white paper

EMPLOYER ACCESS, USE & REGULATION OF SOCIAL MEDIA

Legal Limitations in Employment Screening

BACKGROUND

In recent years, the intersection of personal social media usage with the workplace has caused a blurring of the lines between the private and professional realm.

Social media, or the form of interactive, online communications in which users generate and share content through text messages, audio and/or video images, is no longer an activity solely engaged in and enjoyed in the privacy of one's own home. Employees are increasingly communicating via Facebook, Twitter and LinkedIn, and employers are seeking to access current and prospective employees' social media accounts in order to learn more about them. The risk of making hiring or other employment decisions using information found on social media sites has become an area of increasing concern for employers. Although nothing in the law currently prohibits employers from searching public social media sites for information about employees and applicants, employers need to tread cautiously in using social media information, balancing the perceived need to obtain information against the risks associated with acting on such information. An employee's or applicant's digital footprint can reveal protected characteristics and employers need to be aware of the employment law implications of using such information. Failure to use social media cautiously and intelligently may give rise to legal exposure.

In addition to seeking information on employees and applicants via their social media accounts, employers are also seeking to regulate the content of employees' social media accounts and a growing number have enacted formal social media policies in order to do so. Many of these employers' policies have been struck down as "overbroad" in their reach of what are considered by the National Labor Relations Board (the "NLRB") to be "protected and concerted activities" under Section 7 of the National Labor Relations Act (the "NLRA"). While employers have wide latitude in monitoring employees' social media activities on employer-provided electronic devices, some have sought passwords to access personal, off-duty social media accounts. Proponents of limiting such access consider it an extreme form of a background check, an invasion of privacy. In May 2012, Maryland became the first state to prohibit employers from asking current or prospective employees for their social media passwords. Illinois, California and Michigan followed suit. To date, 13 states have enacted legislation protecting employees' and/or students' online activities and their right to privacy with similar legislation introduced or pending in at least 19 additional states nationwide.[1]

This white paper will examine the legal limitations surrounding employer access to and regulation of social media accounts as well as the risks entailed by employers using information gleaned from such accounts in making hiring or other employment decisions.

[1] While Colorado, Illinois, Maryland, Nevada, New Mexico, Oregon and Washington passed laws applying to employers, Delaware and New Jersey passed laws that apply to academic institutions. Arkansas, California, Michigan and Utah passed laws that apply to both employers and academic institutions.

SECTION 1: SOCIAL MEDIA BACKGROUND CHECKS

As employers increasingly seek to expand the sphere of information learned about applicants in order to avoid costly hires, many are turning to social media searches to assist in their applicant screening.

According to a 2010 Microsoft-commissioned research study, 79% of U.S. recruiters reviewed online reputational data in screening applicants.[2] In addition to unearthing information that may not be relevant to job performance, social media background checks reveal information about candidates' private lives — information covering age, religion, sexual orientation, disability, national origin and race — that are the same kinds of information that cannot be asked in an interview. By viewing a candidate's blogs, posts, photos and videos, employers open themselves up to information that cannot be legally used in the decision-making process. But the dilemma for employers is that such information cannot be "unseen," and they may find themselves in the difficult situation of having to prove a negative hiring decision was not based on discriminatory information obtained via a social media search.

[2] Cross-Tab Marketing Services, Online Reputation in a Connected World, (January 2010), p. 6.

In addition to the possibility of learning protected information, social media information may not be reliable and is often very difficult to verify. In conducting background screening for employment purposes, accuracy of information is paramount for both employer and employee, and the absence of any inherent reliability reduces the effectiveness of any social media search. The process also lacks the protections afforded an applicant and employee required under the Fair Credit Reporting Act (the "FCRA"). Without a pre-adverse or dispute process, applicants have no forum for correcting inaccurate or false information, or for explaining information that may be construed out of context.

The Federal Trade Commission issued a staff opinion letter emphasizing that FCRA "compliance obligations apply equally in the social networking context," including the requirement that reasonable steps are taken to ensure the maximum possible accuracy of the information reported.[3] While there are companies that purport to conduct social media background searches in compliance with the FCRA, they claim to provide reports based on employer pre-defined criteria, excluding all information not legally allowable for hiring.[4] What is left is information that is inherently suspect, as it can be falsified and manipulated, and the mechanics of which call into question the actual use and practical value of the information sought. If a candidate disputes that a photograph, posting or blog is attributable to him or her, or argues that it has been falsified or an account hacked, an employer finds itself in the same dilemma of having to justify hiring decisions and again open to claims. The nature of the information obtained via social media is inherently unreliable and difficult to verify, and can be very problematic for employers seeking to use it.

With the use of social media for hiring and promotion becoming increasingly common, employers should carefully evaluate whether or not it is in their best business interests to supplement their traditional background screening processes with social media searches.

[3] Jackson, FTC Informal Staff Opinion Letter, May 9, 2011.

[4] According to the CEO of one such company, less than one-third of the data comes from the major social platforms of Facebook, Twitter and Myspace, with much of the negative information obtained from comments on blogs and posts on smaller sites as well as bulletin boards. In addition, photos and videos get most people in trouble. See Jennifer Preston, "Social Media History Becomes a New Job Hurdle," The New York Times (July 11, 2011).

BY VIEWING A CANDIDATE'S BLOGS, POSTS, PHOTOS AND VIDEOS, EMPLOYERS OPEN THEMSELVES UP TO INFORMATION THAT CANNOT BE LEGALLY USED IN THE DECISION-MAKING PROCESS.

And if they ultimately determine to do so, they should prudently consider the legal risks attendant with such an approach.

Things to Avoid When Using Social Media in Hiring:

- Avoid making hiring, retention or other employment decisions based in whole or in part on membership in a protected class (such as race, national origin, religion and age) revealed through social media;
- Avoid seeking access to password-protected social media accounts (see Section 2 below); and
- Avoid discriminating against employees and applicants based on activity protected under the NLRA revealed through social media (see Section 3 below).

Protocols for Using Social Media in Hiring:

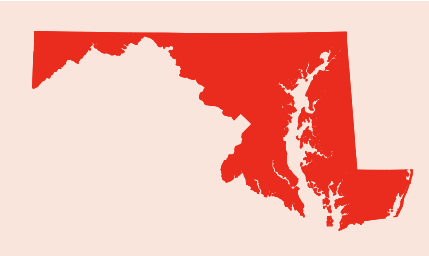
- Use the same protocols for social media screening of applicants or employees no matter their race, gender or other protected class status to avoid disparate treatment liability;
- Make hiring, retention or other employment decisions using accurate and verified information only, understanding that information posted on social media sites is often false or misleading;
- Comply with the FCRA and its state equivalent, if applicable, even if conducting searches in-house; and
- Ensure compliance with the "terms of use" policies of social media websites.

SECTION 2: STATES' & FEDERAL PASSWORD PRIVACY LAWS

In addition to employers seeking to perform social media background searches on prospective and current employees, some have also sought access to social media accounts.

For existing employees, there are instances where employers have legitimate business interests in gaining access. First and foremost, they cite the need to monitor activity in order to protect trade secrets and other proprietary and confidential data. In addition, employers seek to minimize their exposure to risk and legal liabilities and may have a duty to investigate employees' online activities if, for instance, an employee is harassing another or engaging in illegal activity. Some employers need to comply with federal financial regulations and disclosure laws (pursuant to SEC regulation or FINRA social media rules regarding advertising, for example). And employees may still have obligations to employers outside of the office, including maintaining confidential information. While employers generally monitor company systems to make sure employees aren't disclosing proprietary information, engaging in illegal activity or harassing others, they also want to learn as much as possible about prospective employees in order to avoid costly hires.

Those who support limiting an employer's ability to access personal social media accounts, for whatever reason, consider it an extreme form of a background check, an invasion of privacy. Maryland's May 2012 law prohibiting employers from asking current or prospective employees for their passwords was the first of its kind, and was soon mirrored in Illinois, California and Michigan. The enacted legislation generally prohibits employers from seeking access to social media accounts by requiring applicants or employees to disclose usernames or passwords, while still preserving employers' rights to request and require access to employer-provided electronic equipment or in the event the employer has specific information about activity necessitating an investigation. Similar legislation has been enacted in 10 additional states nationwide.



MARYLAND

Maryland's "User Name and Password Privacy Protection Act," which took effect October 2012, prohibits employers from requesting or requiring "that an employee or applicant disclose any user name, password or other means for accessing a personal account or service through an electronic communication device." Employers may, however, require an employee to disclose any of the same for accessing "nonpersonal accounts or services that provide access to the employer's internal computer or information systems." Nothing in the law interferes with the employer's ability to protect its own systems.

Employers' concerns are also addressed and employers' rights are reinforced under the law — employees are prohibited from downloading unauthorized proprietary information of the employer or financial data to a personal website, Internet website or Web-based or similar account. If employers learn of such unauthorized downloading, they can investigate an employee's actions and seek to ensure compliance with applicable securities or financial law or regulatory requirements.

ILLINOIS

Illinois passed a similar law in August 2012 that took effect January 1, 2013. The law makes it unlawful for any employer to request, require or demand any employee or prospective employee to provide any password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking website. It doesn't protect personal emails, however, and leaves open the possibility for employers to demand access to a private email account.

The Illinois law does not have any exceptions for employers to access social media information — not even for work-related investigations of misconduct or harassment or for other legitimate business reasons. Employers can, however, obtain publicly-available information as well as protect their own electronic equipment and email.

CALIFORNIA

In September 2012, California was the first state to endorse a comprehensive social media privacy law that prohibits employers as well as public and private postsecondary educational institutions from demanding access to social media (defined to include email). Employers and postsecondary educational institutions are prohibited from requiring or requesting an employee or applicant to (i) disclose

a username or password for the purpose of accessing personal social media, (ii) access personal social media in the employer's presence (a practice known as "shoulder surfing") and (iii) divulge any personal social media, other than personal social media reasonably believed to be relevant to an investigation of allegations of employee or student misconduct or employee violation of laws. The law does not preclude employers from requiring or requesting an employee, however, to disclose usernames or passwords for the purpose of accessing an employer-issued device.

MICHIGAN

Effective December 28, 2012, Michigan's social media password protection law, the "Internet Privacy Protection Act" (the "IPPA") regulates an employer's access to a current or prospective employee's "personal internet account," which includes not only social media accounts but email and cloud accounts as well.

The Michigan law applies to public and private educational institutions as well as public- and private-sector employers, and is the most protective of students (from nursery school onward).[5] It prohibits an employer from requesting an employee or applicant to grant it access to, allow observation of or disclose information that allows access to or observation of the employee's or applicant's personal Internet account. "Access information" is defined as username, password, login information or other security information that protects access to a personal Internet account.

The Michigan law does not, however, prohibit an employer from asking an employee to help view content in another employee/applicant's personal account. This limitation allows employers to investigate Internet misconduct or compromising posts. Publicly obtained information is also not prohibited from being reviewed and the employer's own systems and equipment are excepted from the IPPA's purview. Finally, unlike any of the other laws, the IPPA expressly protects employers by stating that it does not create a duty for an employer to search or monitor activity on personal accounts.

[5] Arkansas, California, Delaware, New Jersey and Utah also passed legislation applicable to educational institutions. Laws in Arkansas, California, Michigan and Utah apply to both employers and educational institutions, while laws in Delaware and New Jersey only apply to educational institutions. In July 2012, Delaware became the first state to prohibit public and private institutions of higher education or institutions of postsecondary education from requiring disclosure of social media passwords or other related account information. The New Jersey legislation, signed by Gov. Christie in December 2012, "prohibits a public or private institution of higher education from requiring a student or applicant to provide or disclose any user name or password, or in any way provide access to, a personal account or service through an electronic communications device." It also prohibits the institution from inquiring as to whether or not the student or applicant has an account and from retaliating against a student or applicant by not allowing him or her to participate in activities as a result of refusal to provide or disclose his or her information. Similar legislation applicable to employers is pending before the legislature.

FEDERAL INITIATIVES

In addition to legislation at the state level, two federal laws seeking to protect employees' and applicants' privacy rights have been introduced.

The "Social Networking Online Protection Act" ("SNOPA") seeks to prohibit employers from requiring or requesting an employee or applicant to provide a password or other means for accessing a private email account or personal account on a social networking site, while the "Password Protection Act of 2013"[6] would prohibit employers from compelling or coercing any person to provide a password or similar information to access a protected computer that is not owned by the employer. SNOPA was reintroduced to Congress on February 6, 2013, while the Password Protection Act of 2013 appears to have been referred to subcommittee.[7]

With respect to passwords and access to accounts, employers should:

- Review policies to ensure compliance if the employer operates its business in any of the states with password protection laws and pending legislation;
- Obviously, strictly prohibit personnel from asking for access to employee and applicant social media accounts, regardless of whether the employer operates in a state that has a law prohibiting employer access; and
- Train human resource personnel/managers/decision-makers to understand the restrictions with respect to hiring, investigating and disciplining (including shoulder surfing).

[6] The "Password Protection Act of 2012," originally introduced into the 112th Congress on May 9, 2012, was reintroduced in the 113th Congress as the "Password Protection Act of 2013."

[7] In addition to the arguments supporting state laws restricting access, proponents of these types of laws also note that they shield employers and schools from legal action because by preventing access to accounts, it becomes difficult to hold employers and schools liable for the digital posts of employees and students.

SECTION 3: SOCIAL MEDIA POLICIES & THE NLRB

For existing employees, the need to monitor social media activities has resulted in more and more employers enacting policies governing both the on- and off-duty use of social media accounts.

According to a 2012 survey of human resource professionals, 40% of employers reported having a formal social media policy, with 33% indicating they had taken disciplinary action against an employee for violating such policy within the prior 12 months.[8] In issuing a series of rulings and memos in the past year that proffer a broad view of employees' rights to engage in "protected and concerted activities" under Section 7 of the NLRA, the NLRB has taken an aggressive approach toward social media policies, invalidating as "overbroad" numerous policies of large, high-profile, private employers.[9] It continues to actively try to regulate social media use in the workplace, impacting the online activities of both union and non-union private employers, and has concerned itself with any restriction that might hinder discussions among employees relating to the terms and conditions of employment.[10]

The NLRB cited a number of corporate policies as being overbroad and unlawful under the NLRA for chilling the free speech rights of employees. Examples of prohibitions contained in these policies include provisions that discouraged comments about the employer, discussion of company matters, communication of confidential company information and disparagement of co-workers. In one policy, for example, the blanket confidentiality prohibition on releasing "confidential guest, team member or company information" was found to be unlawful because the NLRB found that it would reasonably be interpreted as prohibiting employees from discussing and disclosing information regarding their own and other employees' conditions of

[7] In addition to the arguments supporting state laws restricting access, proponents of these types of laws also note that they shield employers and schools from legal action because by preventing access to accounts, it becomes difficult to hold employers and schools liable for the digital posts of employees and students.

[8] Society for Human Resource Management Survey: Social Media in Business Strategy and Operations (January 2012).

employment, activities protected under Section 7 of the NLRA.[11]

In another case, the NLRB found unlawful the instruction that "[o]ffensive, demeaning, abusive or inappropriate remarks are as out of place online as they are offline," as such prohibition would include protected criticisms of the employer.[12] In addition, such policy's "savings clause," pursuant to which the employer stated that the policy would be administered in compliance with applicable laws and regulations, including the NLRA, was found not to have cured "the ambiguities in the policy's overbroad rules."[13] In another example, the NLRB concluded that a prohibition on employees posting information about the employer that could be deemed "material non-public information" or "confidential or proprietary" was unlawful as it was so vague that employees could reasonably construe it to include subjects involving their working conditions or terms and conditions of employment.[14]

With such seemingly acceptable prohibitions deemed as unlawful, guidance is required on crafting a lawful social media policy. In its May 30, 2012, memo, the acting general counsel of the NLRB offered the clearest glimpse to date of what constitutes an acceptable and lawful social media policy in approving Wal-Mart's policy, which was revised after consultation with the NLRB.[15] While Wal-Mart's policy had similar restrictions as policies previously deemed unlawful, it was Wal-Mart's use of specific examples of prohibited activity that provided context to employees and made clear that the policy was not intended to reach protected communications about working conditions.[16]

For example, Wal-Mart's policy prohibited "inappropriate postings that may include discriminatory remarks, harassment and threats of violence," "posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy," "posts that could be viewed as malicious, obscene, threatening or intimidating" and "offensive posts meant to intentionally harm someone's reputation."[17] By specifically providing examples of plainly egregious conduct, Wal-Mart's policy avoided being deemed overbroad. In addition, Wal-Mart's requirement to maintain confidentiality of its trade secrets and private and confidential information provided sufficient examples of prohibited disclosures, including "information regarding the development of systems, processes, products, know-how, technology, internal reports, procedures, or other internal business-related communications" such that employees could understand the prohibition was not intended to cover protected activity.[18]

[15] Id at 19–24.

[16] Id at 20.

[17] Id.

[18] Id.

BY SPECIFICALLY PROVIDING EXAMPLES OF PLAINLY EGREGIOUS CONDUCT, WAL-MART'S POLICY AVOIDED BEING DEEMED OVERBROAD.

In the constantly changing legal landscape and with limited clear guidance as to what constitutes a lawful social media policy, employers should proactively adopt best practices based on the NLRB rulings and memos to date.

Social Media Policy Best Practices:

- Updating nondisclosure agreements to prohibit disclosure of confidential information specifically in social media accounts (confidential information should be specifically and clearly defined and should not include terms and conditions of employment);
- Clearly articulating in the social media policy the business reasons for the policy and explaining employer's rights to monitor activity in social media;
- Providing specific examples of prohibited activities so employees understand that employer is not trying to reach protected and concerted activities;
- Reminding employees that social media use on company systems is not necessarily private;
- Developing a clear policy as to what off-duty social media conduct is prohibited and again, providing specific examples;
- Providing a strong, specific savings clause — while the NLRB made clear that a savings clause will not cure an otherwise overbroad policy, proper language can demonstrate that the employer's intent is not to reach protected and concerted activity (i.e. "Nothing in this policy is designed to interfere with, restrain or prevent employee communications regarding wages, hours or other terms and conditions of employment"); and
- Examining carefully the NLRB guidance, including the May 2012 memo. It is well worth reading, especially the approved Wal-Mart policy and reasoning behind it.

While guidance has been forthcoming, more remains to be seen where the lines will be drawn between overbroad and lawful policies, and privacy rights versus employers' legitimate business interests.

CONCLUSION: BE CAREFUL WHAT YOU LOOK FOR

While employers may have legitimate business interests in learning all they can about applicants and employees, these interests need to be balanced with individual privacy rights and with the employer's potential liability/exposure resulting from information learned from such access.

In the absence of access to social media accounts, public information is available, but employers are best advised to tread cautiously as information learned through social media can reveal more than employers really want to know — religion, marital status, family photos — information from which discrimination claims can spring. Too much information can be a dangerous thing and information cannot be "unseen" — so any punitive action taken could be viewed as discrimination or retaliation. And what if an employer learns of something, doesn't act and an individual is harmed? What is the employer's responsibility and what exposure exists? Employers need to carefully consider such issues before undertaking social media searches and monitoring activity.