Social Media – An Employment Nightmare

Howard L. Bolter
Bolter Law, LLC
412 South 4th Street, Suite 1050
Minneapolis, MN 55415

Cynthia A. Bremer
Ogletree, Deakins, Nash, Smoak & Stewart, P.C.
90 South Seventh Street, Suite 3800
Minneapolis, Minnesota 55402-4110
(612) 336-6868

Social Media – An Employment Nightmare

I. INTRODUCTION

So many internet tools to use, so little time. With all of the internet options available and new and interesting options popping up every day, job applicants and employers have much to manage. Applicants, striving to put their best foot forward, must be vigilant about their web persona. Employers, eager to make the best hiring decisions, must be cautious about obtaining and using an applicant's internet information. Creative employers can obtain highly damaging or helpful (depending on your perspective) digital dirt. Will that same creativity bring on a nasty lawsuit? Will an applicant's risqué postings or political musings bring their quest for the plum job to a screeching halt? These materials will explore what employers should or should not do when combing through an applicant's background and the possible consequences if not done carefully.

II. POTENTIAL LEGAL ISSUES

Like all employment related matters, if care is not taken, legal actions could result. The following claims illustrate the potential exposure an employer could expect if their background searches are not done carefully and consistently.

A. Invasion of Privacy

1. Elements of action

   a. Invasion of privacy involves three causes of action: intrusion upon seclusion, appropriation, and publication of private facts. *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 235 (Minn. 1998). The most likely claim in an applicant situation would be intrusion upon seclusion.

      (1) Intrusion upon seclusion occurs when one "intentionally intrudes, physically or otherwise, upon the solitude of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." *Id*. There are three elements to the intrusion on seclusion claim: 1) an intrusion, 2) that is highly offensive, and 3) that intrudes into some matter upon which a person has legitimate expectation of privacy. *Swarthout v. Mutual Service Life Insurance Company*, 632 N.W.2d 741, 744 (Minn. Ct. App. 2001). An invasion may occur through the form of investigation or examination into one's private concerns and a defendant may subject themselves to liability even

though there is no publication or other use of any kind of the information obtained. *See Lehman v. Zumbrota-Mazeppa Public Schools*, 2005 WL 894756, at *3 (Minn. Ct. App. 2005) (citing Restatement (Second) of Torts §652B, comment A-B (1977) (parenthetical explanation omitted)).

2. ***Smart Screening Tip:***

a. Difficult to prove given that applicant posting information on the internet for all to see has diminished reasonable expectation of privacy in such information and/or is not highly offended if someone accessed and used such information in employment hiring decision.

b. However, *see Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868 (9th Cir. 2002) where the Court found that employee's (could also apply to applicant) private website which included critical comments about his employer and management was protected from access by unauthorized users under the Stored Communications Act (SCA) 18 U.S.C. §2701 et. seq. This protection prevented users that had authorization to use the private website, but had failed to access the site for themselves from being "users" under the SCA because they never really "used" the service previously. Therefore, such users who provided management their username and password to view the private website, but did not have access to view the private website themselves, violated the SCA. In addition, an applicant must be able to show a nexus between the information obtained on the internet and the adverse failure to hire. *See Gerlich v. United States Dept. of Justice*, 828 F. Supp. 2d 284 (D.C. 2011) (plaintiffs provided undisputed evidence of internet searches and notes from such searches, but failed to overcome the employer's plausible explanations for applicant rejections based on the faces of their applications, such as typographical errors, unimpressive academic credentials and liberal affiliations).

c. If an applicant utilizes available privacy settings, there may be a stronger argument of reasonable expectation of privacy if employer improperly accesses a site in order to view selected applicants and/or is able to circumvent restrictions placed on a particular account in violation of the site policies. *See* Facebook User Conduct, http://www.facebook.com/terms.php; MySpace Terms, http://www.myspace.com/index.cfm?fuseaction=misc.terms

; *Ehling v. Monmouth Ocean Hospital Service Cop.*, 872 F. Supp. 2d 369 (D.N.J. 2012) (the employer's motion to dismiss was denied because under New Jersey common law the plaintiff had a reasonable expectation of privacy that her Facebook posting would remain private as "she actively took steps to protect her Facebook page from public viewing"); *Patterson v. Turner Construction Company*, 931 N.Y.S.2d 311, 312 (N.Y. App. Div. 2011) (if the plaintiff used Facebook's privacy settings to restrict access to the plaintiff's account, his Facebook information was still discoverable if it was relevant).

d. Do not ask applicants for passwords to their social networking sites during the interview/application process. California (A.B. 1844), Illinois (H.B. 3782), Maryland (H.B. 964), Michigan (H.B. 5523), New Jersey (A.B. 2878), and Utah (H.B. 100) have passed laws prohibiting employers from requiring or requesting current and prospective employees to disclose their usernames and passwords to personal social media and online websites. The federal government through the Social Networking Protection Act (SNOPA), as well as various state legislatures, have introduced similar legislation to restrict this practice, including Minnesota.

(1) Proposed Language of Minn. Stat. §181.53:

(i) Conditions Precedent to Employment Not Required

(1). No person, whether acting directly or through an agent, or as the agent or employee of another, shall require as a condition precedent to employment any written statement as to the participation of the applicant in a strike, or as to a personal record, for more than one year immediately preceding the date of application; nor shall any person, acting in any of these capacities, use or require blanks or forms of application for employment in contravention of this section. Nothing in this section precludes an employer from requesting or considering an applicant's criminal history pursuant to section 364.021 or other applicable law.

B. Breach of Terms of Service

1. Could arise if employer obtains information in a manner which violates the social networking site terms of service. For instance, deceptive friending, or assuming a false student or alumni identity to access Facebook information for an applicant. Another example: use of information obtained for commercial purposes, which may be a violation of Facebook terms. However, what is commercial vs. non-commercial use could be subject to various interpretations.

C. Stalking Laws

1. Minnesota law. Minn. Stat. §609.749 subd. 2 provides, in part, that:

   a. A person who stalks another by committing any of the following acts is guilty of a gross misdemeanor:

   * * *

   (2) follows, monitors, or pursues another, whether in person or through technological or other means[.] . . .

2. Conceivably, an employer could be held criminally responsible if their background searches became too intrusive via improper and/or sustained searching of an applicant's social networking pages. Intent to intimidate, threaten, frighten or persecute is not necessary under the Minnesota statute. *See* Minn. Stat. §609.749 subd. 1a. There are no known cases addressing such a claim at this time.

D. Lawful Consumable Products – alcohol use as a basis for rejection

Can or should the use of information showing lawful use or the results of use of alcohol be used as basis for applicant rejection? There is traction for protection of lawful, off duty conduct, which suggests a privacy interest in such conduct.

1. Minnesota law, Minn. Stat. §181.938 subd. 2, provides the following protections for off-duty conduct:

   a. An employer may not refuse to hire a job applicant . . . because the applicant . . . engages in or has engaged in the use or enjoyment of lawful consumable products, if the use or enjoyment takes place off the premises of the employer during nonworking hours. For purposes of this

section, “lawful consumable products” means products whose use or enjoyment is lawful and which are consumed during use or enjoyment, and includes food, alcoholic or nonalcoholic beverages, and tobacco.

b. If rejected for the above reasons, an applicant could seek damages for lost wages, benefits and reasonable attorneys’ fees and costs.

c. As always, proof of the basis for an applicant’s rejection may be very difficult to prove.

2. Reasonable expectation of privacy in non-working life?

a. Minnesota arguably gives applicants a right to expect privacy, beyond the protections of the statute. Thus, those posted photographs of the applicant drinking from a beer bong amid a pile of empty beer cans should not be used as a basis to reject the applicant—in theory. If they are used, there may be an invasion of privacy claim, in addition to the statutory violation.

3. ***Smart Screening Tip:***

a. Be sure to treat all applicants’ off-duty discoveries consistently or be prepared for a discrimination claim.

E. Discrimination

1. Elements

a. Disparate treatment discrimination is based on the well-known *McDonnell Douglas* test requiring a prima facie case, legitimate non-discriminatory reason for adverse action, and a showing of pretext. *St. Martin v. City of St. Paul*, 680 F.3d 1027 (8th Cir. 2012). Courts analyze Minnesota Human Rights Act claims in the same manner as Title VII. *Hoover v. Norwest Private Mortg. Banking*, 632 N.W.2d 534, 542 (Minn. 2001).

b. Applicants could argue that not all applicants were subjected to the same types of internet searches.

(1) Improper motivation for certain searches.

c. Applicants could also argue disparate impact on certain groups through use of consumer reports under FRCA or MCPA, criminal record, or education reports.

d. Disparate impact claims may also exist based on the statistics related to which demographic is using a particular social network.

(1) For instance, 71% of online adults use Facebook, 84% of those users are between the ages of 18-29 while only 60% are between the ages of 50-64. Additionally, 22% of online adults use LinkedIn; those that make less than $30,000 a year make up 12% of users while those that make $75,000 or more make up 38%. See *http://www.pewinternet.org/2013/12/30/demographics-of-key-social-networking-platforms/*

2. Possible Applicant Claims

a. Race/National Origin:

(1) "It could be evidence of unlawful discrimination if an employer checks for such Internet information on only certain types of applicants or employees, for example, African-Americans and Hispanics. It may also be evidence of unlawful discrimination if although the employer searches for such information on all applicants or employees, discriminatory bias affects the employer's evaluation of the information obtained. For example, an employer may view more negatively photos of an African American male, beer in hand, hanging out at a bar with a hip-hop DJ than photos of a white boy, also with beer in hand, hanging out at a rock 'n' roll bar with a bunch of other white boys wearing frat T-shirts. Tell me, was it really the public evidence of drinking that disqualified the individual? How many current employees would be disqualified from employment if never getting publicly intoxicated—or even drinking in public—was a job requirement? These are the kinds of questions the EEOC would ask if discrimination was [sic] raised." Williams and Loundsbury Morrow, *Want to Know Your Employees Better? Log on to a Social Network but, Be Warned, You May Not Like What You See*, 69 Ala. Law. 131 (2008) (footnote omitted).

b. Disability discrimination

(1) If applicant photographs of drug and/or alcohol usage are posted, systematic rejection of such applicants may

give the basis for a claim of perceived disability discrimination.

(2) Posted photographs of an applicant with a physical disability may give rise to a similar claim as it relates to the perception that such an applicant could not perform the essential functions of the job and/or would need reasonable accommodations.

c. Age

(1) A *pro se* plaintiff claimed that he was not hired by an employer because the employer allegedly learned of his age through his LinkedIn profile, which contained the year he graduated from college. Although the plaintiff's allegations were deemed weak, the Court denied the company's motion to dismiss the plaintiff's complaint. *Nieman v. Grange Mut. Cas. Co.*, 2012 WL 1467562 (C.D. Ill. Apr. 27, 2012).

d. ***New claim:*** Genetic Discrimination

(1) Genetic Information Nondiscrimination Act, 42 U.S.C. § 2000ff.

(i) "It shall be an unlawful employment practice for an employer--**(1)** to fail or refuse to hire, or to discharge, any employee, or otherwise to discriminate against any employee with respect to the compensation, terms, conditions, or privileges of employment of the employee, because of genetic information with respect to the employee . . . ." 42 U.S.C. § 2000ff-1(a)(1).

(ii) Applicants are covered. *See* 42 U.S.C. § 2000ff(2)(A)(i).

(iii) Also unlawful to request, require, or purchase genetic information of applicant or family member. 42 USC § 2000ff-1(b).

(2) Could gain illegal genetic information from information about group memberships or from family photographs depicting relatives with some known genetic physical ailment.

3. Probably difficult burden for an applicant to meet.

a. A plaintiff would have to review all searches performed, compare information and determine if similar potentially discriminatory information was used uniformly by the employer on other similarly situated individuals.

4. ***Smart Screening Tip:***

a. Employers should conduct the same type of search on each applicant. Social networking sites should not be searched for some applicants and not others.

b. Neutrality in searches is important.

(1) Employers could/should use non-decision makers to conduct searches.

(2) Cull out potentially discriminatory criteria, providing only non-discriminatory personal or employment related information.

F. Defamation

1. Elements:

a. A false and defamatory statement about the plaintiff; made in an unprivileged publication to a third party; and reputation in the community was harmed by such communication. *Dunn v. Nat'l Beverage Corp.*, 729 N.W.2d 637, 650 (Minn. App. 2007) (citations omitted).

2. An employer's use of defamatory material as a basis for rejection could be construed as republication of defamatory material, thereby exposing the employer to a defamation claim.

a. Any reference to the basis for rejections due to an employer's use of defamatory material discovered on the internet may be construed as compelled self-publication.

3. Blogging about rejected applicants.

a. Employers should monitor their company's sponsored blogs to ensure that defamatory material is not published about applicants in that forum.

4. ***Smart Screening Tip:***

    a. Never communicate the basis for rejection of an applicant to anyone outside the "need to know" group within the employer.

G. Tortious Interference with Contractual Relations

1. Elements

    a. A contractual relationship exists (includes at will employment), a third party has knowledge of such relationship, the third party intentionally procures breach of the contract, without justification. *Nordling v. N. States Power Co.*, 478 N.W.2d 498 (Minn. 1991).

2. Difficult claim in applicant setting:

    a. No claim against employer because employer cannot interfere with its own contract.

    b. Could sue individual searcher(s) or independent third party searchers, but standard of intentional procurement of breach is high as is proof of no justification.

    c. May have stronger arguments for intentional breach without justification if searcher improperly obtains information from social networking sites by violating terms of service for such sites. If doing so at the behest of the employer, perhaps a claim for respondeat superior exists.

H. Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681 et. seq.

1. Provides applicants various rights to information and basis for rejection decisions if based on a background search conducted by a third party.

    a. Applicant rights include notice that an investigation may be performed, their consent to such investigation, and notification if information discovered is used to make an adverse decision.

2. FCRA generally not applicable to internet searches if performed by the employer, not a third party.

    a. However, if a third party were used to search social networking sites, FCRA would give applicants the rights described above.

I. Minnesota Consumer Protection Act (MCPA), Minn. Stat. §13C.001 et. seq.

1. Provides similar protections to FCRA, above.

J. Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §1030

1. This federal law generally prohibits unauthorized access to a computer.

2. A violation may arise if an employer accesses a social networking site through illegitimate means.

   a. Examples: Misrepresenting affiliations with an educational institution in order to create an account or by using another employee or third party's account to gain access. Such conduct is clearly prohibited by most social network terms of service.

3. While the CFAA is a federal criminal statute, employees may bring a private right of action for any person who suffered damage or loss because of a CFAA violation. The civil remedies associated with the CFAA include compensatory, injunctive, and other equitable relief.

K. Negligent Infliction of Emotional Distress

1. Recovery may be available when applicant is within a zone of danger and suffers severe emotional distress with resultant physical injury. *Yath v. Fairview Clinics, N.P.*, 767 N.W.2d 34, 46 (Minn. App. 2009).

2. Exception to the "zone of danger" rule:

   a. Applicant could recover damages for mental anguish or suffering for a direct invasion of their rights, such as defamation, or the like. *Id.*

3. ***Smart Screening Tip:***

   a. An applicant would need to maintain a viable intentional claim like defamation, invasion of privacy, or Computer Fraud and Abuse Act, in addition to the negligent infliction claim, in order for the negligent infliction claim to survive. *See Yath*, 767 N.W.2d at 46 (where invasion of privacy claim failed, dismissal of negligent infliction claim proper, too).

L. Vicarious Liability/Respondeat Superior

1. An employer may be held liable for the intentional and/or negligent conduct of its employees. *Id.* at 47 (citing *Fahrendorff v. N. Homes, Inc*., 597 N.W.2d 905, 910 (Minn. 1999) (elements of vicarious liability for intentional conduct) and *Snilsberg v. Lake Washington Club,* 614 N.W.2d 738, 745 (Minn. App. 2000) (elements of vicarious liability for negligent conduct)).

2. In intentional act vicarious liability, the most likely in a background search claim, Courts must look to whether the source of harm related to duties of employee and whether harm occurs within work-related limits of time and place. *Id.* Critical inquiry is whether employee's acts were foreseeable.

3. Foreseeability should not pose too great an obstacle to the applicant since the background checking was likely mandated by the employer. However, if only limited background checking mandated and the employee/searcher exceeded the mandate, perhaps foreseeability was not possible.

4. ***Smart Screening Tip:***

    a. Make sure policies are in place to clearly define employer expectations and foreseeable actions of employee searchers.

M. Constitutional Violations (If governmental employer)

1. First Amendment

    a. Right to free speech

2. Fourth Amendment

    a. Unlawful search and seizure

N. Employee Related Claims

1. Employer actions related to applicants might trigger claims from existing employees..

    a. Whistleblower laws

        (1) The elements of claim under Minnesota's Whistleblower Act, Minn. Stat. §181.932 subd. 1(a) are:

(i) An employer shall not discharge, discipline, threaten, otherwise discriminate against, or penalize an employee regarding the employee's compensation, terms, conditions, location, or privileges of employment because . . . the employee . . . in good faith, reports a violation or suspected violation of any federal or state law or rule adopted pursuant to law to employer or governmental body . . . . Minn. Stat. §181.932 subd. 1(1). The *McDonnell Douglas* burden shifting analysis requires proof that employee engaged in protected conduct; suffered an adverse employment action; and a causal connection existed between the two. *See Grey v. City of Oak Grove, Mo.*, 396 F.3d 1031, 1034-35 (8th Cir. 2005); *Ring v. Sears Roebuck & Co.*, 250 F. Supp. 2d 1130, 1135 (D. Minn. 2003).

(2) Employee's refusal to conduct search

(i) An employee may have a potential claim based on belief that using their account access to further their employer's interest somehow violates the social networking sites terms.

(ii) Refusal could also generate a potential claim based on employee's belief that the search improperly invades the privacy of the applicant.

(iii) Refusal to search could similarly violate the Computer Fraud and Abuse Act (CFAA) 18 U.S.C. §1030, which provides criminal and civil consequences for unauthorized computer access.

(iv) An employee may also have a claim under a state statute that prohibits an employer from requiring or requesting current and prospective employees to disclose their usernames and passwords to social media sites. (For more see Invasion of Privacy, Section II (A)(2)(d)).

(3) Whistle blogging:

(i) Employee's termination for posting blogs critical of employer's practices or complaining about such practices.

(ii) Depending on employee's social media posts, it may be protected under the National Labor Relations Act (NLRA), whether a unionized employer or not. For example, if the posting represents an effort to unionize, discusses the terms and conditions of employment, criticizes an employer's labor practices, or relates to a labor dispute between an employer and its employees, then the employee's post has a high likelihood of being protected.

(iii) The NLRA grants employees Section 7 rights, which are rights to "engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection." National Labor Relations Act, 29 U.S.C. §157. NLRA Section 8(a)(1) enforces Section 7, which makes it an unfair labor practice for an employer "to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in section 7." National Labor Relations Act, 29 U.S.C. § 158(a)(1).

(iv) The National Labor Relations Board (NLRB) uses a two-step inquiry to determine if an employer violates these rights under the NLRA. NLRB Office of the Gen. Counsel Rep., Memo. OM 12-31, at 3 (Jan. 24, 2012).

(1). The First Step is that a rule is clearly unlawful if it explicitly restricts Section 7 protected activities. *Id.*

(2). The Second Step is that if the rule does not explicitly restrict Section 7 protected activities, it will only violate Section 8(a)(1) upon a showing that: (a) employees would reasonably construe the language to prohibit Section 7 activity; (b) the rule was promulgated in response to union activity; or (c) the rule has been applied to restrict the exercise of Section 7 rights. *Id.*

(3). For example, in *Hispanics United of Buffalo Inc. v. Ortiz*, the NLRB upheld the ALJ's order that five employees engaged in protected concerted activity for the purpose of mutual aid or protection by posting comments on Facebook that responded to a co-worker's criticism of their job performance.

Hispanics United of Buffalo Inc., 359 NLRB No. 37 (N.L.R.B. Dec. 14, 2012).

(4) ***Smart Screening Tip:***

Educate employees involved in searches to eliminate good faith basis for objection. Have written policies to eliminate perception that access to information is for improper purpose and complies with terms of use at various sites.

O. Litigation Caveats

1. Remember: Legal counsel can conduct their own searches in an applicant claim against an employer. Thus, it is important that the ultimate hire for the applicants' job not have information an attorney can search and find lending credence to a discrimination claim or other violation.

2. Discovery of employer searches likely, as well.

   a. One potential drawback in litigation settings is the possibility of adverse discovery of searches done by employers. Forensic computer experts could uncover "smoking guns" amid the digital detritus created during searches.

III. EXAMPLE OF ONLINE RECRUITMENT POLICY (SPACEBOOK CO.)

A. Purpose of Online Recruitment

1. To assist in meeting Spacebook Co. goals:

   a. By increasing recruitment opportunities;

   b. By making effective hiring decisions.

2. To enhance recognition of Spacebook Co.

Spelling out the goals of the activity helps the employees maintain their focus while engaged in the recruitment activity. For purpose of a recruitment policy, the primary goal would seem to be bringing in good people to hire.

However, it is important to recall that like all other outreach activities, online recruitment also presents or contributes to a larger image to the outside world. That image is tied to marketing, sales and all other aspects of the business. Thus, even though social networking by a recruiter or HR employee has a very specific target, it also serves a greater purpose by forming and/or reflecting a part of the company's particular brand.

B. General Principles

All activities conducted in connection with online recruitment must:

1. Comply with all applicable laws;

2. Be conducted in a professional and acceptable manner;

3. Avoid liability or risk for the organization; and

4. Refrain from anything that would cause embarrassment or scandal for Spacebook Co.

These principles are critical. The company must present the commitment to complying with all applicable laws and should reinforce this at all times.

The commitment to professionalism is also critical. Communication via the computer generally is less formal than many other forms of communication, especially on networking sites. Employees should be reminded to remain on guard against lapsing into this informality just as they do when speaking on the telephone, conducting in-person interviews, etc.

In addition, social networking blurs the lines between business and personal time if the recruiting employee is using personal accounts to conduct online recruitment. These employees must be reminded that even though they are engaged in personal pursuits, their actions may reflect on the employer.

C. Conducting Online Screening

All persons (conditionally hired) (reaching the final interview stage) for employment with Spacebook Co. must undergo a thorough online screening. All such screening must be conducted by appropriate persons and in accordance with this policy.

1. Persons Responsible for Online Screening

a. Online screening may only be conducted by persons trained to do so under Spacebook Co. policy and procedures;

b. Online screening may only be conducted by employees not responsible for making or contributing to the hiring decision.

Paragraph 1a is intended from keeping hiring managers, supervisors, and others from interfering or conducting "their own" screening. Online screening should be done only by people who have been educated on the legal parameters, as well as, the employer's principles underlying this policy.

Paragraph 1b provides insulation against discrimination claims. Just as the receptionist has always removed the EEO identification form from the completed application, now the online recruiter will screen out all protected class information and other possible problematic data. From there, the hiring decision can be made by people who have not been exposed to this information.

2. **Persons Subject to Online Screening**

   a. Online screening must be conducted for all persons (conditionally hired) (reaching the final interview stage) for the position in question;

   b. Online screening may only be conducted in regard to persons who have signed the "Spacebook Co. Online Screening Authorization" form;

   c. Online screening may only be conducted in response to a request from a Department Director or above.

Paragraph 2a also addresses the discrimination concern by directing that all persons involved at a particular stage in the recruitment be subject to online screening. An employer who decides that "only young people have Facebook pages so we'll only check them" courts serious age discrimination issues under state discrimination laws that extend coverage below the federal limit of 40.

Paragraph 2b obviously assists in protecting the employer from claims that the applicant was not aware of the intention to do online background checking, and gives the employer the opportunity to convey all of the safeguards and other information they wish to present to the applicant.

Paragraph 2c protects against the casual decision by a manger to check out the applicant. It also protects the recruiter from having to wonder whether a directive to conduct an online search is legitimate.

3. **Types of Information Sought in Online Screening**

Employees conducting online screening must limit their actions to obtaining relevant job-related data. Such data is limited to:

a. Criminal background or activities;

b. Job skills;

c. Work experience;

d. Work habits;

e. Activities in conflict with employer mission;

f. Communication skills;

g. Other unique facts bearing upon applicant's employability.

No surprises here. Online recruitment is just a different tool for achieving the same result that we have always sought – collecting job related data to help make a good hiring decision.

4. **Types of Information Not Sought Or Considered**

Employees conducting online screening must refrain from obtaining data that is not job related, including but not limited to:

a. Protected classifications;

b. Protected activities;

c. Private personal information;

d. Trade secrets/confidential information.

No surprises here either, although online recruitment does present some risks that traditional recruitment methods do not present. For one thing, protected class information is readily available throughout the cyber world. People often list a number of their protected classifications (e.g. marital status, religion, sexual orientation) on social networking sites, while pictures are readily available to determine an applicant's race, gender and perhaps disability status. The same is true for protected activities.

Online recruitment also poses risks of learning too much about an applicant's personal life. Applicants are typically guarded about such things while interviewing but a quick Google check can yield a variety of interesting tidbits.

5. **Methods of Collecting Information**

Employees conducting online screening must at all times:

a. Limit their actions to obtaining relevant job-related data;

b. Observe privacy restrictions and terms of use requirements on any internet site accessed;

c. Refrain from "hacking" inaccessible sites;

d. Discontinuing viewing pictures, postings or other information as soon as it is clear that such items are not job related;

e. Refrain from downloading or otherwise using information amounting to protected intellectual property (except what might be needed to support a legitimate employment decision);

f. Refrain from making false or misleading statements for the purpose of obtaining information on applicants;

g. Refrain from making defaming or disparaging statements about anyone or anything;

h. Make a general record of the sites used to screen the employee.

It is critical that employers stress the proper methods of collecting data. This means observing appropriate privacy standards (Paragraphs 5a – 5d), ignoring protected or proprietary materials (Paragraph 5e), refraining from improper communications (Paragraphs 5f and 5g) and insuring proper documentation of the online recruitment efforts.

If these items are not in the policy, it seems only natural that an applicant, judge and/or jury would conclude that such methods are embraced as part of the employer's online recruitment practice.

6. **Use of Information Received Through Online Screening**

   a. Employees conducting online screening must seek to verify the accuracy of all information received;

   b. All information relevant to the consideration of the applicant must be downloaded and retained for further review;

   c. All information regarding protected classifications and/or activities must be removed from the data transmitted to hiring officials;

   d. Information collected during online screening may not be used or communicated to anybody other than the persons responsible for the hiring decision;

   e. Information collected during online screening may not be used for any reason other than the hiring decision for which the online screening is conducted.

Why bother to collect the information if you are not going to evaluate it properly? Making grand assumptions about applicants based on snippets gleaned from the internet may not serve the best interests of the employer. Recruiters verify all sorts of information received from other sources; they should be particularly vigilant about doing so here.

Paragraphs 6b and 6c address the need to document the information gathered, while 6d and 6e protect against improper use of the information. If an applicant has authorized access to their Facebook page for employment purposes, they should not have to tolerate the use of that information for other purposes, and requiring it may lead to an invasion of privacy claim.

7. **Retaining Information Received in Online Screening**

   a. All information reviewed during online screening must be retained in the applicant file for the same period of time that other materials in that file are retained;

   b. Access to the applicant file is limited to HR Department employees for legitimate business use only.

D. Conducting Social Recruitment

Social Recruitment is the use of social media and related online resources to network for business-related purposes, including recruitment of new employees. All social recruitment must be conducted in accordance with this policy. This policy applies to all social networking sites (e.g. Facebook, LinkedIn, and Myspace), web forums, blogs, discussion groups, chat rooms, picture swapping sites and all other internet sites designed for people to interact with each other.

1. **Employees engaged in social recruitment must clearly identify themselves as employees of Spacebook Co. with responsibilities in the area of human resources and recruitment.**

   a. Employees may not create false identities to "friend" applicants or solicit information from them;

   b. Employees may not misrepresent their purpose in participating in social media;

   c. Employees may not offer or solicit communication "off the record."

This section of the policy switches from the background search focus of online recruitment to the more general world of creating an online HR presence for the purpose of seeking qualified applicants. One of the overriding principles of this activity must be the insistence that the recruiter not seek to hide their professional persona or try to trick the person into divulging otherwise protected or inaccessible information.

Employers should require honesty and integrity in the use of all social recruitment in furtherance of the principles stated in Paragraph A-C.

2. **Employees must act in an ethical and professional manner.**

   a. Employees must behave respectfully and not harass, threaten, disparage, defame or ridicule anyone;

   b. Employees must refrain from behavior reflecting a bias against or in favor of persons of a particular protected classification;

   c. Employees may not act in any manner that would violate any policy of Spacebook Co.;

   d. Employees must at all times provide only truthful statements and accurate information when engaged in social recruiting.

Employers must insist on ethical, appropriate and lawful behavior. Employees engaged in social recruiting represent and act on behalf of the Employer to a very significant extent. Harassing or threatening behavior while engaged in social recruitment is easily identified and documented, which expose the Employer to substantial liability under a number of different legal theories (e.g., discrimination, defamation).

3. **Employees Must Respect Privacy Rights Of Others**

   a. Employees must observe all terms of service requirements and other requirements of any site or service that you use for networking on behalf of Spacebook Co.;

   b. Employees may not violate anyone's privacy or use their copyrighted or protected information, while using social media on behalf of Spacebook Co.

This is also a critical aspect of social recruiting. Again, the recruiter is acting on behalf of the employer. Hacking into an account or otherwise exceeding the legitimate privacy protections of potential employees can create a great risk of liability, as can the use of someone's proprietary information obtained through methods that breached the owner's privacy interests.

4. **Employees Must Protect Confidential Information**

   a. Employees must refrain from divulging any Spacebook Co. trade secrets or confidential information;

b. Employees must refrain from divulging any confidential information or trade secrets of a customer or client;

c. Employees may not comment or address anything related to the following matters:

(1) Anything relating to legal matters in involving Spacebook Co.;

(2) Anything relating to Spacebook Co. financial information;

(3) Anything relating to litigation involving Spacebook Co.;

(4) Anything relating to matters relating to competitors and/or their capabilities;

(5) Anything relating to services, systems or products Spacebook Co. is developing but has not yet implemented.

This section of the policy focuses on the recruiter's responsibility to protect the employer's information and business interests. Employers are required to zealously protect their own confidential information and trade secrets in order to have a hope of obtaining judicial relief in trade secret litigation. In the computer age, one slip can result in a piece of confidential information being instantly transmitted around the globe.

E. Violations of Policy

Employees violating this policy are subject to discipline up to and including termination.

F. Further Information

For more information, please contact (designated employer official).

18715996.1
18803404.1