Lexis Practice Advisor® is a comprehensive practical guidance resource for attorneys. It includes "how to" practice notes, model forms, and on point cases, statutes, administrative materials, emerging issues articles, and treatise sections. The Labor & Employment offering contains access to a unique collection of expertly authored content, continuously updated to help you stay up to speed on leading practice trends. The following is a practice note from the Navigating Social Media subtopic under the Privacy, Technology, and Social Media topic.

Lexis Practice Advisor Labor & Employment

Obtaining Information Regarding Job Applicants and Employees from Social Media Websites

by Marcia Goodman, Mayer Brown LLP

Marcia E. Goodman is a partner in Mayer Brown's Litigation & Dispute Resolution practice and serves as co-leader of the firm's United States Employment and ERISA Litigation Action Group. Assistance provided by Richard Nowak (associate) of this same practice.

It should come as no surprise that social media contains a vast amount of information. For this reason, many employers use social media during the hiring process. In fact, some employers have even gone so far as to require prospective employees to disclose their social media passwords. Not only have such actions elicited much criticism, they also carry certain legal risks as more and more states enact laws banning the practice. In addition, employers should also know that using social media during the hiring process can implicate state and federal discrimination laws.

This practice note addresses how to navigate legal issues surrounding the use of social media to vet potential job candidates. Specifically, it addresses the following subjects:

- Requests for Social Media Passwords
- Social Media May Implicate Discrimination or Retaliation Laws
- Avoiding Social Media Hiring Discrimination Claims
- Stored Communications Act Issues
- Fair Credit Reporting Act (FCRA) Issues

Requests for Social Media Passwords

In 2012, Maryland became the first state to enact a social media privacy law prohibiting employers from requesting social media account information from current or prospective employees. As of June 2015, 21 states have enacted similar laws including: Arkansas, California, Colorado, Connecticut, Illinois, Louisiana, Maryland, Michigan, Nevada, New Hampshire, Montana, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Virginia, Washington, and Wisconsin. In addition, related legislation has been introduced, or is pending, in more than 20 other states.

Although each state's law has unique aspects, they all generally prohibit employers from requesting that current or prospective employees disclose their personal social media information. (New Mexico is the only exception as its law does not expressly prohibit employers from requesting social media information from their current employees. See N.M. Stat. Ann. § 50-4-34 (2014)). Therefore, you should advise employers that have operations in the states listed above to review their hiring practices to make sure that they comply with state law. In addition, given the reasonable likelihood that other states will adopt similar laws in the future and the possibility of federal legislation, you should advise your clients to stay apprised of any legal developments in this area.

Social Media May Implicate Discrimination or Retaliation Laws

In addition to the growing prohibition against requests for a prospective employee's social media passwords, employers should also know of the risks associated with basing hiring and other employment decisions on public information gathered from social media sites.

Existing federal laws – including Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, the Age Discrimination in Employment Act, and the Genetic Information Nondiscrimination Act – prohibit employers from basing employment decisions on factors such as age, race, national origin, religion, marital status, and genetic information. In addition, many state laws protect other characteristics (e.g., sexuality), provide statutory or common law privacy protection, or protect legal off-duty activities. Many individuals indiscriminately post personal information on social media, including information relating to a protected class. Accordingly, you should advise employers that, by viewing such information to make employment decisions, they potentially expose themselves to claims of unlawful discrimination or retaliation.

Although only a limited number of cases discuss employment discrimination in the social media context, it appears that courts will be receptive to such claims. For example, in Neiman v. Grange Mutual Insurance Co., 2012 U.S. Dist. LEXIS 59180 (C.D. Ill. Apr. 26, 2012), a district court denied an employer's motion to dismiss the plaintiff's age discrimination claim. Although the employer argued that it did not know the plaintiff's age when it decided not to hire him (the interview occurred by telephone), the court concluded that it sufficed at the pleadings stage for the plaintiff to allege that the defendant knew his age based on a statement in his LinkedIn profile which said he graduated from college in 1989. In finding that allegation sufficient to place the company on notice that the plaintiff belonged to a protected class, the court stressed that "[i]t is not difficult to determine that someone who graduated from college in 1989 probably was over the age of 40 in 2010." As a result, the company was forced to expend substantial resources and spend significant time litigating an age discrimination claim that the court ultimately dismissed on summary judgment. See Nieman v. Grange Mut. Ins. Co., 2013 U.S. Dist. LEXIS 47685 (C.D. Ill. Apr. 2, 2013).

Avoiding Social Media Hiring Discrimination Claims

As the *Neiman* decision suggests, courts may hesitate to dismiss discrimination or retaliation claims if any reason exists to believe that an employer knew of protected class information based on its review of a plaintiff's social media account.

You should therefore advise employers to take steps to prevent such information from reaching the actual decision-maker. For example, employers should consider, among other things, establishing internal procedures for viewing social media and other websites in connection with employment decisions, having a non-affiliated or independent person review social media and only forward relevant information to those with a need to know such information, and taking steps to ensure employees' or prospective employees' social media accounts are not improperly accessed.

Stored Communications Act Issues

You should also advise employers that the unauthorized gathering of information from social media sites during the hiring process may implicate the Stored Communications Act (SCA). The SCA affords privacy protections to certain "private" communications that are transmitted and stored electronically. Although the SCA predates the invention of both the Internet and social media, courts have applied its protections to cases involving social media.

For example, in Ehling v. Monmouth-Ocean Hospital Service Corp., 961 F. Supp. 2d 659 (D.N.J. 2013), a district court held that certain Facebook postings received privacy protection under the SCA because the employee used Facebook's privacy settings to limit who could see her postings. Accordingly, because only the employee's Facebook friends could view her postings, the court concluded that the SCA applied. The court ultimately granted summary judgment to the employer because it had authorization to receive the employee's Facebook postings. Had the employer accessed the posts without authorization or forced the employee to provide her Facebook password, however, the court would have likely found an SCA violation. Therefore, employers who ask their employees or potential employees for social media passwords or demand access to their social media profiles may—in addition to potentially violating the state social media privacy laws discussed above—violate the SCA.

For more information on the SCA, see Navigating the Stored Communications Act.

Fair Credit Reporting Act (FCRA) Issues

Finally, you should counsel employers that using social media to vet prospective employees or to perform background checks may also implicate the Fair Credit Reporting Act (FCRA).

Although the FCRA will not likely cover an employer's own evaluation of social media during the hiring process, using third party organizations to perform background checks can trigger obligations under the FCRA. Similar to traditional background and credit checks, employers may find it more efficient to outsource social media searches to a third party rather than perform them in house. Among other advantages to outsourcing these types of searches, the third party can redact certain information protected by state and federal law before it reaches the employer. Such redaction limits the risk of the employer considering protected information during the hiring process.

Employers should keep in mind, however, that third party background check providers that search social media sites may be considered consumer reporting agencies under the FCRA. Consequently, employers who rely on social media searches provided by such entities must comply with the FCRA's notice requirements, which may include notifying prospective employees about the background check and obtaining written consent.

For example, in a May 2011 Staff Closing Letter to Social Intelligence Corporation, available at http://www.ftc.gov/enforcement/cases-proceedings/closing-letters/social-intelligence-corporation, the Federal Trade Commission (FTC) concluded that Social Intelligence Corporation, an Internet and social media background screening service company, constituted a consumer reporting agency. It reached this conclusion because Social Intelligence Corporation provided employers with consumer report information based on its review of social media sites and the employers relied on that information in evaluating consumers' eligibility for employment. Although the FTC did not find a FCRA violation, it emphasized that the FCRA's compliance obligations for consumer reporting agencies apply in the social networking context. Accordingly, you should advise employers that, if they outsource social media background checks to a third party, they also must satisfy their reporting obligations under the FCRA.

For more information on the FCRA, please see Understanding Consumer Reports (Including Credit History Checks) Under the Fair Credit Reporting Act and Step-by-Step Guidance for Complying with the FCRA and State Mini-FCRAs. Additionally, for information on state mini-FCRA requirements, please see the relevant practice note for the particular state in the Screening and Hiring topic.