ESR EMPLOYMENT SCREENING RESOURCES
The Background Check Authority℠

Managing the Risks of Using the Internet for Employment Screening Background Checks

An Employment Screening Resources (ESR) White Paper

Table of Contents

Managing the Risks of Using the Internet for Employment Screening Background Checks

An Employment Screening Resources (ESR) White Paper

This white paper will provide an informative introduction for both employers and recruiters using Internet search engines like Google and social networking sites such as Facebook for recruitment and employment screening background checks and the possible legal risks faced when conducting such screening, as well as potential solutions to avoid legal issues.

Introduction

No discussion on employment screening background checks these days is complete without an analysis of how the Internet is used for uncovering information about job candidates. In what is often referred to as Web 2.0,[1] recruiters and employers can harvest information from a variety of new sources such as social networking sites like Facebook, and include numerous other places where applicants may reveal themselves ranging from Twitter, blogs, and YouTube videos to business connection sites such as LinkedIn and search engines like Google. Many employers have focused with laser-like intensity on using the plentiful amount of information found online.

Employers have uncovered what appears to be a treasure trove of job applicant information on the Internet. Using search engines and social networking sites, they believe they are effectively able "to look under the hood" and try "to get into an applicant's head." Unlike traditional hiring tools such as interviews and contacting past employers, social networking sites hold out the promise of revealing the "real" job applicant. Statistics from various surveys and anecdotal evidence confirm there is an increased use of the Internet to screen candidates.

Stories from recruiters and Human Resources 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 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.

What is overlooked in the rush to use the Internet for employment screening background checks is a question that needs to be asked: What are the legal risks for employers using the Internet for employment screening?

The use of social networking sites to obtain deeper levels of information on job applicants is not without risk. Such efforts can potentially raise issues of discrimination, invasion of privacy, improper use of legal off duty conduct, as well as issues relating to authenticity and accuracy. This article will review a number of potential pitfalls and legal landmines

In fact, the dangers of using social networking sites was recognized by no less than two members of the United States Senate in a letter sent to a background screening firm that specializes in reviewing and storing social networking data for employment background checks.[2]

Another challenge for employers is the lack of certainty as to the boundaries and scope of legal use. As discussed in this paper, the phenomenon of social networking sites has progressed much faster than case law or legislative action. It takes time for cases to develop and for legislatures to act. Not only that, but the web sites themselves can modify access or even terms of use without notice, leading to further uncertainty.[3]

It is important to note that this whitepaper addresses the use of the internet and social network sites for recruiting and making hiring decisions. It does NOT cover employer concerns AFTER a person is hired. That is another topic entirely. However, every employer needs to have an "Internet Policy." The National Labor Relations Board

[1] Generally speaking, **Web 1.0** is web pages that viewers look at. **Web 2.0**, stated most simply, refers to the evolution of the web where social interactions and conversations can occur.

[2] See ESR News Blog **'Two US Senators Voice Privacy Concerns Over Background Check Firm Storing Web Footprints of Consumers for Employment Screening'** at: http://www.esrcheck.com/wordpress/2011/09/21/two-us-senators-voice-privacy-concerns-over-background-check-firm-storing-web-footprints-of-consumers-for-employment-screening/.

[3] This white paper will not address a related issues to the use of **Web 2.0**, such as the ease with which less scrupulous job seekers can utilize the internet to obtain worthless college diplomas from degree mills, as well as totally fabricated job histories, in elaborate scams that nice fake accreditation agencies, and live operators that will "verify" the fake information, or elaborate web sites set up to create fake past employers. These issues are discussed in the ESR News Blog at http://www.esrcheck.com/wordpress/tag/diploma-mills/.

(NLRB) recently published a summary of cases that deal with the use of social media searches on current employees (See: https://www.nlrb.gov/news/acting-general-counsel-releases-report-social-media-cases). Although the legal authority for the use of the Internet and social media sites is limited when it comes to hiring, the cases summarized by the NLRB on current employees may have bearing on future court decisions. In addition, an excellent example of how and when to write a social media policy was provided in Inc. Magazine at: http://www.inc.com/guides/2010/05/writing-a-social-media-policy.html.

A social media policy for current employees needs to address issues such as:

- ☑ **Who owns the company computer and what right of privacy does an employee have (i.e. can an employer monitor internet use and e-mails)?**
- ☑ **What is acceptable blogging/posting for employees?**
- ☑ **What happens if an employee posts a derogatory comment about the employer or a competitor, or reveals confidential information?**
- ☑ **If the employers are unionized, how does that affect the social media policy?**

Research Shows Employers Use Internet for Background Screening Despite Risks

Despite the potential risks and uncertainties involved, employers seem intent on using Internet search engines such as Google and social networking sites like Facebook and Twitter for the background screening of job applicants. Whether appropriate or not, the Internet is a public domain, and information about job applicants is being used by Human Resources professionals to screen applicants.

On Data Privacy Day in January 2010, Microsoft released a commissioned research study that outlined the ways human resources professionals worldwide used personal, yet publicly available, online information when screening job candidates. Twelve hundred interviews were conducted for the study in the United States, United Kingdom (U.K.), Germany, and France. Some of the results raised eyebrows.

For example, 79 percent of HR professionals surveyed in the U.S. reported reviewing information found on the Internet when examining job candidates. In addition, 84 percent of the HR professionals surveyed in the U.S. categorized online reputation information as one of the top two factors they considered when reviewing a comprehensive set of candidate information.

"79 percent of HR professionals surveyed in the U.S. reported reviewing information found on the Internet when examining job candidates."

The Microsoft study also found that employers were not only reviewing the information, they were acting on it, as 70 percent of those surveyed in the U.S. had rejected a candidate based on online information, with the top factor for rejection being unsuitable photos and videos online. The study revealed that HR professionals are regularly using information about candidates found on the Internet, which could have significant repercussions.

Social Networking Screening Increasing but Employers have Reservations

A 2009 survey conducted by job networking site CareerBuilder.com of more than 2,600 hiring managers revealed 45 percent of employers used social networking sites to research candidates. The survey also revealed that 35 percent of employers rejected job applicants based on what was uncovered on social networking sites. Of these 35 percent of employers who rejected job applicants based on what was uncovered on social networking sites, the reasons given included:

- ☑ **53 percent cited provocative/inappropriate photographs or information.**
- ☑ **44 percent cited content about drinking or using drugs.**
- ☑ **35 percent cited bad-mouthing of previous employers, co-workers or clients.**
- ☑ **29 percent cited poor communication skills.**
- ☑ **26 percent cited discriminatory comments.**
- ☑ **24 percent cited misrepresentation of qualifications.**
- ☑ **20 percent cited sharing confidential information from a previous employer.**

Employers Wary of Using Social Network Sites and Search Engines for Screening

An 2011 survey from the Society of Human Resource Management (SHRM) – 'SHRM Survey Findings: The Use of Social Networking Websites and Online Search Engines in Screening Job Candidates' – found that, contrary to popular belief, only roughly one-quarter (26 percent) of organizations indicated they used online search engines such as Google to screen job candidates during the hiring process while even fewer organizations (18 percent) used social networking sites like Facebook for that purpose.

Conversely, the SHRM survey found that close to two-thirds (64 percent) of organizations had never used online search engines to screen job candidates or used them in the past but no longer did so, while more than two-thirds (71 percent) of organizations had never used social networking websites to screen job candidates or used them in the past but no longer did so. The reasons why some organizations did not use social networking websites to screen job candidates included the following:

- ☑ **Two-thirds (66 percent) of organizations indicated they did not use social networking websites due to concerns about the legal risks/discovering information about protected characteristics such as age, race, gender, and religious affiliation.**
- ☑ **Nearly one half (48 percent) of organizations did not use these sites because they could not verify with confidence the information from the social networking website pages of job candidates.**
- ☑ **Another 45 percent of organizations indicated that the information found on the social networking sites may not be relevant to a job candidate's work-related potential or performance.**

The survey also revealed a significant increase in the prevalence of formal or informal policies regarding the use of social networking websites to screen candidates over the past three years. While 72 percent of organizations had no formal or informal policies regarding the use of social networking websites for job screening in 2008, this figure has dropped to 56 percent in the recent survey. In addition, 29 percent of organizations plan to implement a formal policy in the next 12 months, up from 11 percent in 2008.

As for how many organizations disqualified candidates based on information found by online search engines or social networking websites, of the small percentage of organizations that used such information only 15 percent of this group indicated that they used online search engine information to disqualify job candidates while 30 percent indicated they used social networking information to disqualify job candidates.

Social Networking Screening Ground Rules can Change at any Moment

Part of the risk of using social media is that the area is so new that courts and legislators have not yet entered into the act, as well as other factors that create uncertainty for employers and labor lawyers. Uncertainty abounds since courts and legislators have not caught up with social media and the ground rules can change at any time without notice.

First, as of the writing of this white paper, there is very little in the way of court cases on point. There are cases in the education arena revolving around tenure and academic freedom where information on a social networking site was involved and cases involving current employees.

However, there are no court decisions yet on the exact issue of the use of the internet for applicant recruiting and selection. It takes time for an aggrieved party to first file a lawsuit, and then the lawsuit has to go before an appellate court on some issue in order to get a ruling. Of course, each case is very fact specific, so the outcome of a particular case may or may not have broad implications.

Neither Congress nor state legislatures have taken any action on this issue either. The last time Congress passed a law that arguably impacts this area was in 1986 with the Stored Communications Act, back in the days of dial up modems and well before the advent of the World Wide Web as we currently know it.[4]

Another issue is that human resources and labor law issues are heavily regulated by state laws, so when court cases begin to appear or legislation is enacted, it may turn out to be a patchwork of various state rules.

It's also worth noting that some of the issues in play in this area rely upon the terms of use of various web sites. So if a social media site indicated that the site is for non-commercial use, it can affect the calculus of piracy unless it is shown that such a restriction is just boilerplate and not enforced in any way. Of course, terms of use can change at a moment's notice, adding another level of complexity.

At this point, given that there is little in the way of legal precedent or legislative mandate, the best that can be done is to take known existing laws and legal principals

[4] The **Stored Communications Act (SCA)** is a federal law enacted by the Congress in 1986, as part of the Electronic Communications Privacy Act. (See: 18 U.S.C. §§ 2701 to 2712) The SCA deals with voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" that are stored by third-party internet service providers (ISPs).

and project them forward to determine how and where they may apply to using social networking for recruiting and hiring. However, this is an area that needs to be followed closely as any day, a new court case can be handed down that may significantly alter our view of how to proceed in this area.

The Landmines and Traps for the Unwary

In using the Internet for the screening of job applicants, employers can encounter a number of legal risks and potential landmines. These can include:

- ☑ **1. Too Much Information (TMI) – Discrimination Allegations**
- ☑ **2. Too Little Information (TLI)**
- ☑ **3. Credibility, Accuracy, and Authenticity Issues**
- ☑ **4. "Computer Twins" & "Cyber-slamming"**
- ☑ **5. Privacy Issues**
- ☑ **6. Requiring Applicants to Provide Facebook or Other Social Media Passwords**
- ☑ **7. Legal Off-Duty Conduct**
- ☑ **8. What is "Fair Game" on the Internet?**
- ☑ **9. Should Background Screening Firms Conduct Internet Background Checks?**

1. Too Much Information (TMI) – Discrimination Allegations

Employers can find themselves in hot water when utilizing Internet search engines and social networking sites for screening due to allegations of discrimination. This issue is sometimes referred to as Too Much Information or TMI. The problem is that once an employer is aware that an individual is a member of a protected group, it is difficult to claim that the employer can "un-ring" the bell and forget the information. All hiring decisions need to be based upon information that is non-discriminatory and is a valid predictor for job performance.

When using Internet for employment screening, recruiters could be accused of discrimination by disregarding online profiles of job candidates who are members of protected classes based on prohibited criteria. A job candidate may reveal information that reflects race, creed, color, nationality, 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. There may even be photos showing a physical condition that is protected by the Americans with Disabilities Act (ADA) or showing someone wearing garb suggesting their religious affiliation or national origin. All of these protected aspects of applicants may be revealed by a search of the Internet.

"When using Internet for employment screening, recruiters could be accused of discrimination by disregarding online profiles of job candidates who are members of protected classes based on prohibited criteria."

Of course, the analysis is complicated by the fact that the aggrieved job applicants may have placed the information on the web themselves. However, it would be challenging to suggest that a person somehow consented to discrimination by placing material on the web that was then used illegally by employers. Until Courts rule on these issues, employers can only try to apply established legal concepts to their online recruiting efforts.

A related issue is whether a firm is treating all applicants in a similar fashion. If employers 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, an employer 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. If a site shows that an applicant has a tattoo or a piercing, employers may need to ask themselves whether having a tattoo is really a good reason not to hire someone.

The problem is that once an employer is aware that an individual is a member of a protected group, they may be exposed to "failure to hire" law suits based upon discrimination or Equal Employment Opportunity Commission (EEOC) claims.

2. Too Little Information (TLI)

On the other hand, a failure to utilize all the available resources could potentially expose employers to lawsuits for negligent hiring if a victim could show that information was easily accessible online that could have prevented a hiring a person that was dishonest, unfit, dangerous, and unqualified, and it was foreseeable that some harm could occur. In other words, employers that do NOT use such web sites can potentially be sued for not exercising due diligence.

For example, if an organization is hiring for a position that involves access to children, and a simple web search may have revealed that the applicant belongs to a group or has written blogs that approve of inappropriate relationships with children, that employer could be at risk for a lawsuit by failing to go on a computer and locate the material. If the employee harms a child, and a lawsuit results, the victim's attorney could argue that the employer failed to exercise reasonable care given the fact that children are very vulnerable and that the employer should have known that the applicant was inappropriate for the job.

This can be a case of Too Little Information (TLI). The result is that employers may be placed in a Catch-22 situation, where they are in trouble if they do use such web sites, and are also in trouble if they do not.

3. Credibility, Accuracy, and Authenticity Issues

"Yet another issue is whether the information found in the Internet about job applicants is even credible, accurate, and authentic – in other words, true."

Yet another issue is whether the information found in the Internet about job applicants is even credible, accurate, and authentic – in other words, true. How does the employer know if it is even true, or just a matter of some people being silly with their friends? The authenticity issue can be that the person said it, but it was not true, or that the applicant was not even the source or subject of the online information.

Employers should keep in mind that the idea behind social network sites is friends talking to friends, and users of these sites have been known to embellish. 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, or 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. Social network sites need to be taken with a grain of salt.

When using Internet for employment screening, how do employers know for sure what is "real" on the Internet? How do employers know that the "name" they found is their applicant's name? They don't.

Even trickier is the issue of third party references to a candidate. If a recruiter or employer goes beyond material that appears to be authored by the applicant, and begins relying upon blogs or pictures posted by others about the applicant, we are entering even more uncertain territories. A third party statement about an applicant is clearly "hearsay" in nature and is inherently subject to greater scrutiny. When a photograph is posted of someone, that is problematic, and there is an issue of whether there was permission to post, and is it even your applicant.[5]

4. "Computer Twins" & "Cyber-slamming"

With more than 300 million Americans today, most people have "computer twins," people with the same 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?

Employers need to make sure what they see online actually refers to the applicant in question. 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 in a chat room, this may be the new phenomena of "Cyber-slamming," where a person can commit defamation without anyone knowing their real identity. Cyber-slamming is online smearing usually done anonymously and includes derogatory comments on websites or setting up a fake website that does not belong to the supposed owner.

For example, with practically no time or effort and at no cost, anyone can set up a blog masquerading as someone else and say anything they want. Short of filing a lawsuit against the Internet Service Provider (ISP) that hosts the blog, in order to obtain records showing the unique IP address of the computer, it is nearly impossible to trace down the person who actually posted the item. Even armed with the IP address, it is extremely difficult as a practical matter to then associate that IP address with a specified account or address, which may even require second lawsuit.

Employers need to be careful that the site they are looking at actually refers to the applicant. In other

[5] If a CRA were to utilize third party comments, then another section of the FCRA comes into play. **FCRA section 606(d)(4)** requires extra precautions when a third party provides adverse information. In such a case, a CRA must either takes steps to insure that the source of information was the best source, or to use reasonable procures to obtain an additional source of information form an additional source with independent direct knowledge. If a search of the Internet shows a criminal record, the CRA must also consider if **FCRA Section 613** applies, which also has special requirements.

words, if negative information about a candidate is found on the Internet or a social networking site, how is the employer supposed to verify that the information is accurate, up-to-date, authentic, and if it even belongs to or applies to the candidate in question?

5. Privacy Issues

Another problem with Internet background checks yet to be fully explored by the courts is privacy. Contrary to popular opinion, everything online is not necessarily "fair game" for employers.

For example, suppose a recruiter or HR professional attended a convention, and after a long day of listening to speakers or walking the trade show, the recruiter has drinks with colleagues at different firms and soon the talk turns to professional subjects, such as how they like their co-workers, their boss, or their company. Of course, at such an informal conversation, no one has signed a Non-disclosure agreement and everyone is talking in a public place. Then suppose one of the recruiter's professional acquaintances proceeds to take what the recruiter considered a private exchange of information between professionals and placed the recruiter's more colorful and derogatory comments on a blog for the world to see. Would the recruiter be offended? Yes. Most reasonable people under such a circumstance would be appalled. Generally accepted standards of normally behavior would dictate that the conversation was meant to be private, even though there was no agreement not to make the information public, even though the conversation took place in a public place. Many people feel the same about their statements made on Internet social media sites.

On the other hand, if users do not adjust the privacy setting so that their social network site is easily available from an Internet search, those users may have a more difficult time arguing that there is a reasonable expectation of privacy.

In addition, the terms of use for many social network sites prohibit commercial use and many users literally believe that their social network site is exactly that, a place to freely socialize. The argument would be that it is the community norm, and a generally accepted attitude, that social media sites are off limits to unwelcome visitors even if the door is left open. After all, burglars can hardly defend themselves on the basis that the front door to the house they stole from was unlocked so they felt they could just walk in. Furthermore, failure to adjust privacy setting does not mean that an applicant has consented to be the victim of discrimination. As a general rule, a consumer cannot comet to discrimination, and certainly, an implied consent based upon a fiacre to adjust privacy settings would be a weak employer argument.

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. Even though they communicate and share photos in a forum that can be public, there is sense that what goes on in social networking sites like 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. Also, these types of websites have "terms of use" that 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, employers 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.

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 people seeing friends near lockers, they 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.

This issue is 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.

Until the courts sort this out one thing does seem certain: If an employer uses subterfuge, such as creating a fake online identity to penetrate a social network site, the privacy line has probably been crossed.

6. Requiring Applicants to Provide Facebook or Other Social Media Passwords

One prime example of a privacy issue that has made news headlines recently is the practice by some employers of asking job applicants to provide login information such as usernames and passwords for their Facebook page and other social media websites.

In 2009, Bozeman, Montana made international headlines when local media reported that the city government's background check had requested that job candidates provide their usernames and passwords for social networking sites for a few years. The background check form stated: "Please list any and all current personal or business websites, web pages or memberships on any Internet-based chat rooms, social clubs or forums, to include, but not limited to: Facebook, Google, Yahoo, YouTube.com, MySpace, etc."

Although the city said the information was not actually sought until a conditional job offer, overwhelmingly negative reactions to the city's policy raised privacy and free speech concerns for job applicants. A poll indicated 98 percent of respondents believed the city's policy had amounted to an invasion of privacy. The City of Bozeman later dropped the requirement until it conducted a more comprehensive evaluation of the practice.

More recently, news stories have appeared concerning background checks in the digital age where prospective businesses, government agencies, and colleges are increasingly curious about the online life of potential workers and students. While it is common for some employers to review publically available Facebook, Twitter, and other social networking web sites to learn about job candidates, many users have their social media profiles set to 'private' which makes them available only to selected people or certain networks and more difficult for employers to view.

Although online privacy is an evolving area of law, employers need to tread carefully in the area of social media background checks since they may open themselves up to discrimination claims if the social network site reveals an applicant's membership in a protected group such as race, nationality, ethnicity, religious afflation, marital status, and medical condition. Employers should also formulate clear policies and procedures to ensure they are looking for factors that are valid predictors of job performance.

Unless an applicant is applying for a position that requires a security clearance, or public safety is involved such as law enforcement, employers need to be very careful in asking applicants for their Facebook or other social media passwords. It is difficult to see how turning over such information is voluntary in the context of a job interview, where the choice is to hand it over or not get the job. If a lawsuit is filed, an applicant can alleged an invasion of privacy, by intrusion into private and personal information where an applicant would show they had a reasonable expectation of privacy. The employer would then have the burden to demonstrate both that such a request was justified, and that a less intrusive means to make the employment decision was not available. That could be a difficult standard for an employer to meet given all of the hiring tools at an employer's disposal.

7. Legal "Off Duty" Conduct

Yet another issue is legal off-duty conduct. If a social media search reveals legal off duty conduct, a candidate can claim they were the victims of illegal discrimination. A number of states protect workers engaged in legal off-duty conduct and 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.

8. What is "Fair Game" on the Internet?

Employers should not simply assume that anything on the web is "fair game" and freely available without consequence. One area where an employer 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 the user's own network. If an employer were to violate Facebook rules and create fake identities just to join a network belonging to a job applicant, that would likely cross over into the realm of employer behavior that is overly intrusive and invades too deeply into private matters.

All of these concerns are just the tip of the iceberg when it comes to social network background checks. Employers need to be very careful when it comes to harvesting information about job candidates from the internet. Employers need to know how to protect themselves against allegations of discrimination and issues with authenticity, accuracy, credibility, and privacy if no further action is taken after the discovery on the Internet that a person is a member of a protected class or when finding negative information. How and when an employer obtains such information is critical.

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 someday 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. The bottom line: Before using the internet to screen candidates, or using third party services, see your labor attorney.

9. Should Background Screening Firms Conduct Internet Background Checks?

It appears that a new industry is popping up, whereby employers can go to third party firms that will scour the internet and locate and assemble a dossier on an applicant's cyber identity. These "social network background checks" will search social networking sites like Facebook and Twitter, blogs, and anywhere else on the Internet for information about job applicants, including things they may have put online years ago and completely forgotten about.

For employers, this can appear to be a valuable service. Failure to utilize these social networking sites when a search could have revealed relevant information could expose an employer to claims of negligent hiring. The argument is also made that many employers are already doing such searches informally, and may not be following best practices to prevent potentially unlawful use of these sites. By outsourcing to a third party, an employer is shielding themselves from allegations of discrimination since they are not viewing potentially discriminatory or irrelevant information.

Firms providing this service may offer to go online for the employer and filter out any information that is either potentially discriminatory or not job related. This may be done by live researchers, or perhaps by automation, based upon key words and phrases. The advantage is that a third party firm undertakes the burden of looking for relevant information and at the same time relieves employers from the legal liability of viewing materials that are inappropriate. Of course, questions can arise as the ability of either human or computer software to actually evaluate what is real or relevant and to give each employer material that may be of particular relevance to them.

However, companies providing social network background checks present a number of challenging questions that HR professionals and recruiters will need to deal with.

Employers should realize that background firms using social media information must follow the federal Fair Credit Reporting Act (FCRA) rules regulating the collection, dissemination, and use of consumer information. A June 2011 blog on the Federal Trade Commission (FTC) website, 'The Fair Credit Reporting Act & Social Media: What Businesses Should Know,' indicated that background checks using information found with online search engines and on social networking sites must follow the same FCRA rules that apply to the more traditional information that FCRA compliant background screening firms and employers have used in the past.

The FTC blog includes the following paragraph to remind users of Internet background checks of their duty to comply with the FCRA:

- ☑ ***"Employment background checks can include information from a variety of sources: credit reports, employment and salary history, criminal records – and these days, even social media. But regardless of the type of information in a report you use when making hiring decisions, the rules are the same. Companies providing reports to employers – and employers using reports – must comply with the Fair Credit Reporting Act."***

Under the FCRA section 603(f), a CRA can be a third party firm that engages in the "assembling or evaluation" of consumers for employment. When a firm is reviewing the internet to create a report about a job applicant's online information for purpose of employment, that is clearly a background report (also known as a "consumer report") under the FCRA. That means that these types of services are essentially background checking firms, with all of the same legal duties and obligations of any other background check firm. Therefore, such sites need to have full FCRA compliance, including client certifications

under FCRA section 604 as well as adverse action notices and numerous other obligations such as re-investigation upon request. Background checking is subject to heavy legal regulation.

Although employers may request that background screening firms perform this function, there are a number of drawbacks.

1. First, a background screening firm does not have the same in-depth knowledge the employer has of the details of the position.

2. If a social network background check is done by a background screening firm, the search falls under the federal Fair Credit Reporting Act (FCRA) which requires a background screening firm to maintain reasonable procedures for maximum possible accuracy.

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

4. A background screening firm performing the search falls under the Accuracy and Relevancy requirements of the FCRA.

FCRA Section 607(b) sets forth in no uncertain terms the duty of a CRA to be accurate. The section reads:

> (b) *Accuracy of report.* Whenever a consumer reporting agency prepares a consumer report it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.

That section means that the accuracy requirement applies to both the information reported, and the duty to ensure it is being reported about the right person.

Congress drove this point home even further in statement of **Congressional findings and statement of purpose** contained in section **602**:

> (b) *Reasonable procedures.* It is the purpose of this title to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, *relevancy*, and proper utilization of such information in accordance with the requirements of this title. (Emphasis added.)

The use of the word “relevancy” in the FCRA further underscores the need for a background check firm to ensure that reasonable steps are taken to only report information relevant to the consumer.

The issue is that it is inherently difficult for a background check firm know if the information online was authored or authorized by the applicant or applies to the applicant.

5. Another issue is that if a consumer disputes that an item on a social networking was authored by the applicant, the Consumer Reporting Agency would have barriers in the dispute process. Under FCRA Section 611, any consumer can dispute the accuracy contents of a consumer report. The CRA then has 30 days (and no more than 45 if a consumer provides supplemental information) to either verify the accuracy of the data or, if unable to do so, remove it. If a consumer disagrees with information from a social networking site, the question arises as to how a CRA can verify that such material belongs to the applicant. Trying to locate what is “real” in the cyber world is very tricky. Although every computer has an ”IP” address, as a practical matter it is very difficult to locate the precise location of an actual computer short of issuing subpoena as part of a lawsuit. Even if the actual computer is found, there can be an additional issue of who was using it if it was at public location.

   As a result, a CRA may end up having to remove the material from the social networking report if there is dispute because of the difficulty of proving it was the consumer that made the entry.

   A strong argument can be made that a CRA that inserts information in a consumer report that it knows, or reasonably should know, cannot withstand a request for re-investigation and would have to be removed, would be a violation of the FCRA’s accuracy requirements. In other words, a CRA should not place in a report

anything it cannot defend if a request for a re-investigation is made.

Because a background screening firm has no way of knowing if the online information is accurate, authentic, or even belongs to the job applicant in question, it is difficult for background screening firms to perform this service consistent with the FCRA. In other words, due to the FCRA, background screening firms may not be best suited to perform these types of 'social network background checks.'

Employers should carefully consider the pros and cons of outsourcing this task to a background screening firm. The solution may well be that employers **should** do the search in-house utilizing approaches and techniques outlined in this whitepaper.

Solutions for Using Internet Background Checks

1. Solutions for Employers

The considerations for employers using the Internet are different then recruiters.

> *"The safest path is to obtain consent from the candidate first and only search once there has been a conditional job offer to that candidate."*

For employers that want to use social network sites to screen a candidate, and do not want to use a background screening firm, the safest path is to obtain consent from the candidate first and only search once there has been a conditional job offer to that candidate. This procedure helps ensure that impermissible information was not considered before the employer evaluates a candidate using permissible tools such as interviews, job-related employment tests, references from supervisors, and a background check. In other words, it demonstrates that an employer used permissible criteria that were objective, and neutral as to protected classes.

At that point, after using permissible screening tools, the reason for employers to search social networking sites would be to ensure that there is nothing that would eliminate the person for employment.

This approach is also is consistent with the Americans with Disabilities Act of 1990 (the "ADA") and similar state laws. Under the ADA, an employer may only inquire about medically related information once there has been a real job offer. Per the EEOC:

"A job offer is real if the employer has evaluated all relevant non-medical information which it reasonably could have obtained and analyzed prior to giving the offer." (http://www.eeoc.gov/policy/docs/preemp.html)

By analogy, waiting until there has been a job offer helps to guard against an inference that an employer was using impressible criteria in deciding who was finalist.

Reasons for an employer eliminating an applicant for employment or withdrawing the job offer would then need to be based upon the use of social networking and internet searches that showed an applicant engaging in behavior that damages the company, hurts business interests, or is inconsistent with business needs. Example of such behavior could include matters such as:

1. Disparaging a co-worker or supervisor during past employment;
2. Engaging in online harassment;
3. Admitting illegal conduct;
4. Engaging in online harassment;
5. Information showing dishonest behavior;
6. Information showing falsehoods in the application or interview process; or
7. Information on the web that shows poor judgment or communication skills.

This is not a complete list, but what all of these factors have in common is that there is a clear nexus between what is found online, and the job. In other words, there is a rational and articulable business justification.

Another method employers may use is to have a person in-house not connected to any hiring decisions review social network sites, in order to ensure impermissible background screening information is not given to the decisions maker. The in-house background screening should also have training in the non-discriminatory use of background screening information, knowledge of the job description and use objective methods that are the same for all candidates for each type of position.

That way, only permissible information is transmitted to the person that is making the decision. Again, this is best done post-offer but pre-hire and with consent. An employer may be looking for online information concerning upon job suitability. For example, did the potential employee say derogatory things about past

employers or co-workers, or demonstrate that he or she is not the best candidate for the job.

To minimize the risks of using the Internet for background checks, Employment Screening Resources (ESR) – a nationwide background screening provider accredited by The National Association of Professional Background Screeners (NAPBS®) – offers the following steps for employers to take when considering using search engines or social network sites for screening:

- ☑ **Using the Internet to screen candidates is not risk-free, especially when it comes to social networking sites. News travels fast on the web, and employers who rely too much upon social networking sites may find that job applicants are not as eager to look at their firm.**
- ☑ **If an employer uses social media searches, they should first consult their attorney in order to develop a written policy and fair and non-discriminatory procedures designed to locate information that is a valid predictor of job performance and non-discriminatory. Employers should focus on objective criteria and metrics as much as possible.**
- ☑ **Employers should have written job descriptions that contain the essential functions of the job, as well as the knowledge, skills, and ability (KSA) required for the job.**
- ☑ **The employer should have ongoing and documented training on how to avoid discriminatory hiring practices. Documentation is the key, since as general rule, if something is not documented, it becomes very difficult to argue that it existed. The employer should have records of information such as the date and time of the training, who attended, who taught, and the materials used.**
- ☑ **As a general rule, the later in the hiring process social media searches are 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 for a social media search until AFTER there has been a conditional job offer to demonstrate that all applicants were considered utilizing legal criteria that were neutral when it comes to prohibited criteria.**
- ☑ **Employers need to be concerned if information found online is potentially discriminatory to job candidates who are members of protected classes based on prohibited criteria such as: race, creed, color, sex (including pregnancy), ancestry, nationality, medical condition, disability, marital status, sexual preference, or age (40+). All of these protected criteria may be revealed by a social media search.**
- ☑ **Employers need to be concerned if information found on the Internet violates state laws concerning legal "off duty" conduct.**
- ☑ **For legal protection, the most conservative approach is to perform a social media search only after consent from the job applicant and a job offer is made contingent upon completion of a background check that is satisfactory to the employer.**
- ☑ **Employers should not use any fake identities or engage in "pretexting" to gain access to information online.**
- ☑ **Whatever an employer's policy is regarding social media searches, 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 the Internet for an applicant's online identity.**
- ☑ **Employers should also consider the use of a person in-house not connected to hiring decisions to review social media sites in order to ensure impermissible or discriminatory information is not given to decision makers. The in-house reviewer should also have training in the non-discriminatory use of online information, knowledge of the job description, and use objective methods that are the same for all job candidates for each type of position. That way, only permissible information is transmitted to the person making the decision. The person in-house conducting the review is on the other side of an "ethics" wall from any decision maker and helps prevent allegations that impermissible information was used in the hiring process.**
- ☑ **As an additional protection, an employer may consider having the in-house reviewer first contact the applicant with any potential information found online before it is passed along to the decision maker in order to allow the applicant the opportunity to dispute the accuracy or applicability of the information.**

2. Solutions for Recruiters

If recruiters use social network sites for background screening, then Employment Screening Resources (ESR) suggests they realize that much of the 'new media' available to them for background screening is still covered by current employment regulations.

Recruiters in the sourcing stage may want to consider having a clear internal policy and documented training that Internet sourcing is not being used in violation of

federal and state discrimination laws and that only factors that are valid predictors of job performance will be considered, taking into account the job description, and the Knowledge, Skills, and Abilities (KSA) required for the position. It also helps to have objective and documented methods and metrics on how to source and screen on the Internet.

Recruiters considering using in the sourcing stage may want to consider some of the following:

- ☑ **Ensure each position has a detailed job description written for that specific position that clearly lays out the essential functions of the job and the knowledge, skills, and abilities (KSA) required for the position.**
- ☑ **Have a clear internal policy that internet sourcing is NOT being used in violation of federal and state discrimination laws and that only factors that are a valid predictor of job performance will be considered, taking into account the job description and the KSA required for the job.**
- ☑ **Have documented training on legal recruiting techniques. The training should include clear information on what would constitute a discriminatory practice.**
- ☑ **Have a clear procedure that outlines key words, criteria, and methodology for sourcing, so recruiters can demonstrate that they are searching for objective requirements to be considered as part of the pool. Even better is if the criteria being used can be measured or have a metric attached.**
- ☑ **If someone meets the objective requirements but is not placed in the pool of potential candidates for other reasons, a recruiter may want to note why the exception is being made. For example, if the social networking web site demonstrated behavior inconsistent with business interests, that should be noted.**

For recruiters, it also could be argued that if a passive job candidate not actively looking for work is passed over because of discriminatory criteria revealed on a social network site, how they can be harmed, since they did not even know they were disregarded and are none the wiser. The problem with that approach is three-fold.

- ☑ **First, discrimination and civil rights laws would likely still apply, even in recruiting passive candidates.**
- ☑ **Second, there are few secrets in the world. If a firm is using discriminatory criteria, a member of the recruiting team who feels uncomfortable about such a practice may well say something – either publicly on the web, or within the organization.**
- ☑ **Third, it can be argued that discriminatory criteria were being used if it turns out that the entire workforce happens to be homogeneous and does not include members of protected classes. Such a statistical anomaly could suggest a pattern of discrimination.**

3. Solutions for Job Applicants

For job applicants, the advice is simple: Don't be the last to know what a web search about you would reveal. If job applicants do not want employers looking at their social networking site, then they should set the privacy parameter to "restricted use only." Savvy applicants can even go on the offense and create an online presence that helps them get a job.

Study Claims Social Network Profiles on Facebook may Predict Future Job Success

A February 2012 study in the Journal of Applied Social Psychology – 'Social Networking Websites, Personality Ratings, and the Organizational Context: More Than Meets the Eye?' – claims that a quick review of social networking website (SNW) profile pages of job applicants on sites such as Facebook can be a better predictor of job success than standardized tests currently used by many human resources departments. The authors of the study examined the psycho-metric properties of the 'Big Five' personality traits assessed through social networking profiles in two studies of SNW users:

- ☑ **Extraversion.**
- ☑ **Agreeableness.**
- ☑ **Conscientiousness.**
- ☑ **Emotional stability.**
- ☑ **Openness.**

The study involved trained "raters" who spent five to ten minutes evaluating 274 Facebook pages of job candidates and answering questions related to personality. The researchers followed up six months later for performance reviews from the supervisors of 69 of the job candidates – approximately 25 percent of the original group – and found that the quick Facebook evaluations more accurately predicted success than standard tests. An excerpt from the study explains more: "Those high in agreeableness are trusting and get along well with others, which may be represented in the extensiveness of personal information posted. Openness to experience is related to intellectual curiosity and creativity, which could be revealed by the variety of books, favorite quotations or other posts showing the

user engaged in new activities and creative endeavors. Extroverts more frequently interact with others, which could be represented by the number of SNW (social networking websites) friends a user has."

The study 'Social Networking Websites, Personality Ratings, and the Organizational Context: More Than Meets the Eye?' is available at this link: http://onlinelibrary.wiley.com/doi/10.1111/j.1559-1816.2011.00881.x/pdf.

Bottom Line with Internet Background Checks: Proceed with Caution

Caution should be exercised when using the Internet for employment screening background checks. There has yet to be a clear law or court cases that set forth how to proceed in this area. In the meantime, employers and recruiters may want to approach the Internet with some caution before assuming that everything is fair game in the pursuit of passive candidates.

The bottom line when using the Internet for employment screening background checks is: Proceed with Caution. Employers should use Internet background checks with extreme caution or otherwise face potential legal landmines that could harm their business.

> *"The bottom line when using the Internet for employment screening background checks is: Proceed with Caution."*

About Employment Screening Resources (ESR)

Employment Screening Resources (ESR) – 'The Background Check Authority℠' – provides accurate and actionable information, empowering employers to make informed safe hiring decisions for the benefit for our clients, their employees, and the public. ESR literally wrote the book on background screening with "The Safe Hiring Manual" by Founder and CEO Lester Rosen. ESR is accredited by The National Association of Professional Background Screeners (NAPBS®), a distinction held by less than two percent of all screening firms. By choosing an accredited screening firm like ESR, employers know they have selected an agency that meets the highest industry standards. For more information about ESR, visit http://www.esrcheck.com/ or call 415.898.0044.

About the Authors

- **Attorney Lester S. Rosen is the Founder and CEO of Employment Screening Resources (ESR). He is the author of 'The Safe Hiring Manual,' the first comprehensive guide for employment screening. He is a recognized safe hiring expert and a frequent presenter nationwide through the 'ESR Speaks' program on background checks. He was the chairperson of the committee that founded the National Association of Professional Background Screeners (NAPBS). Mr. Rosen can be reached at lsr@ESRcheck.com.**
- **Thomas Ahearn is the ESR News Blog Editor – http://www.ESRcheck.com/wordpress/ – and Social Media Manager at Employment Screening Resources (ESR). Email Thomas at tahearn@esrcheck.com.**

Sources:

- http://www.esrcheck.com/wordpress/2009/08/01/the-rush-to-source-candidates-from-internet-and-social-networking-sites-2/
- http://www.esrcheck.com/wordpress/2011/01/25/employers-firing-employees-over-information-found-on-popular-social-media-sites-face-legal-risks/
- http://online.wsj.com/article/SB10001424052748703954004576089850685724570.html
- http://thehiringsite.careerbuilder.com/2009/08/20/nearly-half-of-employers-use-social-networking-sites-to-screen-job-candidates/
- http://www.esrcheck.com/wordpress/2010/12/21/esr-background-screening-trend-6-for-2011-using-social-network-sites-such-as-facebook-to-screen-job-candidates-increases-legal-risk-for-employers/
- http://www.esrcheck.com/wordpress/tag/social-networking-sites/
- http://www.esrcheck.com/Top-Ten-Trends-In-Background-Screening-2011.php
- http://www.esrcheck.com/wordpress/2010/09/29/social-network-background-checks-of-job-applicants-present-challenges-for-employers-and-recruiters/
- http://www.esrcheck.com/wordpress/tag/social-networking-sites/page/2/
- http://www.esrcheck.com/wordpress/2010/07/14/can-recruiters-or-employers-rely-on-business-connecting-sites-instead-of-background-checks/
- http://www.esrcheck.com/articles/Caution-Using-Search-Engines-MySpace-or-Facebook-for-Hiring-Decisions-May-Be-Hazardous-to-Your-Business.php
- http://business.ftc.gov/blog/2011/06/fair-credit-reporting-act-social-media-what-businesses-should-know
- http://www.microsoft.com/presspass/features/2010/jan10/01-26DataPrivacyDay.mspx?rss_fdn=Top%20Stories
  - http://news.cnet.com/8301-13578_3-10268282-38.html
  - http://news.cnet.com/8301-13578_3-10269770-38.html
  - http://news.yahoo.com/job-seekers-getting-asked-facebook-passwords-071251682.html
  - http://www.shrm.org/Research/SurveyFindings/Articles/Pages/TheUseofSocialNetworkingWebsitesandOnlineSearchEnginesinScreeningJobCandidates.aspx
  - http://www.esrcheck.com/wordpress/2011/09/21/two-us-senators-voice-privacy-concerns-over-background-check-firm-storing-web-footprints-of-consumers-for-employment-screening/
  - http://onlinelibrary.wiley.com/doi/10.1111/j.1559-1816.2011.00881.x/pdf