Legal Insight

K&L GATES

www.klgates.com

August 7, 2012

Practice Group:

Labor and Employment

Employers "Surfing" into Unchartered Waters with Social Media Practices

By Christine Watts Johnston and Anne Reuben

The recent media frenzy and resulting flurry of legislative activity at both the federal and state level to ban employers from requesting or requiring access to employee or applicant social media highlight a new reality for employers: social media has blurred employees' private and professional lives, creating shaky legal ground for even the most cautious employer. The chances of an employer stumbling into unforeseen legal problems exist because the numerous areas of law touched by social media have failed to evolve at the same pace at which social media use has expanded. Even well-intentioned employers may not be considering the different ways accessing information about their current and prospective employees may expose them to liability. Highlighted below are several areas of potential risk that employers should consider as their social media practices and policies progress.

Privacy Laws

Following the media activity about employers accessing social media information from employees or prospective employees, Maryland and Illinois passed laws banning the practice, and several states have similar legislation pending.[1] Likewise, Senator Bluementhal from Connecticut introduced the Password Protection Act of 2012 (the "PPA") as broad federal legislation designed to proscribe an employer's access to any employee information held on any computer that isn't owned or controlled by the employer. The PPA, if passed, would extend beyond Facebook and other social media sites to prohibit employers from asking for passwords to social media or personal webmail accounts such as gmail, even if an employee is accessing those sites from a work computer. The bill does not, however, limit an employer's ability to set its own policies governing use of its electronic resources or set parameters around use of social media in the workplace.

Aside from these new laws directly addressing the issue of requesting on-line access to social media sites, existing laws such as the Stored Communications Act ("SCA") and/or the Computer Fraud and Abuse Act ("CFAA") also may be implicated by employers' social media practices. For example, the practice of requesting an employee or job applicant's social networking password may constitute "unauthorized access" under the SCA. The SCA prohibits intentional access to electronic information without the individual's authorization. The CFAA prohibits the intentional access to a computer, without authorization, to obtain information. "Without authorization" is critical in this context. Whether accessing social media activity constitutes a violation of these statutes will likely depend, at least in part, on the individual's willingness to surrender personal information. Although these laws have not been tested in the context of requesting information from "applicants," courts have found that when a supervisor requests a current employee's log-in information, and accesses otherwise private information with those credentials, that supervisor may be subject to civil and/or criminal liability under the SCA.[2]

Employers should also consider the privacy expectation employees have in their out-of-work activities. Some states, such as California, prohibit employers from taking employment action against employees on the basis of lawful conduct outside of work. Other states protect against unreasonable intrusions into an employee's private life. Accordingly, even if an employer isn't otherwise

prohibited based on computer-specific laws, long-standing general privacy protections may implicate what an employer can and cannot consider in making decisions about an employee or prospective employee's job or conditions of employment based on information gleaned through social media.

Anti-Discrimination Laws

Pre-screening job applicants through social media, as well as the continued monitoring of employee social media sites, also increases risks for employers under federal anti-discrimination laws, such as Title VII, the Americans with Disabilities Act ("ADA"), and the Age Discrimination in Employment Act ("ADEA"). Through social media, employers are likely to gain access to private, protected information that may be impermissible to factor into employment decisions, including, for example, information related to religious views, marital status, disability, or age. Even if inadvertently seen by an employer, the employer may then have to defend itself and its employment decisions and establish that the information related to an individual's protected status did not factor into the employer's decision to take an adverse action. Thus, simply knowing that an individual is a member of a protected category increases an employer's exposure to potential discrimination claims.

Even if an employer is not making individual employment decisions on the basis of social media, an employer who uses such tools could face claims of disparate impact discrimination. For example, employees or prospective employees of certain ages, race or gender may be more or less likely to use certain social media outlets.

National Labor Relation Act

Similar to the concern about an employer's accessing information relating to an employee's status as a member of a protected category, an employer could learn about an employee or prospective employee's ties to organized labor through social media searches or monitoring. An employer's knowledge of an applicant's or employee's current or prior union activity could heighten the risk that the employer faces an unfair labor practice charge under the National Labor Relations Act ("NLRA"). With the National Labor Relations Board's ("NLRB") recent focus on social networking, there is a high likelihood that they would tackle this issue if presented with the opportunity.

The NLRB's primary attention has been on the legality of employers' social media policies, in both unionized and non-unionized workplaces, due to the potential that such policies unlawfully chill the exercise of an employee's right to discuss the terms and conditions of employment under Section 7 of the NLRA. On May 30, 2012, the NLRB Acting General Counsel released his third memoranda describing the NLRB's approach to social media policies and specifically approved of one employer's social media policy. The memoranda reiterated the NLRA position that where the terms of a social media policy are overbroad or ambiguous, the NLRB will likely find the policy, or at least the offending section of the policy, to be in violation of the NLRA. While the NLRB did acknowledge employers' rights to protect trade secrets and confidential information, it has viewed many employer standard form policies as overbroad. Additionally, the NLRB has stated that the inclusion of a "savings clause," assuring that the policy will be administered in compliance with applicable laws and regulations (including Section 7 of the NLRA), does not cure ambiguities in an overbroad policy's rules.

The NLRB has pursued several notable unfair labor charges against employers—both unionized and non-unionized—who have terminated or disciplined employees based on social media postings about working conditions. Such cases highlight the fact that employers who may be otherwise enforcing

employment policies may be running afoul of NLRB rules to the extent that the employee's posting or social media activities are viewed as "concerted activity."

Fair Credit Reporting Act

Employers' use of third-party materials including social networking sites for pre-employment background screening may implicate the Fair Credit Reporting Act ("FCRA"), which places certain disclosure and authorization requirements on employers. The Federal Trade Commission's Division of Privacy has concluded that FCRA rules apply in the social networking context. Thus, when using a third-party information gathering service, employers must ensure FCRA compliance, particularly prior to taking adverse action on the basis of a "consumer report," as broadly defined by the FCRA.

Terms of Use of Social Media Sites

A social media site's Terms of Use may also inhibit an employer's ability to use social media information in its employment decisions. For example, Facebook's Statement of Rights and Responsibilities provides that "You will not…take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law."[3] Moreover, Facebook's Chief Privacy Officer issued a statement following the uproar over employers accessing employee or applicant social media sites that "Facebook takes your privacy seriously . . . [w]e'll take action to protect the privacy and security of our users, whether by engaging policymakers or, where appropriate, by initiating legal action."[4] This threatened action arises out of the company's terms of service agreement prohibiting users from sharing of passwords, accessing accounts belonging to other members, or doing anything else that might jeopardize the security of their accounts. Likewise, some websites explicitly prohibit the use of information found through their services for employment screening.

Conclusion

While some employers may be celebrating the availability of vast new resources to gather knowledge about employees and prospective employees at seemingly low cost, the potential pitfalls are significant. As employers continue to grapple with the issue, there may be times when monitoring employees' social media accounts is not unlawful, such as to deter and investigate harassment in the workplace, discourage the posting or disclosure of the employer's trade secrets or confidential information, or to properly conduct internal background checks.

However, due to the lack of any sweeping legislation or decisive case law in the areas discussed above, the viability of legal challenges brought by aggrieved employees will continue to be unpredictable until the legislature or courts decide the legality of certain practices. Employers may also face bad publicity or employee morale concerns if their social media practices are viewed as too invasive.

Employers who do opt to screen or monitor employees through social media should consider several practical steps to limit their exposure to claims.

- Develop and consistently apply a policy for how the company will use social media resources in pre-screening, hiring and employee monitoring.
- Train employees who will have access to and responsibility for use of social media for employment related decisions.
- Counsel other decision-makers to follow the company policy to avoid inadvertent exposure to claims based on decision-makers accessing protected information or violating privacy laws.

- Provide applicants and employees with advance notice and ensure that you have obtained valid consent to any use of social media resources.
- Comply with Terms of Use of relevant websites and avoid improper search tactics.
- Update company policies governing social media to attempt to avoid claims of interference with employee rights to engage in concerted activities.

For more information, or to update your employment policies, practices or forms, please contact the authors or your K&L Gates employment lawyer.

Authors:

Christine Watts Johnston
christine.johnston@klgates.com
+1.617.261.3138

Anne Reuben
anne.reuben@klgates.com
+1.704.331.7525

---

[1] States with pending legislation include: California, Massachusetts, Michigan, Minnesota, Mississippi, New York, South Carolina and Washington.
[2] *See Peitrylo v. Hillstone Restaurant Group,* 2009 WL 3128420 (D.N.J. 2009); *see also Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).
[3] http://www.facebook.com/legal/terms
[4] https://www.facebook.com/notes/facebook-and-privacy/protecting-your-passwords-and-your-privacy/326598317390057