Copyright & New Media Law

Making sense of complex legal issues

VOLUME 20, ISSUE 2 • SPRING 2016

Social Media Use By Applicants and Employees: The Conundrum

BY JASON C. GAVEJIAN, JD., CIPP

PRINCIPAL, JACKSON LEWIS

Despite its prevalence and immense popularity, social media continues to pose challenges for organizations as they struggle with a minefield of legal risks. Navigating the legal pitfalls related to social media usage by applicants and employees is often one of the most difficult tasks an organization faces.

If you are unfamiliar with the term "social media," I would like to welcome you to the year 2016. Social media is defined as "forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)"[1] and has grown over the past decade to become a part of our everyday lives.

As the definition makes clear, an innumerable amount of websites or mobile applications may be considered "social media." Five of the most prevalent social media sites are Facebook,[2] LinkedIn,[3] YouTube,[4] Twitter,[5] and Instagram.[6]

Organizations regularly utilize social media to locate and attract new business and to recruit top applicants for employment. Applicants and employees increasingly utilize social media to connect with friends and co-workers, and to network with contacts. Whether for business or personal use, individuals can access social media sites from a myriad of devices and at virtually any time. Regardless of when or how

1 *Merriam-Webster.com*.

2 As of March 31, 2016, Facebook had 1.65 billion monthly active users, with 1.5 billion of those accessing the site on their mobile devices. "Company Info," *Facebook Newsroom*.

3 Linkedin has over 433 million registered members with more than 40 million students and recent college graduates making up LinkedIn's fastest growing demographic and professionals signing up at a rate of more than two new users every second. "About Us," *LinkedIn Newsroom*.

4 YouTube has over 1 billion users—almost one-third of all people on the Internet—and every day, people watch hundreds of millions of hours on YouTube and generate billions of views reaching more eighteen to thirty-four and eighteen to forty-nine year-olds than any cable network in the U.S. "Statistics," *YouTube*.

5 Twitter has over 310 million monthly active users. "Company," *Twitter*.

6 Instagram has over 500 million monthly active users. "Press News," *Instagram*.

applicants and employees utilize social media, they are using it to communicate with contacts, to talk about their employers, to discuss their views or opinions, and to share content they find relevant.

Despite its prevalence and immense popularity, social media continues to pose challenges for organizations as they struggle with a minefield of legal risks. Navigating the legal pitfalls related to social media usage by applicants and employees is often one of the most difficult tasks an organization faces. As such, this article will provide an overview of two of the most common questions employers ask with respect to social media.

May we review an applicant's or employee's social media content?

Yes, but… organizations must exercise caution in how they access information about a job applicant or employee available through social media. Currently, twenty-three states have enacted laws that make it illegal for an employer to request and/or require employees or applicants to provide the usernames and passwords necessary to access their social media and other online accounts.[7] While the laws vary by jurisdiction, in the applicable states, your organization is likely prohibited from:

7 "State Social Media Privacy Laws," National Conference of State Legislatures (April 6, 2016).

- Requiring or coercing an employee or applicant to disclose the password to a personal social media account;
- Requiring or coercing an employee or applicant to access a personal social media account in the presence of the employer or its agent;
- Requiring or coercing an employee or applicant to disclose any personal social media account information;
- Requiring or causing an employee or applicant to add anyone to the list of contacts associated with a personal social media account;
- Requiring or causing an employee or applicant to alter or change his settings to allow a third party to view the content of a personal social media account;
- Discharging, disciplining, or otherwise penalizing (or threatening to do the same) an employee for refusing to disclose or provide access to a personal social media account as prohibited above; and
- Failing or refusing to hire an applicant for refusing to disclose or provide access to a personal social media account as prohibited above.

It is recommended that, regardless of jurisdiction, organizations avoid engaging in the actions outlined above.[8] This is especially true now as it is likely more states will enact similar legislation in the near future. In fact, the number of states prohibiting this type of activity has grown from zero to twenty-three in just four years, and, in 2016, similar legislation has been introduced or is pending in at least fourteen other states. [9]

Regardless of state statutory prohibitions, it is essential for organizations to avoid certain other activities that might violate federal or common law, such as circumventing an applicant's or employee's privacy settings by pretending to be someone else in order to gain access to a restricted site.[10] Similarly, using existing technologies that permit the tracking or logging of keystrokes to allow an employer to discern an employee's username and password to online accounts runs the risk of violating the Stored Communications Act ("SCA"), which generally prohibits accessing the online account of another without that individual's consent.[11] Less technologically savvy employers who simply pressure or otherwise obtain access to an individual's social media activity from an individual's co-workers who are friends or their online connections can also raise SCA issues, as well as potential violations of common law privacy torts (*e.g.*, intrusion upon seclusion). Notwithstanding these prohibitions, if a current employee or some other third-party voluntarily, and without coercion, provides your organization with an individual's social media content (not user name and password), such information may be reviewed as if it was publicly available.

In short, if an applicant's or employee's social media content is not publicly available, an organization should not take steps to gain access to that non-public content. By contrast, employers are permitted to review an applicant's or employee's public social media content.

May we utilize social media content in making employment decisions?

This is one of the most common questions I receive from clients. Nearly all employers are turning to social media sources for information about job applicants,[12] yet these sources are replete with information that should not be considered in the hiring process. Additionally, a myriad of scenarios that may prompt an employer to discipline an employee for his or her social media use should be avoided.

The most obvious situation is a current employee who engages in illegal web-based activity while at work. Another common scenario is an employee who spends the majority of her on-duty time using social media sites having nothing to do with her job responsibilities. Other situations may include employees who criticize a supervisor or client, post distasteful photos or videos, or call in sick and then tweet or post about being out and about. In the health care industry, employee social media activity can be particularly troubling, such as when employees post about patients' injuries (with photos) on social media.[13]

Generally speaking, assuming you have lawfully obtained the social media content, so long as you do not violate state or federal discrimination laws, nothing currently prohibits an employment decision based on information an applicant or employee makes publicly available. However, when using social media to review applicants or employees, an employer may inadvertently become aware of certain information or characteristics of an applicant or employee that can expose the employer to risk of a lawsuit if the employer makes a decision adverse to the individual based on that information or characteristic.

Various federal and state laws prohibit employers from basing an employment decision on an applicant's or employee's race, age, sexual orientation, marital status, disability, arrest history, conviction[14] or credit history, political affiliation, receipt of workers' compensation benefits, whistleblower activity, lawful off-duty conduct, and even genetic information.[15] By way of example:

8 Generally, these laws *do not* prohibit certain industries (*e.g.*, securities, finance) who have to comply with specific regulatory requirements from conducting investigations concerning the use of personal websites, web-based accounts, or similar accounts by an employee for business purposes. Employers in these types of highly regulated industries need to balance regulatory requirements with the privacy interests of their employees.

9 "Access to Social Media Usernames and Passwords," National Conference of State Legislatures (April 6, 2016).

10 *See, e.g.,* Pietrylo v. Hillstone Rest. Group, No. 06-5754, 2008 U.S. Dist. LEXIS 108834 (D.N.J. July 24, 2008) (holding employer liable after employer accessed Plaintiffs' private password-protected MySpace through a "greeter's" password after the greeter's manager requested access).

11 *See, e.g.,* Rene v. G.F. Fishers, Inc., 817 F. Supp. 2d 1090 (S.D. Ind. 2011).

12 Matt Singer, "Welcome to the 2015 Recruiter Nation, Formerly Known as the Social Recruiting Survey," *Jobvite* (Sept. 22, 2015).

13 *See, e.g.,* Molly Hennessy-Fiske, "When Facebook goes to the hospital, patients may suffer," *LA Times* (Aug. 8, 2010); "HIPAA Case Study: Temporary Employee Post Patient Records on Facebook, Hospital Faces Stiff Penalties," *Dexcomm* (June 19, 2012); "Hospital workers axed for Jason Pierre-Paul breach," *Daily News* (Feb. 5, 2016).

14 The EEOC recently set new parameters on the use of criminal records in hiring and retention decisions. *See EEOC Enforcement Guidance Number 915.002* (April 25, 2012). *See also* "Ban the Box," Jackson Lewis.

15 Employers should be aware of the Equal Employment Opportunity Commission's focus on eliminating systemic discrimination, such as discriminatory barriers in recruitment and hiring.

- **Genetic Information:** The general rule under the federal Genetic Information Nondiscrimination Act[16] ("GINA") is that genetic information cannot be collected by an employer or used for an employment purpose, unless an exception applies. Thus, purposefully searching for more information on social media about the health of an applicant's or employee's spouse or family member (perhaps because of concerns of significant cost to the company's medical plan or increased need for the employee to take leaves of absence) is prohibited under GINA.
- **Discrimination:** A manager or supervisor may learn information from an applicant's or employee's social media status that they would not otherwise have, such as learning that the individual is a member of a protected class (*e.g.*, disabled, older, or pregnant). As mentioned above, these protected classes may not lawfully be considered in employment decisions.
- **Lawful Off-Duty Conduct:** An employer may find photos on an applicant's or employee's social media account showing the individual engaged in activities that appear to be illegal, such as smoking marijuana. But the individual could be legally using it for medicinal purposes or using it in a state or country where using marijuana is permissible. The material the individual is smoking may not even be marijuana or another illegal substance. Even where conduct clearly appears to be illegal, an employer may be prohibited from taking action based on such activities. For example, in California, employers are prohibited from excluding someone from employment based solely on an arrest, marijuana conviction more than two years old, or conviction that has been expunged or dismissed.[17]
- **Background Checks:** The federal Fair Credit Reporting Act[18] ("FCRA") requires employers to obtain consent before conducting background checks through consumer reporting agencies. If an employer decides not to hire an applicant based on information in a consumer report obtained from a social networking site through a third party, the employer may be required under the FCRA to notify the applicant that its decision was based on that information. At the state level, likely in response to recent economic conditions, new laws in certain jurisdictions prohibit employers from discriminating against employees and applicants on the basis of credit-related information, such as payment history.[19]
- **Whistleblowers:** Federal and state whistleblower laws may protect employees who utilize social media to complain about certain company activities, conditions affecting public health and safety, or violations of public policy standards, as well as employees who report potential securities fraud violations.[20]
- **Political Activities:** Especially pertinent in an election year (particularly one with such polarizing candidates as this year), many states prohibit employers from regulating employee political activities and affiliations, influencing employees' political activities, or taking action against an employee for political speech.[21]
- **National Labor Relations Board:** Employers (including non-union employers) need to be mindful of recent interpretations of the National Labor Relations Act[22] ("NLRA") concerning protected rights to engage in concerted activity as applied to social media policies and employee discipline based on social media activity. Not all concerted activities are protected by the NLRA; only those activities in which employees engage for the purpose of collective bargaining or other mutual aid or protection are covered.[23]

An employment decision based on the activities described above could make the employer vulnerable to a lawsuit by the individual involved alleging the decision was discriminatory or otherwise unlawful. The law is far from clear in these areas as they apply to social media, and employers should consider each situation independently.

While you are likely thinking that you would never rely on an individual's lawful activity or membership in a protected class to make an employment decision, the difficulty you may face once this information is accessed is proving that you did not rely on it. Proving the negative is often extremely difficult for employers.

Conclusion

Ultimately, hiring, disciplining, and firing are all critical parts of the employment relationship, and what constitutes appropriate social media use in one workplace may not in another. An organization relying on social media content or information to make any employment decision should be aware of the potential legal repercussions and consult with legal counsel to manage the risks inherent in any adverse employment decision. ■

Jackson Lewis
Morristown, New Jersey
www.workplaceprivacy.com
jason.gavejian@jacksonlewis.com
Twitter: @jaygavejian

16 122 Stat. 881 (2008) (modifying multiple sections of Titles 29 and 42 of the U.S. Code).
17 CAS. LAB. CODE §§ 432.7 & 432.8.
18 15 U.S.C. (§) 1681
19 Heather Morton, "Use of Credit Information In Employment," National Conference of State Legislatures (May 6, 2015).
20 *See, e.g.*, 18 U.S.C. § 1514A; 45 C.F.R. 164.502(j).
21 *See, e.g.*, CAL. LAB. CODE § 1102; COL. REV. STAT. ANN. § 8-2-108; LA. REV. STAT. ANN § 23:961; MINN. STAT. ANN. § 10A.36; MO. ANN. STAT. § 115.637(B); NEB. REV. STAT. ANN. § 32-1537; NEV. REV. STAT. ANN. § 613-040; S.C. CODE ANN. § 16-17-560; W.VA. CODE ANN. § 3-8-11; SEATTLE, WASH. MUN. CODE § 14.04.040.
22 29 U.S.C. (S)(S) 151-169
23 *See, e.g.*, Federal Security, Inc., and James R. Skrzypek and Janice M. Skrzypek and Joseph Palm, 359 NLRB No. 1 (Sept. 28, 2012). *See also* "Acting General Counsel releases report on social media cases," *National Labor Relations Board*, (Aug. 18, 2011); "Acting General Counsel releases report on employer social media policies," *National Labor Relations Board* (May 30, 2012)