where employees are terminated because of information employers gained from the workers’ personal social networking page, employers must look closely to both an employee’s conduct and their own policies in determining whether termination is legal under the
circumstances. The National Labor Relations Board (NLRB) is on the front lines of the virtual wave of social media suits, applying law that was enacted long before the technology existed.37

NLRB Decisions

Recently, the NLRB was forced to weigh in on the impact of social media on employees’ rights and unfair labor practices.38 The NLRB has identified social media tools to include text, audio, video, images, podcasts, and other multimedia communications.39 Of twenty cases dealing with the issue of whether an employee’s conduct via social media was protected as “concerted activity” (and therefore protected under Section 7 or Section 8(a)(1) of the NLRA), the NLRB found that in half of the cases the employer discharged the employee unlawfully. Of eight cases on the question of policy, seven employers were found to have unrevised policies that were overly broad.40

As Applied to Social Media

The legal theories behind established employment policies have not changed much over the years—however the way in which we communicate both at work and at home has dramatically transformed. The challenge is to apply traditional laws to today’s instant, casual, broadcast style of social networking communication in terms of concerted activity. Prior to 2004, courts were not concerned with how many “likes” an employee received about their work-related comment on their “wall”. Likewise, courts did not have to consider an employee’s ability to reach an average of 634 people in the click of tweet.41 In order to apply traditional legal standards, we must address the types of conduct that employers can consider in potentially adverse employment decisions. Employers need to be aware of protected concerted activity before taking any adverse action against information posted on a social networking site.

What is Protected Activity?

It is well established that important terms and conditions of employment include wages, benefits, and working conditions.42 Employers violate Section 8(a)(1) by restricting, through policy or handbook instruction, employees’ right to discuss with employees and/or non-employees important terms and conditions of employment.43

It is noteworthy that under the Sarbanes-Oxley Act of 2002, public company employees also have whistleblower protection when reporting circumstances of fraud under 18 U.S.C. §1341, §1343, §1344, or §1348.44 The party must first report to statutory defined authorities, such as federal agencies, member of Congress, and/or supervisors.45 Before adverse decisions are made, employers should consider first if the conduct or posting was protected activity.

What is Concerted Activity?

According to the NLRB Reports, using social media for collective dialog and shared concerns about important terms and conditions of employment are concerted, and therefore protected, activities.46 In recent NLRB social media cases the Board has found employee conduct on social networking sites or public message boards to be protected concerted activity in eleven of twenty cases.47 In all eleven cases the employee “engaged in, with, or on the authority of other employees, and not solely by and on behalf of the employee himself” under the Meyers test. The critical inquiry in identifying concerted activity is the link between the employee and their coworkers, and the actions of the employee on behalf of the group to achieve common goals.48 Concerted activity measured by social media standards is supported by communication including
but not limited to “thank you for having faith in me & helping my voice be heard!,” “keep fighting the good fight;” “great letter;” “thanks for helping us stay informed;” and “like the comment.” The Meyers test also extends to early phase of concerted activity which “in its inception involves only a speaker and a listener.” Employers should also be cautious not to discredit concerted activity just because there is no online reaction or support. Content posted on a social networking site should be closely reviewed under the Meyers test and weighed against the modified Atlantic Steel test for protected concerted activity and employers should proceed with caution if the topic involves terms and conditions of employment protected by Section 7.

Section 7 does not define the Meyers test as requiring interaction with other employees; however, courts have generally limited the actions of a single employee to be concerted activity “only when (1) that in which the lone employee intends to induce group activity, and (2) that in which the employee acts as a representative of at least one other employee.” Preemptive strikes to curtail possible concerted activity will likely violate Section 8(a)(1) by creating a “dam...at the source of supply.”

An employee, however, otherwise engaged in protected concerted activity, can lose that protection by opprobrious conduct. Whether or not protection is lost depends on several factors: (1) the place of the discussion; (2) the subject matter of the discussion; (3) the nature of the employee’s outburst; and (4) whether the outburst was, in any way, provoked by an employer’s unfair labor practice. In the context of social media, however, NLRB has added its own modified Atlantic Steel test when applied through the use social networking sites like Facebook. Because social media is a worldwide web of social connections, its reach has far more impact than just those present at the time of the conduct.

To address the impact conduct may have on third parties, the NRLB borrows from the Jefferson Standard announced in NRLB v. IBEW Local No. 1229, to consider the denigration of the employer’s products and services. The Board will balance impact to the company against protected conduct. In cases where postings are critical of an employers’ managers, the Board tolerates a fair amount of attack on personal characterizations, for example name-calling, so long as there are no verbal or physical threats. The Board considers whether employee conduct which includes disparaging comments against an employer, retains protection by evaluating the exposure level to the employer, whether the comments are defamatory and/or critical of products or business policies of the employer.

**What is Not Protected Concerted Activity?**

Mere complaints and unsupported gripes are not likely to be found as protected concerted activity. In the nine cases where the NRLB found no protected concerted activity the conduct was not protected because it did not relate to important terms and conditions of employment. Posts complaining about the irritations sounds being made by a coworker, for example, do not qualify as a protected or concerted activity. In many instances, non-coworker posts of sympathy and support do not substitute the required support from co-workers and the intention to “engage in with or on the authority of other employees, and not solely by and on behalf of the employee himself” under Meyers. In one case, for example, “[t]he Charging Party did not discuss her Facebook post with any of her fellow employees, and none of her coworkers responded to the posts. Moreover, the Charging Party was not seeking to induce or prepare for group action, and her activity was not an outgrowth of the employees' collective concerns.” Therefore the court found no case of concerted activity.

**V. Framing Social Media Policies**
Avoid Overly Broad Social Media Policies

Social media policies will not protect employers if the policy is overly broad or restricts employees’ rights under Section 7. When limiting an employee’s right to communicate on social media (or otherwise), the terms and conditions restricting comments to being “professional” or “appropriate” need to be particularly defined in the policy.

Employers should specify in their policies what constitutes “appropriate” manners in which employees are allowed to discuss rights allowed under Section 7, including criticism of labor policies, treatment of employees, and terms and conditions of employment. Accordingly, employers should define with specificity what constitutes “insubordination or other disrespectful conduct” and “inappropriate conversation” when subjecting employees to disciplinary action by engagement. In general, employers may prohibit abusive or profane language in policies—however, whether or not employee conduct is abusive or profane is a factual inquiry and may not violate a policy. Preventing the use of social media to engage in unprofessional communication was also found to have an adverse effect on an employee’s Section 7 rights. However, if an employee’s discipline was a result of the employee’s “interference” with the employee’s own work or that of other employees or otherwise actually interfered with the employer’s operations, and that the interference was the reason for the discipline,” employers may avoid liability even if an overly broad social media policy exists.

Policies should be carefully drafted to avoid broad or ambiguous terms. If employees reasonably believe the policy prohibits Section 7 rights, the policy is unlawful. The addition of savings clauses within company policies which employees do not reasonably believe preserve Section 7 rights will not correct potential ambiguity.

Avoid Inferences that Impinge Section 7 Rights

The Board has held that an employer violates Section 8(a)(1) when they maintain a work rule that reasonably tends to chill employees in the exercise of their Section 7 rights. The Board has implemented a two-step inquiry to test for Section 7 violations. The Board first considers explicit Section 7 restrictions which are unlawful. If the policy does not “explicitly restrict activity protected by Section 7, the violation is dependent upon a showing of one of the following: (1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights.” Employers should review their policies closely for possible ambiguous references that employees may reasonably believe restrict Section 7 activities.

VI. Conclusion

Employers should make careful considerations in adjudicating current employees’ continued employment as a result of comments and conduct on social networking sites. Protected concerted activity and overly broad social media policies can create liabilities for employers. Recruitment and selection through social media sites should be closely monitored for disparate impact, and employers are urged to use a wide range of sourcing solutions to avoid creating disparate impact scenarios. Employers should take care in engaging in or providing legal, permissible, and uncoerced access to social networking sites, and create a process by which applicants and candidates have an opportunity to dispute potentially inaccurate information published online. Adhering to statutory, regulatory, and agency guidance, as well as case law, will help employers
maximize their insight on candidates while avoiding the potential pitfalls of social media use in the employment processes.

Kellie A. O’Shea (PHR) is the Director of Sales & Implementation at Creative Services, Inc., a firm that specializes in background investigation, drug screening and security consulting solutions. She is a 2013 J.D. candidate from the University of Massachusetts School of Law at Dartmouth and is advanced FRCA certified.

3 U.S. CONST. amend. I.
4 Id.
6 Id. at 482-84 (citing Meyer v. Nebraska (teaching German when prohibited by law) and Pierce v. Society of Sisters (private or parochial school when Oregon law prohibited.)
7 Id. at 484.
8 Facebook Data Use Policy, http://www.facebook.com/about/privacy/your-info#everyoneinfo (last visited March 21, 2012.)
12 Id.
13 See infra p.5-6.
14 18 U.S.C. § 1030
18 See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 C.A.9 (2002) where the 9th Circuit reversed summary judgment against Konop because Davis’s access to the website using another person’s login information (not considered yet a “user” of the system), was interpreted as “intercepted” in violation of the Stored Communications Act but not “intercepted” in violation of the Wiretap Act.)
20 Id.
23 FTC Opinion Letter (May 9, 2011) http://www.ftc.gov/os/closings/110509socialintelligenceletter.pdf (last visited March 21, 2012) (citing applicable provisions including consumer reporting agencies must take reasonable steps to ensure the maximum possible accuracy of the information reported from social networking sites. Consumer reporting agencies also must provide employers who use their consumer reports with information about their obligations under the FCRA, such as their obligation to provide employees or applicants with notice of any adverse action taken on the basis of these reports.)

Id. at 9.

Id. at 10.

Id. at 11.

Id. at 12.


Id.


Id.


58 N.R.L.B. Advice Memo Wayne Gold, Regional Director Region 5 FROM Barry J. Kearney, Associate General Counsel Division of Advice 506-0170, 506-2001-5000 SUBJECT: Children's National Medical Center, Case 05-CA-036658.)
59 Id.
65 N.L.R.B. v. Cooper University Hospital, 4–CA-38044.
66 N.L.R.B. v. ER Solutions, 19–CA-32943.
70 Martin Luther Mem’l Home Inc., 343 NLRB 646, 647 (2004).