Can Employers Demand to See Employees' and Applicants' Facebook Pages?

It has been reported that some employers are requiring job applicants to disclose their login information and passwords in order to access Facebook and other private information housed on social media. It has long been known that interviewers troll the Internet to obtain publicly-available information about a candidate as part of a background check. But now, as more people are making their social media profiles private, employers are requesting login information from prospective candidates in order to see their profiles. Some hiring managers are directing candidates to access their private accounts on the employer's computer and then "shoulder-surfing" the candidate's photographs, posts, and "tweets."

Motivations for Accessing Private Social Media Accounts

Why are some employers now resorting to reviewing social media sites or searching the Internet as part of their background check on applicants?

Most employers today are reluctant to provide meaningful references for fear of being sued for defamation. For example, California prohibits employers from intentionally interfering with former employees' attempts to find jobs by giving false or misleading references. While the law in most states permits an applicant to sue for defamation if the statements made by his or her former employer as part of a job reference are false and contributed to the candidate not receiving the position, the reality is that very few such lawsuits have been filed across the country. However, many employers resort to providing only 'name, rank and serial number' for former employees or simply say "no comment." Consequently, future employers have little meaningful data about an employee's performance or workplace demeanor to make an informed hiring decision.

Second, many employers are concerned about being held liable for failing to conduct a full and complete background check out of fear that one of their applicants – who had a history of misconduct that wasn't uncovered during the background check – repeats that conduct once again after being hired. These "negligent hiring" lawsuits, however, are still relatively rare. The theory behind these claims is based upon the notion that had the employer conducted a sufficient background check, it could have prevented later harm by never hiring the applicant in the first place.

The question of whether an employer could actually be held liable for failing to insist upon reviewing password-protected social media accounts is far from settled leaving many with legitimate concerns.

Finally, the sad reality is that resume fraud appears to be on the rise. Many employers have come to realize that applicants whom they have already hired have either fabricated work experience or education or greatly exaggerated/embellished credentials. Employers are seeking new ways to combat this trend.

The Legal Consequences of Requiring Access to Private Social Media Accounts

Numerous legal issues are triggered when employers require applicants to provide access to this information. Discrimination claims are one of the biggest concerns. For example, an employer might learn information about an applicant (such as their marital status, religion, sexual orientation or ethnicity) which might later allow that individual, if they are not hired, to contend said information is the reason why they weren't ultimately hired. Learning that a candidate either recently became pregnant or is planning to – whether held against that individual or not – can form the basis of a discrimination claim. Once the employer is on notice of a trait or characteristic learned from social media, they subject themselves to the very same claim that would be brought if identical information had been learned during an interview. The major difference – one that could be viewed very differently by a trier of fact – is that this information will have been obtained involuntarily by requiring Facebook credentials as opposed to perhaps voluntarily disclosed by the candidate.

Employers also subject themselves to claims that the applicant's right of privacy was invaded. Some states such as California afford a constitutional right of privacy that applies to private entities. Although it has not been tested in the Facebook context, a California applicant may have a viable claim that requiring the disclosure of a confidential password – which allows access to private, personal information – constitutes an invasion of privacy. Other states may allow such a claim to proceed based upon some type of common law invasion of privacy cause of action. Regardless of the type of claim, a court will first look at whether the applicant had a reasonable expectation of privacy. The only possible way to lower and perhaps eliminate that expectation, and potentially avoid such a claim, is to be explicit in places like job advertisements and applications that disclosure and access to private social media sites is a condition of being considered for hire.

In addition, some states have laws that prohibit employers from making adverse decisions based on off-duty lawful conduct. For instance, under New York law, employers cannot refuse to hire an individual based on his off-duty recreational activities, certain political activities, and the use of legal consumable products. While there does not appear to be a court decision directly on this point, it does not seem far-fetched that an applicant may pursue a claim under this or other similar statutes.

An employer's request for access to personal electronic accounts clearly violates one state law. On May 2, Maryland became the first state to outlaw such a practice with the "User Name and Password Privacy Protection Act." Effective in October of this year, that new law will prohibit an employer 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 communications device." It precludes an employer from discharging or otherwise penalizing any employee who refuses to provide this information with some exceptions.

Finally, there is legal authority for the proposition that coercing employees to divulge passwords violates an existing federal statute – the Stored Communications Act (SCA).

The SCA is violated when one intentionally accesses electronic information without authorization. The Ninth Circuit Court of Appeals recently found that an employee had a cognizable legal claim under the SCA when his employer accessed a secure website that contained criticisms of management using someone else's login information. *Pietrylo v. Hillstone Restaurant Group d/b/a Houston's,* 2009 U.S. Dist. LEXIS 88702 (D.N.J., September 25, 2009).

In March, Senators Charles Schumer and Richard Blumenthal asked the Department of Justice (DOJ) to investigate whether employers who ask for Facebook passwords are violating the SCA or the Computer Fraud and Abuse Act (CFAA). The CFAA makes it a crime for current or former employees to intentionally access a protected computer issued or owned by their employer "without authorization" or in a manner that "exceeds authorized access," resulting in damage and loss. The DOJ has not yet issued an opinion. Nonetheless, employers face a risk of violating the SCA or CFAA if they request confidential social media credentials and use that information to login into secure websites.

State And Federal Legislative Actions To Watch

In addition to Maryland, 12 other states, including California and New York, have moved to limit employers' rights to access social media. Illinois stands to be the second state to bar employers from seeking social media passwords. The Governor has signed the "Right to Privacy in the Workplace Act" and it goes into effect October 1, 2012.

Congress has also moved swiftly to respond to this practice. Recently, House Democrats introduced "The Password Protection Act of 2012" and Senator Blumenthal introduced a companion bill in the Senate with identical prohibitions. These bills would amend the Computer Fraud and Abuse Act and prohibit employers from:

- forcing prospective or current employees to provide access to their own private account as a condition of employment;
- discriminating or retaliating against a prospective or current employee because that employee refuses to provide access to a password-protected account; and
- engaging in an adverse employment action as a consequence of an employee's failure to provide access to his/her own private accounts.

The Password Protection Act of 2012, as currently written, preserves the rights of employers to:

- permit social networking within the office on a voluntary basis;
- set policies for employer-operated computer systems; and
- hold employees accountable for stealing data from their employers.

Both bills establish what may be viewed as a right of workplace privacy, prohibiting employers access to private employee data under any circumstances, even if the employer uses its own computers to access that data.

Another piece of proposed federal legislation in the House is the "Social Networking Online Protection Act" offered in April. This would prohibit employers and schools from requiring or requesting that employees and certain other individuals provide a user name, password, or other means for accessing a personal account on any social networking website.

Several states are moving forward with legislative measures. Delaware is considering "The Workplace Privacy Act." It would make it unlawful for employers to mandate that an employee or applicant disclose password or account information that would grant the access to their social networking profile or account. It would also prohibit employers from requesting that employees or applicants log onto their respective social networking profiles or accounts to provide the employer direct access.

California is considering a ban on requests for social media information. Assembly Bill 1844, introduced in February, would bar an employer from requiring an employee or applicant to disclose a username or account password to access a personal social media account that is exclusively used by the employee or prospective employee. California is also considering the "Social Media Privacy Act." In this proposed bill, public and private employers (as well as postsecondary educational institutions) are precluded from threatening an individual with or taking specified pecuniary actions (e.g., discharge, discipline, or otherwise penalize) for refusing to disclose permissibly requested information related to their personal social media account. Employers may request, but not require, an employee to provide access to a personal social media account to aid in an investigation concerning allegations of harassment, discrimination, intimidation or potential violence.

Practical Considerations and Conclusion

Employers have legitimate concerns as to whether they are obtaining the information they need to make a fully informed decision about candidates they are interested in hiring. At the same time, they need to be mindful that there are legal risks if they attempt to obtain information from password protected social media sites. Beyond this, employers need to seriously consider what these actions say about their corporate culture. Given the proliferation of social media usage in this country and in light of how important the new entrants into the workforce feel about their ability to communicate and express themselves this way, an employer may be hindering its ability to attract the best and brightest applicants by using these methods.

Employers need to decide if already existing procedures for conducting extensive, legal background checks are sufficient methods for obtaining needed information, or if more aggressive means need to be employed.

Stephen J. Hirschfeld is a founding partner at Curiale Hirschfeld Kraemer LLP and the CEO of the San Francisco-based Employment Law Alliance – a network of more than 3,000 labor and employment attorneys worldwide. Kristin L. Oliveira is Of Counsel at Curiale Hirschfeld Kraemer LLP. They can be reached at shirschfeld@chklawyers.com

and koliveira@chklawyers.com respectively, or via the firm's website: http://www.chklawyers.com.