WHITEPAPER:
Ten Potential Dangers When Using Social Media Background Checks

By Lester Rosen, Esq.
Employment Screening Resources (ESR)

ESR
EMPLOYMENT SCREENING RESOURCES®

Phone: (415) 898-0044
Toll Free: (888) 999-4474
http://www.esrcheck.com

WHITE PAPER:
Ten Potential Dangers When Using Social Media Background Checks

Introduction

These days no discussion about employment screening is complete without an analysis of how so-called "social media background checks" can be used for uncovering a treasure trove of information about job candidates. Employers can harvest information from a variety of social media sites such as Facebook, YouTube, Google+, LinkedIn, and Twitter, as well as forums, sharing services, and discussion boards.

Many employers have focused with laser-like intensity on using the plentiful amount of information found online. Using social media sites, they believe they are effectively able "to look under the hood" and "get into an applicant's head." Unlike traditional hiring tools such as interviews and contacting past employers, social media sites hold out the promise of revealing the "real" job applicant.

Social Media is also used extensively for sourcing and recruiting as well. Since recruiting occurs earlier in the hiring process, some of the practical issues are different but there are still serious legal pitfalls and traps that need to be considered.

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

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

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 position of the National Labor Relations Board (NLRB) is also an important consideration for a post-hire social media policy. Such a policy can touch on issues that include:

- ☑ 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?

ESR
EMPLOYMENT SCREENING RESOURCES®

Phone: (415) 898-0044
Toll Free: (888) 999-4474
http://www.esrcheck.com

WHITE PAPER:
Ten Potential Dangers When Using Social Media Background Checks

Social Networking Screening Ground Rules Can Change at Any Moment

Part of the risk of using social media for background checks is that the area is so new that courts and legislators have not yet fully entered into the act. 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, employers are lacking clear court decisions on issues concerning 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. Courts can also disagree and have conflicting decisions. As a general principal, it takes decisions from a number of courts for clear ground rules to begin to emerge.

Congress has not 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. State legislators have passed laws regulating the ability of employers to request applicant passwords, but have also largely left the area unregulated so far.

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 terms of privacy 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.

Uncertainty abounds since courts and legislators have not caught up with social media and the ground rules can change at any time without notice.

At this point, given the lack clear of legal precedents or legislative mandate, the best that can be done is to take known existing laws and legal principals and extrapolate their probable impact on the use of social media by employers.

ESR
EMPLOYMENT SCREENING RESOURCES®

Phone: (415) 898-0044
Toll Free: (888) 999-4474
http://www.esrcheck.com

WHITE PAPER:
Ten Potential Dangers When Using Social Media Background Checks

The Social Media Explosion

"Social media" is defined as forms of electronic communication such as Web sites for social networking and microblogging through which users create online communities to share information, ideas, messages, and other content such as videos. An important trend is that social media is not just for "young" people any more, defined as the 18-29 year old age group. Social media is incredibly popular with 78 percent of online adults in the 30-49 age group and 55 percent in the 50-64 age group using social networking sites as of September 2013, according to a Pew Internet Project Social Networking Fact Sheet (http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/).

Due to the growing popularity of social media, employers would be hard pressed to completely ignore such an enormous amount of available online information when screening prospective new hires. Some of the popular social media websites in terms of usage include the following (data from Wikipedia.org and subject to change):

Many social media sites allow the owner or subscriber to set privacy settings to restrict members of the public from viewing the content in whole or in part. Other social media sites allow the world to view the material without restriction.

Phone: (415) 898-0044
Toll Free: (888) 999-4474
http://www.esrcheck.com

WHITE PAPER:
Ten Potential Dangers When Using Social Media Background Checks

Social Media Hurts AND Helps Job Candidates

The 2015 Annual CareerBuilder Social Media Recruitment Survey found more than half of employers – 52 percent – used social media to research job candidates while more than one-third – 35 percent – were less likely to interview job candidates if they were unable to find information about them online.

Nearly half of hiring managers – 48 percent – found information online that caused them not to hire a candidate that included:

- Provocative or inappropriate photographs – **46 percent**
- Information about candidate drinking or using drugs – **40 percent**
- Candidate bad-mouthed previous company or fellow employee – **34 percent**
- Poor communication skills – **30 percent**
- Discriminatory comments related to race, religion, gender, etc – **29 percent**

Almost one-third of hiring managers – 32 percent – found information online that caused them to hire a candidate that included:

- Candidate's background information supported job qualifications – **42 percent**
- Candidate's personality a good fit with company culture – **38 percent**
- Candidate's site conveyed a professional image – **38 percent**
- Candidate had great communication skills – **37 percent**
- Candidate was creative – **36 percent**

The research suggests hiring managers are using social media to glimpse the candidate's behavior and personality outside of the interview and to see how the candidate fits with the company culture.

On the other hand, it seems that social media users are also becoming more sophisticated and are using social media accounts as a job search tool by creating an online presence an applicant hopes employers will find.

ESR
EMPLOYMENT SCREENING RESOURCES®

Phone: (415) 898-0044
Toll Free: (888) 999-4474
http://www.esrcheck.com

WHITE PAPER:
Ten Potential Dangers When Using Social Media Background Checks

Job seekers who believe the information they post on public social media websites does not affect their search for employment should think again. A 2016 survey released by the Society for Human Resource Management (SHRM) found employers used the Internet and social media more than ever to recruit and screen potential employees, and some even disqualified applicants based on social media content.

The survey revealed that 84 percent of organizations used social media to recruit in 2015, up from 56 percent in 2011. In addition, 44 percent of organizations agreed that social media profiles of job candidates provided information about work-related performance while 36 percent rejected a job candidate because of "concerning information" found on a public social media profile or online search.

More than four out of 10 organizations – 43 percent – used social media or online search engines to screen job candidates in 2015, and the most popular social media used to screen them included:

LinkedIn – **93 percent**
Facebook – **63 percent**
Twitter – **29 percent**
Professional or association social networking sites – **29 percent**
Google+ – **26 percent**

The top reasons for organizations to screen social media profiles of job candidates included:

Obtaining more information about the applicant than provided in a resume – **61 percent**

Easily verifying information from a resume – **50 percent**

Candidates including their social media sites on resumes– **41 percent**

The little time and effort used related to the information gained – **34 percent**

ESR
EMPLOYMENT SCREENING RESOURCES®

Phone: (415) 898-0044
Toll Free: (888) 999-4474
http://www.esrcheck.com

WHITE PAPER:
Ten Potential Dangers When Using Social Media Background Checks

Ten Potential Dangers When Using Social Media Background Checks

Social media background checks are used now more than ever by employers. The 2015 CareerBuilder survey found more than half of employers – 52 percent – used social media to research job candidates in 2015, up from 39 percent in 2013. In using social media background checks, employers may encounter these ten potential dangers:

- ☑ 1. Too Much Information (TMI) Leading to Discrimination Allegations
- ☑ 2. Too Little Information (TLI)
- ☑ 3. Credibility, Accuracy & Authenticity Issues
- ☑ 4. "Computer Twins" & "Cyber-Slamming"
- ☑ 5. Privacy Issues in a Brave New Online World
- ☑ 6. Requiring Applicants to Provide Social Media Passwords
- ☑ 7. Legal Off-Duty Conduct
- ☑ 8. What is "Fair Game" on the Internet? The Dangers of Pre-Texting and Social Engineering
- ☑ 9. Should Background Screening Firms Perform Social Media Background Checks?
- ☑ 10. Hurting Employer Brand

The following is a discussion of the Ten Potential Dangers When Using Social Media Background Checks:

1. Too Much Information (TMI) Leading to 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 (TMI). The problem is that once an employer is aware an individual is a member of a protected group, it is difficult to claim the employer can "un-ring" the bell and prove that the information whose use would be discriminatory was not considered when rejecting an applicant.

All hiring decisions need to be based upon information that is non-discriminatory and is a valid predictor for job performance. When using the Internet for employment screening, employers could be accused of discrimination by disregarding online profiles of job candidates who are members of protected classes based on prohibited criteria under Title VII of the Civil Rights Act of 1964.

There are also numerous state discrimination laws. 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 or state law. There may even be photos showing a physical condition that is protected by the Americans with Disabilities Act (ADA) or suggesting religious affiliation or national origin. All of these protected aspects of applicants may be revealed by a search of the Internet.

The analysis is complicated by the fact that 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.

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.

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. In March 2014, a panel of experts at a Social Media Commission Meeting at EEOC Headquarters in Washington, D.C said that the growing use of social media by employers, applicants, and employees in the 21st century workplace may implicate and impact the federal laws prohibiting discrimination in employment that the EEOC enforces.

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 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 employers may be placed in a "Catch-22" situation where they are in trouble if they do use social media searches and are in trouble if they do not.

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.

3. Credibility, Accuracy & Authenticity Issues

Another issue is whether information found on the Internet about job applicants is even credible, accurate, or authentic. In other words, 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. In addition, since many social media users utilize pseudonyms, the names on emails do not reveal identity and employers many not even be able to identify a person's online activity. This means that at times looking for social media information is like looking for a very small needle in a very large haystack.

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 if 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.

Also, since applicants have been made aware in the popular media that employers may look online, savvy job applicants may well create a social media presence as part of a self-promotion campaign aimed at assisting their employment efforts. In the alternative, some applicants have locked down their online presence behind privacy settings making it even harder to locate actionable 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.

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

A related issue is "Computer Twins" and "Cyber-Slamming." With the current population in America reaching more than 323 million and the world's population approximately 7.4 billion in 2016, most people have "computer twins," people with the same names and even a similar date of birth. There is also the question of how to even know for sure the applicant actually wrote the item or authorized its posting. Or is the negative information a case of "Cyber-Slamming"?

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 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 in a Brave New Online World

A significant issue with using the Internet to screen applicants is the issue of privacy. The conventional wisdom is that anything online is "fair game" because any reasonable person must understand that the whole world has access to the Internet. If a site permits a consumer to use privacy settings to limit access, failure to adjust their privacy setting to prevent anyone from seeing their postings, may make it more difficult to argue that there is a reasonable expectation of privacy.

However, contrary to popular opinion, there are strong arguments that everything online is not necessarily "fair game" for employers. Even though consumers communicate and share information and photos in a forum that can be accessed in part by the public, there is an argument that what goes on in social networking sites like Facebook is only intended for the user's own personal community and like "what goes on in Las Vegas" should stay there. The argument would be that it is the generally accepted community norm and 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 left 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 if a recruiter or employer finds items that cannot legally be considered in the hiring process. As a general rule, a consumer cannot consent to discrimination, and an employer accused of using social media information in a discriminatory fashion could not argue there was implied applicant consent.

The argument in favor of privacy rights on social media sites 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, "terms of use" on many social media websites 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. Employers can argue however that the routine boilerplate "terms of use language" where someone simply hits the "I agree" button is not much of a privacy barrier. In addition, an employer could argue that if an applicant fails to utilize readily available privacy controls provided by the website, then that undercuts any reasonable belief that what was on the website would remain confidential especially given widespread publicity that such sites are being used by employers. In addition, if a website is primarily a business connection service such as "LinkedIn," where consumers specifically place business related information the entire world is invited to view, then there is less likely to be a reasonable expectation of privacy.

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 and the right to "seclusion from intrusion" from the preying eyes of employers can depend upon the specific facts of the case being litigated. 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 Social Media Passwords

As of August 2015, twenty-two states have enacted laws about social media privacy that apply to employers to prevent them from requesting usernames and passwords to social media websites and personal Internet accounts of employees and job applicants, according to a list of social media password privacy legislation from the National Conference of State Legislatures (NCSL).

The list of states passing legislation to limit employer access to personal online content of employees and applicants is rapidly growing. As of August 2015, twenty-two states – Arkansas, California, Colorado, Connecticut, Illinois, Louisiana, Maine, Maryland, Michigan, Montana, Nevada, New Hampshire, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Virginia, Washington, and Wisconsin – had passed such online privacy protection legislation.

Under these laws, "social media" is broadly defined to include email accounts, photographs, videos, blogs, podcasts, instant messages, electronic mail (e-mail), Internet website profiles, and standard social media websites such as Facebook, Twitter, and LinkedIn. Most of the laws also include exceptions when passwords are necessary to comply with a state or federal law or regulation or to access the employer's own internal computer or information system.

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 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. Bozeman later dropped the requirement until it conducted a more comprehensive evaluation.

Prospective businesses, government agencies, and colleges are increasingly curious about the online life of potential workers and students for background checks in the digital age. While it is common for some employers to review publically available Facebook, Twitter, and other social media 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 an applicant for their Facebook or other social media password. 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 allege 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.

Phone: (415) 898-0044
Toll Free: (888) 999-4474
http://www.esrcheck.com

WHITE PAPER:
Ten Potential Dangers When Using Social Media Background Checks

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? The Dangers of Pre-Texting and Social Engineering

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 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.

Another technique is popularly called "Social engineering." That is term used to describe techniques for using psychological manipulation of people into performing actions or divulging confidential information. An example would be pretending to be a friend just to obtain access to a consumer's password protected area. 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.

9. Should Background Screening Firms Perform Social Media Background Checks?

It appears that a new industry has popped 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 media 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.

WHITE PAPER:
Ten Potential Dangers When Using Social Media Background Checks

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.

Whether a background screening firm can fulfill this function is currently open to some debate. Using background screening firms to provide 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 blog on the Federal Trade Commission (FTC) website, 'The Fair Credit Reporting Act & Social Media: What Businesses Should Know,' indicated background checks using information found with search engines and on social networking sites must follow the same FCRA rules that apply to the more traditional information 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 reviews the Internet to create a report about a job applicant's online information for the purpose of employment, the report created is clearly a background report (also known as a "consumer report") under the FCRA. That means these types of services are essentially background check 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. FCRA Section 607(b) sets forth in no uncertain terms the duty of a CRA to be accurate. The section reads:

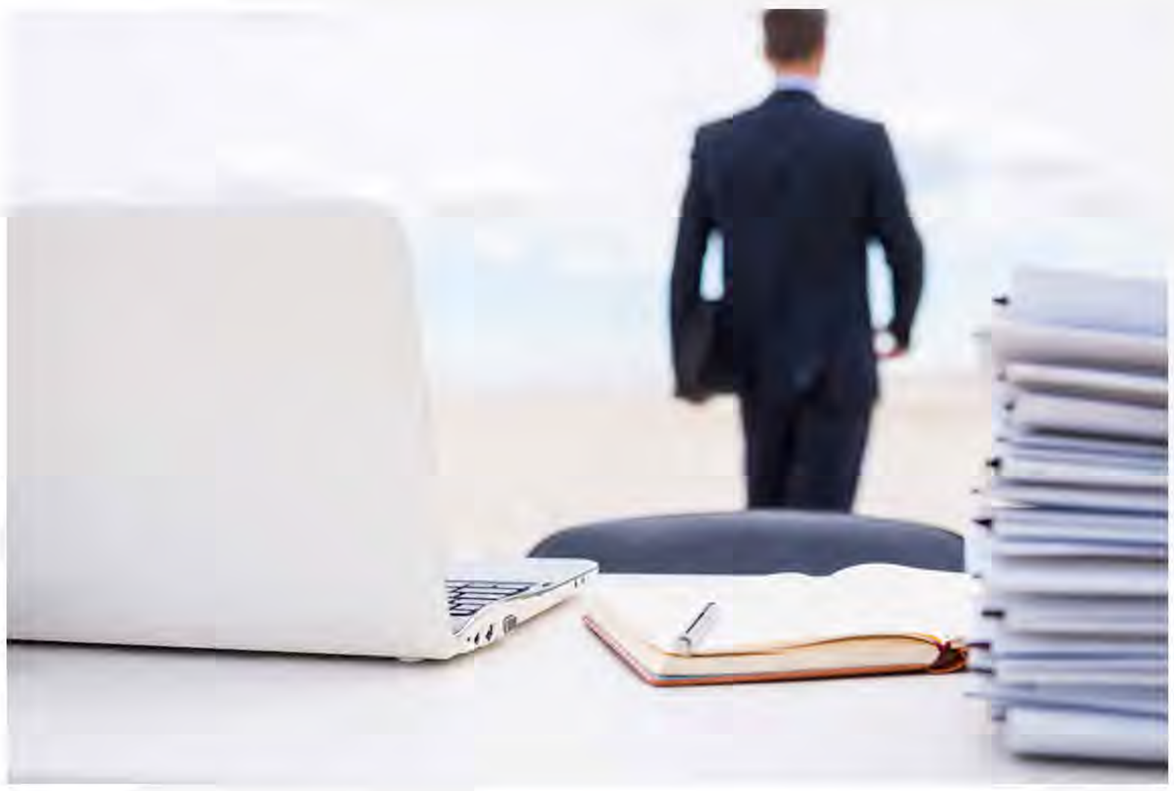
(b) Accuracy of report. Whenever a consumer reporting agency prepares a consumer report it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.

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. In addition, if an applicant disputes a report, a background screening firm has a legal duty to re-investigate and to remove any information it cannot confirm within thirty (30) days and no longer than forty-five (45) days. As a practical matter, 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. Within the tight time deadlines, it may not be possible for a background check firm to discover the information or take steps to acquire the information from an ISP. A screening firm may well have to remove disputed information from the report anytime a consumer objects. The argument can be made that information in a report that cannot be validated if the consumer objects should not be reported in the first place since there are inherent accuracy issues. That is another reason it is difficult for background screening firms to perform this service consistent with the FCRA.

In other words, due to the FCRA accuracy requirements, 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.

10. Hurting Employer Brand

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. Employers may spend a great deal of time and money developing a "brand" to attract the best and most qualified applicants. A use of social media that is perceived as unfair or intrusive can hurt the brand causing good candidates to seek employment elsewhere.



A 2012 study conducted on the effects of screening in the workplace described in the article 'Judging a Facebook by Its Cover' found organizations using social media screening to find the best applicants through sites like Facebook may reduce their attractiveness to applicants and current employees. In the study, 175 students applied for a fake temporary job they believed to be real. After being informed they were screened, applicants were less willing to take a job offer since they felt their privacy was invaded and that the screening reflected negatively on the organization's fairness and treatment of employees.

A use of social media that is perceived as unfair or intrusive can hurt the brand causing good candidates to seek employment elsewhere.

WHITE PAPER:
Ten Potential Dangers When Using Social Media Background Checks

Recruiters are Also Subject to Social Media Pitfalls and Legal Exposure

For recruiters, it also could be argued that if passive job candidates not actively looking for work are 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 this 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.**

Recruiters are in a different situation then a hiring manager or HR Director, since a recruiter is presumably looking online for passive candidates or active jobseekers who have listed their resume. Obviously, the notion of consent does not apply, nor can a recruiter avoid looking at online cyber identities early in the process. However, that means it is even more critical for recruiters to show they are using fair and impartial procedures that are standardized and to try to develop and maintain metrics as to the search methodology. The bottom line for recruiters is that the dangers and pitfalls of a social media use are still present.

Recruiters are in a different situation then a hiring manager or HR Director, since a recruiter is presumably looking online for passive candidates or active jobseekers who have listed their resume.

ESR
EMPLOYMENT SCREENING RESOURCES®

Phone: (415) 898-0044
Toll Free: (888) 999-4474
http://www.esrcheck.com

WHITE PAPER:
Ten Potential Dangers When Using Social Media Background Checks

Solutions for Employers Using Social Media Background Checks

To minimize the potential legal risks of using social media 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:

- ☑ 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. Employers may also consider having a diversity policy as well.

- ☑ 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 information viewed online was used in a discriminatory way. There is an analogy in this approach to how employers review medical related information under the Americans with Disabilities Act (ADA). The later sensitive information is obtained, the less likely it is an employer can be accused of using prohibited criteria in employee selection.

- ☑ 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 if done too early.

- ☑ 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

ESR
EMPLOYMENT SCREENING RESOURCES®

Phone: (415) 898-0044
Toll Free: (888) 999-4474
http://www.esrcheck.com

WHITE PAPER:
Ten Potential Dangers When Using Social Media Background Checks

- A best practice is for employers to standardize their processes to the extent possible for each position, so that similarly situated people are treated in a similar fashion. The general approach and methodology should be standardized so that no one is singled out for special treatment.

- An employer may also consider having the person in charge of social media searches contact an applicant about any negative or derogatory information before passing it on to the decision makers. Although not required by law, it is a practice worth considering.

- 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.

Bottom Line on Social Media Background Checks

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.

About Employment Screening Resources® (ESR)

Employment Screening Resources® (ESR) – 'The Background Check Authority' – is a nationwide screening firm accredited by The National Association of Professional Background Screeners (NAPBS®), a distinction held by a small percent of screening firms. ESR Founder and CEO Attorney Lester Rosen literally wrote the book on background screening with 'The Safe Hiring Manual.' ESR provides effortless legal compliance, proven expertise, less work/lower cost, results you can trust, and painless migration.

For more information about Employment Screening Resources® (ESR), visit http://www.esrcheck.com/call Toll Free 888.999.4474, or email sales@esrcheck.com.

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, and a frequent speaker nationwide on background check issues. He was chairperson of the committee that founded the National Association of Professional Background Screeners (NAPBS). He can be reached at lsr@esrcheck.com.

Thomas Ahearn is Editor of the ESR News Blog and Social Media Manager at Employment Screening Resources® (ESR). To keep up on the latest screening developments, visit ESR News at http://www.ESRcheck.com/wordpress/.
Email Tom at tahearn@esrcheck.com.

Connect with ESR on Social Media