

A Warning To Employers: the Use of Myspace or Facebook In Hiring Decisions May Be Hazardous to Your Business!

By Lester S. Rosen

While social networking sites like Myspace and Facebook may appear to be treasure troves for employers at first glance, they can actually prove to be hazardous to businesses when used for hiring decisions.

Employers and recruiters have uncovered what appears to be a gold mine of applicant information on the internet. By searching social networking sites such as Facebook or MySpace for potential hires, recruiters feel they are effectively able to "get into an applicant's head" and see a more accurate portrait of who that person is.

Unlike the traditional hiring tools such as team interviews, psychological testing, calling past employers, and background checks, social networking sites hold out the promise of revealing the "real applicant." Statistics from various surveys, news articles, and anecdotal evidence confirm that there is an increased use of social networking sites to screen candidates.

Stories from recruiters show why these sites are so enticing.

One recruiter recounts how she had found "The Ideal Candidate" for a prestigious consulting firm. Then, just out of curiosity, she ran the applicant's phone number on a search engine, and – wow! Up popped some rather explicit ads for discreet adult services that the applicant was apparently providing at night. Another recruiter tells the story of finding an applicant's MySpace page, where the intern had demonized his firm, his boss and his coworkers in considerable detail and by name.

Here is the usual approach for a recruiter utilizing the internet to screen candidates. Search by name for the candidate. Refine the search by taking the applicant's name and then adding the terms "Facebook" or "MySpace." Next, a recruiter can go to MySpace and Facebook directly and see whether they find a site belonging to the applicant. Depending upon how a user chooses to set his or her own privacy settings, finding information on a social network site can be very hit or miss. Also, a recruiter can search a blog search engine, such as www.google.com/blogsearch. Business sites such as Zoominfo or LinkedIn can be run.

This article, however, examines why such an apparently easy to use and readily available tool has its dangers and drawbacks.

No Court Cases of Record Yet

At this point in the evolution of social networking, there are no published cases yet on point. Lawsuits take time to work their way through the courts until an appellate court is finally called upon to issue an opinion. However, it is all but certain that some day an employer will

land in court being sued on allegations of discrimination or a violation of privacy for making use of a social networking site in the hiring process.

One reason that the use of social networking sites presents a risk stems from their original purpose. In the beginning, users intended to limit access to friends or members of their own network, arguably creating a reasonable expectation of privacy. It's like a "cyber high school," but instead of seeing your friends near your locker, you can see friends and make contacts all over the world. Younger workers in particular may well regard invading their social network sites in the same way older worker may regard someone that crashes a private dinner party uninvited – a tasteless act that violates privacy.

The conventional wisdom, however, is that anything online is fair game because any reasonable person must understand that the whole world has access to the internet.

When analyzing the privacy issues, an employer may want to take the "Las Vegas test." Assume you are at a business meeting in Las Vegas, and at the end of the day you adjourn with professional colleagues to a cocktail lounge in the hotel lobby. Several drinks later, you engage in a very frank exchange about your employer or co-workers. You may be indiscrete or even act a little silly. How would you feel if a colleague took photos with a cell phone and sent them to everyone you knew, along with some of your more interesting comments? Technically, you were "in public" – in a public cocktail lounge. True, but most people would still call it an invasion of privacy. This is based on an objective belief founded on broadly based and widely accepted community norms that what goes on in a private conversation should not be seen by the entire world, even if it occurred in a public venue where anyone could have seen or heard.

For many young workers today, social networking sites are the equivalent of that Las Vegas cocktail lounge!

Even though they communicate and share photos in a forum that can be public, there is sense that what goes on in MySpace or Facebook stays there and should stay there. This argument is buttressed by the fact that in order to enter some social networking sites, a user must agree to "terms of use" and to get details of another site member, the new user must set up their own account. Additionally, these types of websites have "terms of use" typically do not allow "commercial" uses, which can include screening candidates. Since a user must jump through some hoops, it can be argued that there is an expectation that the whole world won't be privy to confidential information.

On the other hand, a recruiter can argue that the routine "terms of use language" where someone simply hits the "I agree" button is not much of a privacy barrier. In addition, if an applicant fails to utilize the privacy controls provided by the website, that undercuts any reasonable belief that what was on the website would remain confidential.

This Issue Far From Being Settled

The bottom line is that the question of whether an applicant has a reasonable expectation of privacy can depend upon the specific facts of the case being litigated, and the issue is far from settled. Frankly, it could be decided either way.

That is why recruiters should not simply assume that anything on the web is fair game.

One area where an employer or recruiter would be flirting with particular trouble is if information from Facebook or MySpace is obtained by manipulating the sites. This could be done by creating multiple identities or by using "pretexting," which can include pretending to be someone else or something you are not. For example, Facebook allows greater access into sites within your own network. If a recruiter were to violate Facebook rules and create fake identities just to join a network belonging to an applicant, that would likely cross over into the realm of employer behavior that is overly intrusive and invades too deeply into private matters.

Off-duty conduct is another tricky area. Some states have prohibitions limiting use of private behavior for employment decisions. However, employers do have broader discretion if such behavior would damage a company, hurt business interests, or be inconsistent with business needs.

Is It Discrimination?

Discrimination can also become a substantial issue. A candidate may say or depict all sorts of things that reflect race, color, religion, national origin, ancestry, medical condition, disability (including AIDS), marital status, sex (including pregnancy), sexual preference, age (40+), or other facts an employer may not consider under federal law or state law.

This can give rise to the problem of "Too Much Information," also popularly referred to as "TMI." The employer's own search of these sites can make an employer knowledgeable of factors that should NOT be considered for employment purposes. The issue then becomes: "How do you **unring the bell?**" How do you prove that you didn't use the information you found as part of your hiring decision?

A related issue is whether a firm is treating all applicants in a similar fashion. If recruiters or human resource staffers are performing internet searches on a hit or miss basis, with no written policy or standard approach, an applicant that is subject to adverse action as a result of such a search can potentially claim to be a victim of discrimination.

Also problematic is that on social network sites, a recruiter may view photos, personal data, discussion of personal issues and political beliefs, behavior at parties, and other information that an applicant may not have intended for the world to see. Employers may have to consider whether what a person says on their site is true, and if true, whether it would be a valid predictor of job performance – if fact, whether it would be employment related at all. After all, people *have* been known to exaggerate or make things up. They may believe they are just having fun or spoofing their friends.

Or if a site shows, for example, that an applicant has a tattoo or a piercing, what then? Employers may need to ask themselves whether having a tattoo is really a good reason not to hire someone.

Employers that hire younger workers may need to come to grips with new generational differences.

One rule to remember: If a website is searched by a background screening firm on behalf of an employer, then consent and certain disclosures is mandated under the federal Fair Credit Reporting Act (FCRA).

What's REAL on the Internet?

In addition, how do you know what is "real" on the internet? How do you know that the "name" you found is your applicant? You don't. With more than 300 million Americans today, most of us have "computer twins" (i.e. people with our names and even a similar date of birth). There is also the question of how does a recruiter even know for sure the applicant actually wrote the item or authorized its posting? How does the recruiter know if its even true, or just a matter of someone being silly with their friend?

There are anecdotes on the internet of false postings under another person's name – a sort of "cyber identity theft." If anonymous information is posted, such as in a chat room, there is the new phenomena of Cyperslamming, where a person can commit defamation without anyone knowing who they are.

What Are the Lessons for Employers and Recruiters?

1. Using the Internet to screen candidates is not risk-free, especially when it comes to social networking sites.
2. There are no legal cases yet, but news travels fast on the web, and employers who rely overly much upon social networking sites may find that job applicants are not as eager to look at their firm.
3. If an employer or recruiter uses the internet, they should first consult their attorney in order to develop a written policy and a fair and non-discriminatory procedures. As a general rule, the later in the hiring process the Internet is used, the less open an employer may be to suggestions that matters viewed on the Internet were used in a discriminatory fashion. The most conservative approach is to not use the Internet until AFTER there has been a conditional job offer.
4. For legal protection, **employers should considering obtaining consent so that applicants are on notice that their web persona is fair game. Employers should not use any fake identities or engage in "pretexting" to gain access to information.**

5. The most conservative approach is to perform an internet search AFTER there is consent and a job offer is made contingent upon completion of a background check that is satisfactory to the employer.
6. Whatever your policy is, it should be written. For employers that recruit at college, there is a trend to require employers to notify students ahead of time as to their policy for searching online for an applicant's cyber identity.

For job applicants, the advice is simple: Don't be the last to know what a web search about you would reveal.

If you do not want employers looking at your social networking site, then set the privacy parameter to "restricted use only." As a savvy applicant, you can even go on the offense and create an online presence that helps you get a job!

Lester S. Rosen is an attorney at law and President of Employment Screening Resources , a national background checking company located in California offering employment screening services such as employee background screening, job verification, and credential verification. He is the author of, "The Safe Hiring Manual--Complete Guide to Keeping Criminals, Imposters and Terrorists Out of Your Workplace." (512 pages-Facts on Demand Press), the first comprehensive book on employment screening. He is also a consultant, writer and frequent presenter nationwide on pre-employment screening and safe hiring issues. He has qualified and testified in the California, Florida and Arkansas Superior Courts as an expert witness on issues surrounding safe hiring and due diligence. His speaking appearances have included numerous national and statewide conferences. He is a former deputy District Attorney and criminal defense attorney and has taught criminal law and procedure at the University of California Hastings College of the Law. His jury trials have included murder, death penalty and federal cases. He graduated UCLA with Phi Beta Kappa honors, and received a J.D. degree from the University of California at Davis, serving on the Law Review. He holds the highest attorney rating of A.V. in the national Martindale-Hubbell listing of American Attorneys. Mr. Rosen was the chairperson of the steering committee that founded the National Association of Professional Background Screeners (NAPBS) a professional trade organization for the screening industry, which now has over 500 members. He was also elected to the first board of directors and served as the first co-chairman in 2004.