New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
An ALM Publication
Labor&Employment:
Social Media in Focus
SOLOMON LAW FIRM PLLC
MONDAY, MARCH 9, 2015

The EEOC Hears Concerns About Social Media and Hiring

BIGSTOCK

BY KATHRYN BARCROFT AND BARRIE DNISTRIAN

Less than a decade ago, employers large and small would typically evaluate and hire potential employees on the basis of some fairly standard assessment tools: job applications and/or resumes; in-person interviews; personal and professional references; and transcripts or test scores.

Kathryn Barcroft is special counsel at Cohen & Gresser. Barrie Dnistrian is counsel at The Weinstein Law Firm.

Depending on the sensitive nature of the job opportunity, an employer might have dug deeper into an applicant's background; a criminal background and/or credit check could aid the employers in deciding whether the new employee at the till, supervising small children or inputting confidential medical data, was indeed trustworthy.

Today, however, employers have an additional source of information at their disposal thanks to the advent and prolific use of social media by prospective employees.[1] Popular social media sites such as Facebook, Twitter, Instagram, and LinkedIn, among others, can provide an employer with a unique and very clear peephole into the personal life of an applicant that might otherwise appear perfect "on paper." Because a qualified job candidate may not have considered his future job prospects when he posted lewd Mardi Gras photos back in 2009, or took to Twitter to rail against President Obama in 2012, a quick check of social media by a recruitment manager could sink an otherwise certain offer of employment.

While social media sites are useful tools for an employer seeking to screen job applicants on the basis of "organizational fit" or professional connections, for instance, the wealth of additional information available on those very same sites may turn the tool into a double-edged (and discriminatory) sword. For example, an applicant's social media profile may not only reveal his philanthropic nature and stellar communication skills, but also his membership in a "protected class." Even a cursory review of an applicant's biographical information on Facebook or vacation photos on Instagram can readily disclose the applicant's race, gender, national origin, color, religion, age, disability, or marital status. Because federal, state and local anti-discrimination statutes prohibit covered employers from making employment decisions on the basis of an applicant's protected class status (including those made in connection with recruitment and hiring),[2] an employer's use of social media as a screening tool may trigger claims of disparate treatment and/or disparate impact by rejected candidates.[3]

For this reason, among others, the U.S. Equal Employment Opportunity Commission (EEOC or Commission) convened a meeting on March 12, 2014 to gather information regarding the use of social media and its impact on the federal laws enforced by the Commission. In a release dated March 12, 2014, the Commission acknowledged that the "use of social media has become pervasive in today's workplace" and that the meeting "helped the EEOC understand how social media is being used in the employment context and what impact it may have on the laws we enforce and on our mission to stop and remedy discriminatory practices in the workplace."[4]

According to a survey published by the Society for Human Resource Management (SHRM) in 2013, 77 percent of the companies surveyed reported using social networking sites to recruit job candidates—a figure that more than doubled since 2008. While significant in number, only 20 percent of the companies surveyed by SHRM also use social media to screen (or background check) job applicants. The substantial dichotomy in these figures is likely attributable to the potential legal risks perceived by employers who use social media; in fact, 74 percent of the surveyed organizations admitted that they avoid screening applicants in this manner for fear of "discovering information about protected characteristics ... when perusing candidates' social profiles."[5]

Employers should be cautious in their use of social media for screening purposes in light of the testimony given during the March 12th meeting, and the fact that technology changes faster than the law. To this point, EEOC's acting associate legal counsel, cited an EEOC letter dated May 15, 2012, which acknowledged that although "the EEO laws do not address the legality per se" of employers requesting passwords and accessing applicants' social networks, the EEOC's position is clear: "covered employees must not use personal information from social networks to make employment decisions on a prohibited basis, be it race, color, religion, national origin, sex, age, disability, or protected genetic information." For example, "rejecting an applicant because he is Muslim, as disclosed through social media postings, would violate Title VII of the Civil Rights Act of 1964 ... Similarly, rejecting an individual with a family history of breast cancer, as shown in the caption to a photo of her completing the "Race for the Cure" in memory of her sister ... would violate the Genetic Information Nondiscrimination Act."[6]

Employers should be cautious in their use of social media for screening purposes in light of the testimony given during the March 12th meeting, and the fact that **technology changes faster than the law.**

Because employers are using social media to supplement traditional hiring practices and thus, must comply with a hodgepodge of old and new laws at the federal and state level, testimony was provided to the EEOC regarding the most practical ways for employers to avoid the legal pitfalls of screening applicants via social media.[7] As the EEOC highlighted in its release, these compliance tips include, among others: the selection of a third-party or designated person within the company who lacks hiring authority to conduct the social media background checks on applicants; the use of publicly available information only; and avoiding requests for passwords or usernames from job applicants.

In connection with requests by employers that job applicants provide their social media usernames and passwords, the EEOC release noted that at least four states already prohibit such requests and that similar legislation is pending at the state and federal levels. Importantly, this numbers was much higher by the end of 2014. According to a report issued by SHRM in August 2014, at least 18 states had either passed or enacted laws barring requests for access to employees and job applicants' social media accounts, and at least 28 states had similar legislation either introduced or pending.[8] In New York, Assembly bill No. A04388, which would prohibit employers from requesting or requiring username and login information as a condition of hiring, is currently before the State Assembly Labor Committee.[9]

Federal password protection legislation has not fared as well. In 2013, the Password Protection Act was introduced in Congress, but failed to make it out of committee.[10] Similarly, the Social Networking Online Protection Act (or SNOPA) was introduced in the House of Representatives in 2012 and 2013, but also stalled once referred to committee.[11] Nevertheless, other federal statutes address similar privacy concerns and employers should be aware of them before peering into an applicant's non-public social media account. For instance, if employers choose to designate a company employee or a third-party entity to review the social media profiles of job candidates, as was suggested to the EEOC, the Stored Communications Act of 1986 (SCA)[12] and the Fair Credit Reporting Act (FRCA)[13] are likely implicated. The SCA prohibits intentional access of electronic communications services (including social media sites) without authorization and thus, prohibits employers from accessing an applicant's private social media.[14] In addition, the FCRA requires any employer that conducts a background check (or through a consumer reporting agency to first provide notice to the applicant that a background check will take place, obtain consent from the applicant to conduct a background check, provide notice to the applicant that information having a negative impact on the applicant's eligibility for employment has been found, and allow the applicant time to correct any incorrect information found in the consumer report.[15] Because employee background checks can include information obtained from a host of sources, including social media, these same rules apply.[16]

The EEOC release reiterated the point raised by several panelists during the March 12th meeting—namely, that the use of social media in the hiring process can "provide a valuable tool for identifying good candidates by searching for specific qualifications." However, in using social media to screen candidates, employers must remain mindful of applicable state, federal

and local laws and that "the improper use of information obtained from such sites may be discriminatory" since protected class status "can be discerned from information on these sites."

Case Law Overview

Case law addressing claims of discrimination due to improper use of social media during the hiring process has been slow to emerge, ostensibly due to the "newness" of the medium's use in the employment context. However, as exemplified below, the claims that have been brought in several federal courts and before the EEOC tend to focus on the employer's discriminatory use of social media in choosing between job applicants.

In *Gaskell v. Univ. of Kentucky*,[17] a district court in Kentucky analyzed a claim of discriminatory hiring by a university that had gathered and used information from social media Internet searches during its vetting of candidates for a newly created position. Based on the facts presented, the court determined that the plaintiff presented sufficient evidence of a Title VII violation based on the defendant's refusal to hire and denied the defendant's motion for summary judgment.[18] As the court noted, there was no dispute that the plaintiff, Gaskell, was a leading candidate for the position, or that during the hiring process, one of the university's hiring committee members conducted a search of social media. The search led to a link on Gaskell's website that contained an article referencing certain conservative religious beliefs. Because Title VII protects against unlawful employment practices, including discrimination against an individual "with respect to compensation, terms, conditions, or privileges of employment, because of such individual's ... religion,"[19] the court found that sufficient evidence existed to create a triable issue of fact as to whether the search committee evaluated candidates for employment on the basis of illegal criteria and whether plaintiff's "religious beliefs were a substantial motivating factor in [the university's] decision not to hire him."

In *Nieman v. Grange Mutual Ins.*,[20] a federal district court in Illinois analyzed a job applicant's claim that a prospective employer discriminated against him in violation of the ADEA on the basis of a social media search conducted during the hiring process that revealed his age.[21] Specifically, the pro se plaintiff claimed that the company rejected his application for employment because the human resources department had actual knowledge of his age based on his LinkedIn profile, which included his college graduation date. The court ultimately determined that the plaintiff presented sufficient evidence of age discrimination to survive a motion to dismiss. The take away from this case, in keeping with the testimony provided to the EEOC, is that an employer's use of social media to disqualify a candidate on a protected class basis could serve as evidence against an employer charged with employment discrimination.

In *Reese v. Salazar, Sec'y, Dep't of Interior*,[22] the EEOC addressed the issue of social media and discrimination in employee recruitment. The plaintiff, alleging violations of the ADEA and Title VII by a government agency, claimed that she was not selected for a Park Ranger position due to her age (61) and sex (female), and that, generally, the agency's use of social media for recruitment had a disparate impact on older workers because they used computers less frequently than younger people. The Administrative Judge analyzed the disparate treatment claim and found that while the complainant alleged a prima facie case of age and sex discrimination, the agency articulated a legitimate, nondiscriminatory reason for its action. The Administrative Judge also found that the plaintiff failed to present evidence that social media was the exclusive means for recruitment by the agency and that no prima facie case of disparate impact existed because "an analysis of the data showed that there was no significant disparity based on the number of applicants in each age bracket." These determinations were upheld on appeal.

In Brief

Like any new technology, the law needs time to play catch-up with its impact on individual rights. As these cases demonstrate, and as the EEOC reiterated in its press release, "the EEO laws do not expressly permit or prohibit use of specified technologies ... . The key question ... is how the selection tools are used."

1. An estimated 1.35 billion users access Facebook on a monthly basis. As of December 2014, Instagram and Twitter boast 300 million and 284 million monthly users, respectively. John Constine, "Instagram Hits 300 Million Monthly Users to Surpass Twitter, Keeps It Real With Verified Badges," TechCrunch, Dec. 10, 2014, http://techcrunch.com/2014/12/10/not-a-fad/.

2. Federal laws that prohibit discriminatory practices in the recruitment and hiring of employees include Title VII of the Civil Rights Act of 1964 (Title VII), the Americans with Disabilities Act (ADA), the Genetic Information Nondiscrimination Act of 2008, and the Age Discrimination in Employment Act of 1967 (ADEA). Additional federal laws not enforced by the EEOC also proscribe discriminatory practices in the hiring and employment context. See EEOC, "Federal Laws Prohibiting Job Discrimination, Questions and Answers," http://www.eeoc.gov/facts/qanda.html. Many states and municipalities, including New York and New York City, have similar anti-discrimination laws. See, e.g., New York State Human Rights Law, N.Y. Exec. Law §296; New York City Human Rights Law, N.Y. Admin. Code §8-107(1).

3. For example, an employer's use of an applicant's membership in a protected class as a basis to disqualify him or her from employment may give rise to a disparate treatment claim. An employer's use of targeted advertising on a social media site to recruit job candidates from a specific group (such as men only or individuals under the age of 40) may give rise to claims of disparate impact.

4. See EEOC, Press Release, "Social Media is Part of Today's Workplace but its Use May Raise Employment Discrimination Concerns," March 12, 2014, http://www.eeoc.gov/eeoc/newsroom/release/3-12-14.cfm.

5. See Written Testimony of Jonathan Segal, Partner, Duane Morris; Managing Principal, Duane Morris Institute testifying on behalf of the Society of Human Resource Management, at pp.2-3, http://www.eeoc.gov/eeoc/meetings/3-12-14/segal.cfm.

6. See Written Testimony of Carol R. Miaskoff, Acting Associate Legal Counsel, EEOC, at p.3, http://www1.eeoc.gov//eeoc/meetings/1-14-15/miaskoff.cfm?renderforprint=1. The May 15, 2012 letter referred to by Ms. Miaskoff was an EEOC response to an inquiry by Sens. Charles E. Schumer and Richard Blumenthal regarding the legality of employers requiring job applicants to provide their social media usernames and passwords as part of the hiring process. Id.

7. See Written Testimony of Renee Jackson, Associate, Nixon Peabody, at p.3, http://www.eeoc.gov/eeoc/meetings/3-12-14/jackson.cfm.

8. Aliah D. Wright, "More States Ban Social Media Snooping," Society of Human Resource Management, Aug. 12, 2014, http://www.shrm.org/hrdisciplines/technology/articles/pages/social-media-snooping.aspx.

9. New York Assembly, 2015-2016 reg. sess. A04388.

10. Password Protection Act of 2013, H.R. 2077, 113th Cong.; Password Protection Act of 2013, S. 1426, 113th Cong.

11. Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012); Social Networking Online Protection Act, H.R. 537, 113th Cong. §2(a) (2013).

12. 18 U.S.C. §2701 et seq. (1986).

13. 15 U.S.C. §1681 et seq. (1970).

14. See *Pietrylo v. Hillstone Restaurant Group*, Civ. Case No. 06-5754, 2009 WL 3128420 (D.N.J. Sept. 25, 2009) (employer violated SCA by knowingly accessing a password-protected chat-group on social networking website without authorization); see also *Ehling v. Monmouth-Ocean Hosp. Service*, 872 F. Supp. 2d 369 (D.N.J. 2012) (finding SCA will apply to Facebook postings marked "private" because they are (1) electronic communications, (2) transmitted via an electronic communication service, and (3) are in electronic storage).

15. Federal Trade Commission, "Using Consumer Reports: What Employers Need to Know," January 2012.

16. Lesley Fair, "The Fair Credit Reporting Act & social media: What businesses should know," Federal Trade Commission, June 23, 2011, http://www.ftc.gov/news-events/blogs/business-blog/2011/06/fair-credit-reporting-act-social-media-what-businesses. see also, e.g., Maneesha Mithal, FTC, Social Intelligence Corp., Letter to Renee Peabody, May 9, 2011, http://www.ftc.gov/sites/default/files/documents/closing_letters/social-intelligence-corporation/110509socialintelligence letter.pdf ("Consumer reporting agencies must comply with several different FCRA provisions, and these compliance obligations apply equally in the social networking context.").

17. *Gaskell v. Univ. of Kentucky*, Civ. A. No. 09-244-KSF, 2010 WL 4867630 (E.D. Ky. Nov. 23, 2010).

18. 42 U.S.C. §2000e et seq., as amended.

19. 42 U.S.C. § 2000e-2(a)(1).

20. *Nieman v. Grange Mutual Ins.*, No. 11-3403, 2013 WL 1332198 (C.D. Ill. April 2, 2013).

21. 29 U.S.C. §621 et seq.

22. *Reese v. Salazar, Sec'y, Dep't of Interior*, Slip. Op. EEOC Agency No. NPS100602 (May 3, 2012) and Appeal No. 0120122339 (Nov. 15, 2012), available at http://www.eeoc.gov/decisions/0120122339.txt.