New Jersey Law Journal
STATEWIDE LEGAL AUTHORITY SINCE 1878
An ALM Publication
VOL. 224 NO. 12 MONDAY, MARCH 19, 2018 NJLJ.COM

EMPLOYMENT LAW

Social Media in the Hiring Process: Pitfalls and Protections

By Lisa Gingeleskie

PHOTO BY SHUTTERSTOCK.COM

Employers commonly utilize social media to gather information about prospective employees as part of the hiring process. Although social media can be very useful for this purpose, the law on what is permissible use by an employer is underdeveloped. While we wait for the law to catch up to technology, it is imperative that employers are advised as to the existence of certain legal pitfalls when using social media in the hiring process, as well as those practices they can implement to help avoid future liability.

Targeted Advertising

Federal, state and local anti-discrimination laws prohibit discrimination in hiring based on a prospective employee's protected class. Employers can unwittingly run afoul of these laws, however, when they use social media to recruit or research prospective employees. For example, more and more employers are using targeted advertising to recruit employees. This form of advertising allows employers to use social media platforms, like Facebook, to select a targeted audience based on a range of factors, including age, race and interest. Using the extensive data it collects from its members, social media sites are then able to specifically isolate the employer's advertisement so that it is shown only to those recipients that fall within the employer's chosen audience. While the ability of employers to deliver a message to a particular audience may seem advantageous for purposes of recruiting the most desirable candidate, choosing to use targeted social media advertising to post an open position with one's company may create an appearance of discrimination against non-targeted groups. This form of recruiting, commonly referred to as "microtargeting," has recently raised concerns over whether such conduct violates the federal Age Discrimination Employment Act

Gingeleskie is a member of the Labor, Employment & Employee Benefits group at Lindabury, McCormick, Estabrook & Cooper in Westfield. She concentrates her practice in the areas of labor and employment law as well as ERISA and employee benefits law.

(ADEA), which protects individuals who are 40 years of age or older from employment discrimination based on age. In New Jersey, this practice may also run afoul of the New Jersey Law Against Discrimination, which makes it unlawful for any person to aid and abet or incite, compel or coerce unlawful acts of discrimination.

This exact argument was raised by the Communications Workers of America (CWA) in a recent class action suit against T-Mobile U.S., Amazon.com and Cox Communications, all three of which had recruitment advertisements on Facebook that targeted users by age. The lawsuit claims that millions of older Americans were excluded from viewing these ads in violation of the ADEA. One of the dozens of ads at issue targets applicants interested in finance and features a millennial-aged woman working happily behind her computer. The recruiting campaign was scheduled to run through the Facebook feeds of users 25 to 36 years old who lived in Washington D.C., or had recently visited the area, and who had demonstrated an interest in finance. For those millions of other Facebook users who did not fall within this specific category, the ad did not exist.

Other advertisements at issue include images of employment recruitment ads that when clicked on by a user, bring up a screen requiring the user to confirm their age falls within the range of the group being targeted. For example, one such pop-up screen would read, "There may be other reasons you're seeing this ad, including that T-Mobile Careers wants to reach people ages 18 to 38." These types of ads are not uncommon. In fact, the database utilized by the CWA in bringing forth its class action suit demonstrates precisely how often employers recruit by age.

While the outcome of this suit is still pending, it is likely just the tip of the iceberg of what complainants are referring to as discriminatory redlining. One of the biggest problems employers face in protecting themselves against liability is simple awareness of the law and the level at which employers approach compliance with the ADEA. If employers are not aware of and advised against this form of microtargeting and the legal exposure that may follow, they are walking blindly into a field ripe with potential liability. In fact, after the CWA filed its class-action suit, many employers have taken steps necessary to change their recruiting strategies. These steps include eliminating the use of microtargeting altogether or, alternatively, using several different targeted advertisements as part of a more comprehensive recruiting plan that also includes traditional recruiting avenues such as job fairs. At the very least, practitioners need to advise their clients that use of targeted advertising contains legal risks and review the content of those targeted ads to ensure that they are composed and posted in a manner that does not give rise to discrimination claims.

Social Media Background Checks

Besides the use of recruitment ads, employers often utilize social media to review the profiles of job applicants. Again, while this practice can be helpful to employers in identifying the most desirable candidates for the position in question, it can also create the potential for hiring discrimination claims. Specifically, if a prospective employee can demonstrate that his or her candidacy was negatively affected by the results of a social media search containing information about his or her protected class status or lawful off-duty conduct, the employer is at risk of incurring legal and financial liability.

The leading case on this issue is *Gaskell v. Univ. of Kentucky*, 2010 U.S. Dist. LEXIS 124572 (E.D. Ky. Nov. 23, 2010). There, the plaintiff, Gaskell, applied for the position of director of the University of Kentucky's MacAdam Observatory and was not hired. Instead, the University hired a former student and employee within its Physics & Astronomy Department. Although the university conceded that Gaskell had more education and experience, it argued that the other candidate demonstrated more of the qualities that the university wanted in its observatory director. After further discovery, it was revealed that

during the search process, one of the committee members discovered Gaskell's personal website referencing certain religious topics, including articles that questioned the theory of evolution and contained Gaskell's own statements blending religious and scientific thought. This information was circulated to the search committee who, as members of a scientific community, expressed concerns over Gaskell's statements. In the end, the search committee recommended another candidate for the position. When reviewing the university's motion for summary judgment, the court concluded that there was a genuine issue of fact as to whether religion was a motivating factor in its decision to not hire Gaskell. As a result, *Gaskell* becomes a perfect example of how viewing a prospective employee's social media during the hiring process can reveal information about his or her protected status, like religious belief, and how use of that information can serve as the basis for legal action against an employer.

As a result of this holding, practitioners must be certain to advise their clients to redact any protected class information from their social media searches prior to making an employment decision. In order to avoid this risk altogether, many employers utilize third-party social media background check providers when conducting these types of searches. By using a third-party provider, employers eliminate the risk of inadvertently acquiring information about that applicant's protected status, as the third party deletes this information prior to sharing its search results with the employer, thereby insulating the employer from potential liability claims. It is important to remember, however, that social media background check companies are considered consumer reporting agencies under the Fair Credit Reporting Act (FCRA) because they assemble or evaluate consumer report information that is furnished to employers and used as a factor in determining employment. Accordingly, social media background check companies must comply with all FCRA regulations, including notifying the prospective employee that the employer may obtain a consumer report for employment purposes, and getting written consent from the prospective employee prior to obtaining any such report.

If an employer chooses to perform social media background checks in-house, social media screening should be performed by the Human Resources Department and protected information should not be shared with hiring managers. It is also best to create a list of social media sites that will be searched for each prospective employee and use the list to screen all prospective employees in a uniform manner.

Password Protected Information

Lastly, employers should be aware that several states have passed laws prohibiting employers from requesting password and username information or otherwise accessing the password-protected portions of a prospective employee's personal social media accounts. If employers are interested in searching social media for information about prospective employees, they should confine their search to information that is publicly available. Employers should not request usernames or passwords of applicants in order to gather additional information about that candidate. Employers should also avoid sending friend requests to an applicant, or even connecting with friends of a prospective employee, in order to avoid any potential claims that the employer was trying to gain access to otherwise private information.

As evidenced throughout this article, the issue facing employers today is not the collection of information itself, but how that information is being used. In a world where employee and applicants' background and personal information is merely a click away, employers need to be wary of the risks associated with the use of that information. As guidelines and case law continue to evolve, it is the responsibility of practitioners to not only educate employers of these risks, but also to recommend those steps necessary to protect against potential liability. ■