



Sacred Heart
UNIVERSITY

Sacred Heart University
DigitalCommons@SHU

WCOB Faculty Publications

Jack Welch College of Business

9-2012

Invisible Discrimination: Employers, Social Media Sites and Passwords in the U.S.

Richard L. Pate

Sacred Heart University, pater@sacredheart.edu

Follow this and additional works at: http://digitalcommons.sacredheart.edu/wcob_fac

Recommended Citation

Pate, R.L. (2012). Invisible discrimination: Employers, social media sites and passwords in the U.S. *International Journal of Discrimination and the Law* 12(3), 133-146. doi: 10.1177/1358229112470300

This Article is brought to you for free and open access by the Jack Welch College of Business at DigitalCommons@SHU. It has been accepted for inclusion in WCOB Faculty Publications by an authorized administrator of DigitalCommons@SHU. For more information, please contact ferribyp@sacredheart.edu.

Invisible discrimination: Employers, social media sites and passwords in the U.S.

Richard L Pate

Abstract

With the advent and popularity of social networking sites, the boundaries of the relationship between the employer and employee/prospective employee have stretched well beyond the workplace and working hours. Predictably, this relationship expansion has led to uncharted adversarial scenarios between the respective parties. Unfortunately, in this new, vibrant cyber world, traditional employment law considerations are struggling for deference and rumination. Notwithstanding this ostensible indifference, each phase of the relationship is heavily impacted by social network media. Applicant recruitment, information gathering and applicant selection stand to be impacted by the social network communications made by employees or prospective employees. This article examines whether present and proposed law protects job applicants from potential, unlawful discrimination resulting from the employer's use of social media in its applicant recruitment, information-gathering and applicant selection processes.

AQ1

AQ2

Keywords

applicant, discrimination, employment law, Facebook, password, social media sites

Introduction

With the advent and popularity of social network sites, the boundaries of the relationship between the employer and employee/prospective employee have stretched well beyond

John F Welch College of Business, Sacred Heart University, Fairfield, CT, USA

Corresponding author:

Richard L Pate, John F Welch College of Business, Sacred Heart University, 5151 Park Avenue,
Fairfield, CT 06825-1000, USA

Email: pater@Sacredheart.edu

the workplace and working hours. Predictably, this relationship expansion has led to uncharted adversarial scenarios between the respective parties.

Ensuing legal disputes necessitate an expansion of the law's applicability to this new world, or new legislation for it. The respective parties, employers especially, require a level of predictability regarding their respective rights and duties. While this predictability can only be offered by a body of well settled law, unfortunately, in this new, vibrant cyber world, traditional employment law considerations are struggling for deference and rumination.

AQ 3

AQ 4

Notwithstanding this ostensible indifference, each phase of the relationship is heavily impacted by social network media. Applicant recruitment, information gathering and candidate selection stand to be impacted by the social network communications made by employees or prospective employees. While the number of Facebook users has reached 1 billion, no legislation exists specifically regulating the employer's access to and use of social network information for hiring and firing purposes.

This article examines whether present and proposed law protects employees' and prospective employees' rights from potential unlawful discrimination resulting from the employer's use of social media in its applicant recruitment, information-gathering and applicant selection processes.¹

The employer's interests²

Employers should look

The employer's desire to obtain and digest all possible information regarding a job applicant prior to selection is a logical business interest. A preliminary study finds a strong correlation between job performance and Facebook profiles (Kluemper et al., 2012). In a study published in the *Journal of Applied Social Psychology*, raters were asked to rate university students by personality related questions, such as '[I]s this person dependable?' after viewing the student's Facebook page only (ibid.). Raters were, in essence, asked to form impressions of an applicant based solely on viewing the publicly available material (photos, status updates and conversations) on the applicant's Facebook page.

The raters then assigned a grade to each applicant for the attributes of a good employee: emotional stability, conscientiousness, extroversion, intellectual curiosity and agreeableness. Such findings were subsequently (six months later) matched to the student's job performance evaluation completed by the students' respective employers. The study found a clear and strong relationship between 'good' Facebook scores and job performance. Generally, the raters gave positive grades to students who traveled and had many friends and a variety of interests or hobbies.

Such indications suggest that a reasonable employer should review job applicants' social media communications. In its recruiting and selection process, it is, of course, in the employer's interest to distinguish between a poor applicant and a good applicant.

Employers may need to look

Under some circumstances, a review of an applicant's profile page may be more than a logical business decision, but may also constitute a legal duty. Employer responsibility

for the actions of an employee can potentially be based on two different theories. First, under the doctrine of *respondeat superior*, when the employee commits a tort while in the course of his employment duties, the *employer* is rendered liable to the victim of the tort (Epstein, 2008: 432). While it is true that this type of vicarious liability, generally, does not create an affirmative duty to peruse an applicant's profile page prior to offering the position,³ a prudent employer would be better served to conduct such review in search of evidence for propensity toward tortious conduct (Mooney, 2010: 758).

Second, unlike vicarious liability, which is based on the indirect liability of the employer, direct liability may also be imposed on the employer for the eventual tortious acts of the employee.⁴ An employer may be directly liable based on the theory of negligent hiring. This doctrine stems from pure negligence concepts, that is, an employer must exercise reasonable care when hiring a person to perform specific duties.⁵ For example, an employer may be deemed to be acting unreasonably, i.e. negligently, when it employs a person, previously convicted of child abuse, to work in a position entailing direct contact with children, if harm to the children ensues. Most states' law holds employers liable for the tortious acts of the employee when the employees' tortious acts were reasonably foreseeable at the time of hiring (Larson, 2010: pt. 1, ch. 11). Negligent hiring is based on the fact that it was negligent for an employer to hire the employee given what the employer knew or should have known about the employee at the time of hiring. Using Connecticut as an example, '[t]he ultimate test of the existence of the duty to use care is found in the foreseeability that harm may result if it is not exercised.'⁶ 'It is well settled that defendants cannot be held liable for their alleged negligent hiring [...] of an employee accused of wrongful conduct unless they had notice of said employee's propensity for the type of behavior causing the plaintiff's harm.'⁷

AQ5

Since foreseeability is the basis of this tort, the inevitable question is whether employers *must* perform a perfunctory investigation of an applicant's profile page (especially given the relative ease of doing so) prior to employing the candidate. No case has explicitly found that a failure to review online information before hiring an employee who later commits a tort constitutes negligence hiring. Other than statutorily required background checks in connection with sensitive positions such as teachers and law enforcement personnel,⁸ current law is not clear on this point.⁹ Some courts have imputed to employers the obligation to investigate an applicant's background.¹⁰ In other jurisdictions the existence of the duty may depend on the nature of the position sought, the hazardous nature of the employee's tasks, the level of interaction of employee with public and the correlation between the employee's prior misconduct and the nature of the position sought.¹¹ Notwithstanding this lack of clarity, seemingly, it is in the interest of the employer to conduct a review of an applicant's profile before hiring the applicant.¹²

AQ6

Employers do in fact look

In fact, employers do conduct reviews of applicants' profile pages. According to a study conducted for CareerBuilder.com by Harris Interactive, 45% of employers surveyed use social networks to select applicants.¹³ Just one year earlier, a similar study found that 22% of employers were using social network sites such as Facebook, MySpace, Twitter and LinkedIn to review applicants.¹⁴ The study found that 35% of employers based their

decision to deny applicants jobs on the content viewed on the respective applicant's social networking site.¹⁵ In the study, Facebook proved to be the most popular social media site for employers to conduct their applicant screening (followed by LinkedIn, MySpace and Twitter).¹⁶ Over 50% of the employers who participated in the survey stated that provocative photos played the biggest role in a decision not to hire an applicant, while 44% of employers used applicants' references to drinking and drug use as red flags as a contributor to not employing the applicant.¹⁷ A survey commissioned by Microsoft in 2010 also showed that 79% of the U.S. employers which participated in the study used the Internet to screen applicants and that 70% employers rejected applicants based on the search results (Cross-Tab, 2010).

Not only have employers demonstrated their willingness to search profiles, but recently they have also demanded applicants' passwords to respective social media sites as a condition of employment.¹⁸ The practice first came to attention when the Maryland Division of Corrections (DOC) policy required that job applicants for employment with the DOC provide the government with their social media account usernames and personal passwords for use in employee background checks (Curtis, n.d.). As consequence, a corrections officer named Robert Collins was required to provide his Facebook login and password to the DOC. During the interview the interviewer logged on to Collins's social media site and read the latter's postings and those of his family and friends.

The above conclusions indicate that the employer (1) should review profiles, (2) at times may need to review profiles, (3) most times will review the profiles and (4) will use the information contained in profiles to deny a position. Stated differently, the law cannot and should not stop employers from searching profiles. How are these legitimate business and legal concerns contrary to the interests of the applicant?

The applicant's interests

It is the applicant's interest to participate in the world of social media sites without giving up the opportunity to gain employment because of merit or without being denied a position because of age, for example. However, when viewing unconstrained media site profiles, an employer is likely to discern, among other things, the age, religion, color, race, gender, disability, sexual orientation, military status or nationality of an applicant. This information gives the employer the ability to go beyond legitimate applicant recruitment and selection. The employer is afforded the opportunity to enter the realm of unlawful discrimination.

Typically, other than an applicant's gender (most times discoverable from the name on application) the applicant's attributes are likely to be revealed only after an interview. In fact, some characteristics may never be discovered. However, a pre-interview review of a profile is likely to reveal the above-mentioned classifications before the applicant meets with employer. Accordingly, the employer's ability to discriminate is greatly facilitated.

If the description of the issue were to end here, one could argue that social media sites have done nothing more than reduce the world to a small town; that is, a place where all residents (including employers) know the characteristics of all their neighbors (including job candidates) prior to any job interview. Consequently, one could argue, the ability to

discriminate using profiles has been facilitated only to the levels present in any small town where everyone knows everyone else. However, this argument would fail.

The adversarial system: no notice – no fight

Litigation

A fundamental difference exists between a small town and the cyber world: in the small town, the applicant has knowledge of the fact that the employer has the knowledge necessary to discriminate prior to an interview. The employer, for example, knowing the applicant's age before an interview, may decide not to select the applicant for an interview because of her age. The applicant, on the other hand, has the knowledge to suspect discriminatory conduct and therefore the ability to consider pursuing legal redress.

In the world of online profiles, however, absent an in-person interview, an applicant is not likely to know that she was denied an interview or position because of her age (an attribute the employer viewed on her profile), since she, generally, will have no knowledge of the employer's review of her profile page. In essence, the employer is rendered free to discriminate without the applicant's knowledge.

This predicament severely curtails the enforcement of anti-discrimination statutes in the recruitment phase. The U.S. legal system is based on the adversarial system.¹⁹ As opposed to the inquisitorial systems where a judge or other public decision maker is the proponent of the facts and legal evaluation,²⁰ 'an adversary system relies upon the parties to produce the facts and legal arguments that will be forwarded on their behalf, for such a system to function properly, the parties must be somewhat equally capable of producing their cases' (Rubenstein, 2002). '[The] accepted virtue of the common law, adversarial system of justice is that it leaves more control in the parties . . . By placing control in the individual over the state the adversary system reflects deeper values of liberalism and even natural justice' (Seligman et al., 2001). Our decision to resolve legal disputes in this manner, however, triggers equality concerns (Rubenstein, 2002: 1874). 'If one side in adversarial adjudication is ill-equipped – it cannot afford access to the system, or has less time and money to pursue evidence, or less skill in developing legal claims – then what emerges as the stronger case might not necessarily be the better case . . . [T]he parties must be given relatively equal opportunities to present their case' (ibid.; see also Wertheimer, 1988). The adversarial system hinges on party control of the investigation and presentation of evidence.²¹

AQ7

AQ8

The anticipatory use of social media information by employers does not simply trigger such concerns; it eradicates the adversarial system. More specifically, when an employer views the content of an applicant's profile prior to an interview, it gains an overwhelming competitive edge over the applicant and the law in the adversarial setting. As stated above, this preliminary view of the profile allows the employer to make the hiring decision without the applicant's knowledge that he or she is even under consideration. If an employer discerns an applicant's color, for example, and bases its decision not to hire on such factor, it is essentially free to unlawfully discriminate effortlessly and without much consequence; the applicant will simply never know that this misconduct has occurred.²² Without notice of the wrongdoing, the applicant will not seek redress;

hence, she will not investigate the matter, file a charge of discrimination or litigate the case; no adversarial setting will ever be called into play. That is, no enforcement of the anti-discrimination law will occur.

As stated above, in an adversarial system, the parties must be put on equal footing to present their case (Rubenstein, 2002: 1874). The adversarial system rests on each party's ability to investigate and present the evidence (Resnick, 1982: 379). The above-described applicant is clearly not on equal footing with the employer. In fact, she is likely to never become one of the adversaries. In essence, social media sites remove possible discriminatory conduct from the purview of justice by temporally moving such conduct outside reality and into the cyber world, rendering unlawful discrimination invisible.

Agency enforcement

The Equal Employment Opportunity Commission (EEOC) has the authority under Title VII and the ADA to file a Commissioner's charge independently of an employee or applicant's charge,²³ arguably lessening the harm caused by the lack of an adversarial system. The EEOC Compliance Manual states as follows:

While the principal means for implementing Commission policy is the investigation of individual charges, EEOC-initiated investigations are a necessary part of the enforcement process. Discrimination victims are often unaware of their rights or unaware of discriminatory practices. While this is typically so in cases of systemic discrimination, it is also true in cases where discrimination is less pervasive. Field offices should not hesitate to recommend Commissioner charges or initiate directed investigations when such action will fulfill EEOC's law enforcement mission.²⁴

The EEOC has a special interest in pattern or practice of discrimination cases because "it has access to the most current statistical computations and analyses regarding employment patterns" [and] was thought to be in the best position "to determine where 'pattern or practice' litigation is warranted" and to pursue it."²⁵

However, notwithstanding this mandate, in the end, the EEOC's authority to initiate its own litigation is rarely used. In 2011, only 47 Commissioner's charges were filed, while 99,947 charges were filed by individuals against their employer. The EEOC's reliance on the adversarial system is evident.²⁶ Given this heavy reliance, ostensibly, the EEOC is as powerless as the individual applicant as a means of discovering and redressing discriminatory conduct. After all, with the possible exception of pattern and practice cases (where statistics play a major role), the EEOC is in no better position than the applicant when it comes to discovering invisible discriminatory conduct. In the end, the EEOC's own enforcement of anti-discrimination law is also rendered less than efficacious.

The legal (and social) issues are then formulated: How can the law avoid interfering with the prudent employer's need to review content that clearly aids in its recruitment and selection process, and simultaneously deny the employer the opportunity to view and weigh factors which may potentially lead to unlawful discrimination? And how can the law achieve this without the applicant's notice of the unlawful discrimination?

The irrelevancy of current legislation²⁷

The password trend

The analysis begins with the most recent trend in the employer–employee/applicant relationship, that is, the employer’s practice of demanding applicants’ social media site passwords as a condition of employment or as a part of the hiring (see Maryland Division of Corrections matter described above). Although new, the practice may be short lived. Maryland itself became the first state to pass legislation prohibit employers from requiring applicants and employees to disclose their passwords (the law took effect on 1 October 2012).²⁸ On 1 August 2012, Illinois signed into law (effective 1 January 2013) amendments to the Right to Privacy in the Workplace Act,²⁹ thereby prohibiting, among other things, employers from asking applicants and employees to provide passwords and log-in information to personal social networking sites. Similar legislation has been introduced in California, Illinois, Maryland, Michigan, Minnesota, Missouri, New York, South Carolina and Washington.

Congress is currently considering two related bills. In April 2012, Representatives Eliot Engel and Jan Schakowsky introduced the Social Networking Online Protection Act,³⁰ and, in May 2012, Senator Richard Blumenthal and Representative Martin Heinrich introduced the Password Protection Act of 2012.³¹ Both proposed laws would prohibit employers from, among other things, requiring or asking an employee or applicant to provide a password for access to a personal social media account.

The proposed bills have been referred, respectively, to the House Committee on the Judiciary and the House Committee on Education and the Workforce. However, notwithstanding the recent re-election of President Obama, the likelihood that such proposals will be enacted into law remains low; the U.S. House of Representatives remains in control of the Republicans and the primary sponsors of the bills are Democrats.³² Regardless of the likelihood of passage, the proposals have, ostensibly, sent a clear message to employers, and, in the end, state legislation (if the trend continues) is likely to render federal law unnecessary.

Lawmakers’ overall reaction to this latest practice indicates that employees will not be subject to the password requirement. However, the legislative reaction does not protect the employees from the use of information that is openly available on the Internet.

The Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA), among other things, regulates employment background checks performed by third parties on behalf of an employer.³³ The Act requires that, when a third party prepares a background check of an employee or applicant, the latter must be notified of the investigation, given the opportunity to give or refuse consent, and notified if information from the report is used to make an adverse hiring decision. The FCRA requires an employer to ‘clearly and accurately notify applicants in writing if they will be the subject of a consumer credit report prepared by a consumer reporting agency.’

Unfortunately, the FCRA and its protections do not apply when an employer performs its own profile search. Accordingly, the FCRA would be of no aid to the aforementioned applicant.

Stored communications statutes

As stated above, this article's analysis is based on applicants whose profile is public. In instances where the applicant's media site is not public but is nevertheless accessed by an employer without the applicant's consent, a violation of the Stored Communications Act may be found. The Electronic Communications Privacy Act (ECPA)³⁴ includes federal wiretapping laws and federal laws prohibiting unauthorized access to communications in electronic storage.

Title II of the ECPA created the Stored Communications Act (SCA),³⁵ intended to 'address access to stored wire and electronic communications and transactional records.' The SCA makes it a federal crime for anyone to 'access' without 'authorization', or in excess of authorization, a 'facility providing electronic communication services and thereby obtaining access to a wire or electronic communication while it is in electronic storage.' The SCA would be of no help to an applicant with a public profile.³⁶

AQ 10

AQ 11

Federal Computer Fraud and Abuse Act

Although this Act is often used by employers to pursue claims against their employees, arguably, an employer who exceeds its authorized access to a profile or the social network's server may be in violation of the Computer Fraud and Abuse Act (CFAA).³⁷ Again, however, the CFAA would be of no help to an applicant with a public profile.

Title VII, the ADA and the ADEA

An array of anti-discrimination statutes exists if we consider state and federal law. The most fundamental federal statutes, however, follow. Under Title VII of the 1964 Civil Rights Act,³⁸ an employer shall not 'fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin.'³⁹ Under the Americans with Disabilities Act (ADA),⁴⁰ an employer cannot make an adverse employment decisions against 'an individual with a disability who, with or without reasonable accommodation, can perform the essential functions of the employment position that such individual holds or desires.' Pursuant to the Age Discrimination in Employment Act (ADEA), it is against the law for an employer 'to fail or refuse to hire or to discharge any individual or otherwise discriminate against any individual ... because of such individual's age.'⁴¹

AQ 12

As a consequence of this legislation and disparate treatment and disparate impact principles, employers are prohibited or discouraged from making inquiries such as the following examples:⁴²

- What is your race?
- What is your national origin?
- What is your religion?
- How old are you?
- Are you disabled?
- Are you married?

Do you have children?
Do you plan to have children?
Are you pregnant or planning to become pregnant?
How much do you weigh?
What is your religion?⁴⁵

The introduction of social media sites into this paradigm demonstrates the absolute irrelevance of employment law in the cyber world. A profile or even simply a posted photo of an applicant may offer the employer the answer to most of these inquiries, without the need to pose a single unlawful question. Also, as stated above, the employer can collect and consume such responses without the applicant's knowledge that she is unknowingly responding to unlawful inquiries. To a great extent, this represents the demise of anti-discrimination protection at the employee online recruitment and selection phase. The more the employer looks, the more it sees; the more it sees, the greater the potential for discrimination.

In the end, no current federal statute specifically prohibits employers from obtaining or utilizing information gathered from profile searches.

Conclusion and recommendations

The preliminary findings of this note are as follows: (1) the employer should review profiles, (2) the employer may need to review profiles, (3) the employer will, generally, review profiles and (4) the employer will, generally, use information contained in profile to make a hiring decision. It is also clear that (5) the employer's review of social media sites takes any potential discriminatory conduct outside the temporal parameters contemplated by current anti-discrimination statutes, and, consequently, (6) the applicant and the EEOC are unlikely to discover the discriminatory conduct. Finally, (7) without notice of the misconduct, the adversarial system stops functioning and (8) with it the enforcement of anti-discrimination law at that employment phase.

Based on these conclusions, it seems clear that the law cannot (and should not) stop employers from searching profiles. Accordingly, to remain consequential in this new world, anti-discrimination protection must find a presence in that pre-interview slice of time. Two avenues seem most apt for achieving this end.

Reporting searches

The first option is to steer away from the reasoning reflected in the current 'password-related legislation' discussed above. That is, given the absence of an adversarial system to enforce the law, a categorical prohibition of employer's use of social media content in hiring decisions would be less than a weak warning. Since it seems clear that employers are actually using the online content to make decisions, the first clear choice is to require employers to report to the EEOC and the applicant every instance of social media site review (in the context of making hiring-related decision). As a result, the applicant and the EEOC would have notice of the review and the option to re-enter the adversarial system should discriminatory conduct be suspected.

The reporting system currently required by the FCRA should be expanded.⁴⁴ As stated above, among other things, this law regulates employment background checks performed by third parties on behalf of an employer.⁴⁵ The Act requires that, when a third party prepares a background check of an employee or applicant, the employer must 'clearly and accurately notify applicants in writing if they will be the subject of a consumer credit report prepared by a consumer reporting agency.'⁶⁵ The FCRA's protections have not been expanded to cover an employer that conducts its own background check. Amending the law to make it applicable to an employer's own searches would, as stated above, reactivate the adversarial system by giving notice to the applicant and the EEOC. Of course, traces of the problem remain: How can one ascertain if the self-regulated reporting is a true reflection of the employer's searches? For unscrupulous employers, the ones more likely to discriminate, the searches and the discrimination would and could easily remain invisible.

AQ 13

The small town presumption

The second option consists of applying a rebuttable presumption element to discrimination cases dealing with this issue. In discrimination cases related to this issue, employers would hold the burden of rebutting the presumption that they did view social media sites when they made their hiring decision. This is arguably a quasi-irrefutable presumption in instances where an employer has an actual, declared Internet screening policy.

Obviously, the employer's burden of rebutting the presumption would be onerous. However, placing this burden on the employer in order to rescue the adversarial system is a burden worth imposing. In the end, such a presumption would create no greater burden than that of an employer operating in the small town alluded to above. As in the small town, the presumption puts the two adversaries on equal footing by giving the applicant constructive notice of the employer's profile review. Consequently, as in the small town, the employer knows the applicant and the applicant knows this fact prior to recruitment efforts. This 'small town presumption' is as imperfect as the current effectiveness of existing anti-discrimination legislation in small communities. However, at a minimum, it offers such body of law presence and relevancy in the cyber world.

Notes

1. The focus of this article is on the effects of social media sites/profiles on discriminatory practices in the workplace. However, it should be mentioned that the growth of such communications has also impacted employee privacy, discipline and discharge, and has also not left union-protected employees unscathed.

Several cases have seen the application of tort-based legal theories such as defamation, invasion of privacy, wrongful disclosure of confidential information or trade secrets. Cases against public employers also rely on the U.S. Constitution, arguing that profile searches constitute an unreasonable search and seizure. Other cases have raised exceptions to the general at-will doctrine such as violation of public policy and statutory protections such as anti-retaliation statutes based on protected activities such as free speech.

For examples of cases dealing with discipline and discharge of employees due to social media site posts, see *Simonetti v. Delta Airlines*, No. 1:05-CV-2321, 2005 WL 2407621

(N.D. Ga. Sept. 7, 2005), in which a flight attendant posted a suggestive photo of herself on MySpace page and was later discharged for the same; and *Pietrylo v. Hillstone Rest. Grp.*, No. 06-5754 (FSH), 2008 U.S. Dist. LEXIS 108834 (D.N.J. July 25, 2008), in which an employee was discharged after starting a MySpace page and posting numerous comments about management. See also www.higheredmorning.com/professor-suspended-for-facebook-posts (accessed 1 September 2012), regarding a professor who was suspended after a student reported humorous comments on her Facebook page, about “not wanting to kill” any students that day; see also Webley (2011).

Social media sites’ popularity has also impacted union-protected employees. On 30 May 2012, the National Labor Relations Board (NLRB), through its Acting General Counsel (GC), issued a third Operations Management Memo on social media cases in less than a year; see www.nlr.gov/news/acting-general-counsel-releases-report-employer-social-media-policies (accessed 8 July 2012).

See also the 2011 NLRB survey, which indicates that the NLRB has reviewed more than 129 cases involving social media sites. The central issues of cases regard discharge or discipline of employees based on their social media posts and whether the posts are a protected activity under the National Labor Relations Act; see www.uschamber.com/sites/default/files/reports/NLRB%20Social%20Media%20Survey%20-%20FINAL.pdf (accessed 28 August 2012).

2. Throughout this article, the terms ‘social media site’ and ‘profile’ are used synonymously and are defined as follows: a form of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages and other content (such as videos). See www.merriam-webster.com/dictionary/social%20media (accessed 23 September 2012). Popular examples include Facebook, Twitter, LinkedIn and YouTube.

Throughout this article it is presumed that an applicant’s social media site/profile (such as a Facebook profile) is public and not protected by privacy settings.

3. Restatement (Second) of Agency § 219(1) (1958).
4. Restatement (Second) of Agency § 213 (1958).
5. *Ibid.*
6. *Perodeau v. Hartford*, 259 Conn. 729, 754, 792 A.2d 752 (2002).
7. *Knicrumah v. Albany City School District*, 241 F.Supp.2d 199, 211 (N.D.N.Y.2003).
8. For example, Connecticut law requires all public school employees hired on or after 1 July 1994 to submit to state and national criminal history record checks when they are hired. According to a survey by *Education Week*, 42 states require criminal background checks for teacher certification. The states that do not have background check requirements for teachers are Illinois, Indiana, Massachusetts, North Carolina, Ohio, Pennsylvania, Tennessee and Wisconsin. See *Education Week* (2003).
10. See, for example, *Kendall v. Gore Props, Inc.*, 236 F.2d 673 (D.C. 1956); *Weiss v. Furniture in the Raw*, 306 N.Y.S.2d 253 (N.Y. Civ. Ct. 1969); *Robertson v. Church of God Int’l*, 978 S.W. 2d 120, 125 (Tex. App. 1997) (‘One who retains the services of another has a duty to investigate the background of that individual for fitness for the position....’).
11. ‘Liability of the employer is predicated on the employer’s antecedent ability to recognize a potential employee’s “attribute[s] of character or prior conduct” which would create an undue risk of harm to those with whom the employee came in contact in executing his employment

responsibilities.... The scope of the employer's duty in exercising reasonable care in a hiring decision depends on the employee's anticipated degree of contact with other persons in carrying out the duties of employment. The requisite degree of care increases, and may require expanded inquiry into the employee's background, when the employer expects the employee to have frequent contact with the public or when the nature of the employment fosters close contact and a special relationship between particular persons and the employee.' *Moses v. Diocese of Colorado*, 863 P.2d 310, 323–324 at 327–328 (Colo.1993), cert. denied, 511 U.S. 1137, 114 S.Ct. 2153, 128 L.Ed.2d 880 (1994) (citations omitted), quoting *Connes v. Molalla Transport System, Inc.*, 831 P.2d 1316, 1321 (Colo.1992).

For example, in *Ponticas v. K.M.S. Invs.*, 331 N.W.2d 907, 911 (Minn. 1983), 'the apartment manager had access to tenants' homes, his employer had a duty to conduct a reasonable investigation to explore whether the manager posed a high risk of injury to the apartment complex's residents. The employee in question had a criminal history of armed robbery and other felonies that a cursory criminal background check would have revealed. Additionally, the employee had listed his mother and sister as his employment references. Due to the ease with which the employer could have discovered that the employee had committed violent crimes and had provided sham employment references, the court upheld the jury's finding that the employer was liable for negligent hiring'(Peebles, 2012: 1397).

See also Bick (2009a,b).

12. In jurisdictions where the duty clearly does not exist, an argument could be made that, if an employer may only be liable for what is reasonably foreseeable, it behooves him not to review any profiles and to argue ignorance of any of the applicant's propensities. However, as can be learned from the statistics below, the employer is likely to deem the benefits of a search to outweigh the possible consequences of the review.
13. www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8/19/2009&ed=12/31/2009 (accessed 30 June 2012).
14. Ibid.
15. Ibid.
16. Ibid.
17. Ibid.
18. This trend has been met with opposition, as discussed below.
19. See, for example, *Lassiter v. Dep't of Soc. Servs.*, 452 U.S. 18, 28 (1981) ('[O]ur adversary system presupposes [that] accurate and just results are most likely to be obtained through the equal contest of opposed interests...'); *McNeil v. Wisconsin*, 501 U.S. 171, 181 n.2 (1991) ('What makes a system adversarial rather than inquisitorial is ... the presence of a judge who does not (as an inquisitor does) conduct the factual and legal investigation himself, but instead decides on the basis of facts and arguments pro and con adduced by the parties').
20. As is the case in most of Europe (see Langbein, 1985).
21. Resnik (1982: 380 n.23); see also Resnik (2000: 2136) ('Equipage for civil litigants – from filing fees to investigation to counsel for experts – is generally left either to the legislature or to the market').
22. Arguably, an applicant could hire an expert to find an online trail left by an employer's search. However, without some notice of the employer's search or suspicion thereof, the applicant's curiosity is unlikely to be sufficiently aroused to take such steps. Also, in the cases where the suspicion or notice is present, the cost of such steps may be prohibitive.

Title VII of the Civil Rights Act, the Americans with Disabilities Act (ADA) and the Age Discrimination in Employment Act (all discussed below) do require employers to retain applications and other personnel records relating to hiring process. One could argue that such records could be used to trigger investigations, etc. However, the unscrupulous employer, the one most likely to discriminate, is unlikely to abide by this law if it knows the chances of being found out are minimal. Moreover, the applicant is not automatically entitled to a copy of such records, so who would review such innumerable documents?

23. See 42 U.S.C. § 2000e-6(e) (2008); 29 C.F.R. §§ 1601.7–11; § 2000e-5(b);

1 EEOC Compliance Manual (BNA) 8:0001 (2001) (hereinafter referred to as EEOC Intake): ‘Under Title VII/ADA, EEOC must have a basis to investigate possible violations and must obtain a Commissioner charge and notify the respondent of such basis by specifying the date, place and circumstances to be covered by the investigation. Under ADEA/EPA, there are no prerequisites which must be met to investigate.’

No Commissioner’s charge provisions are found in the Age Discrimination in Employment Act (ADEA) and the EPA; however, the EEOC may investigate violations of these two statutes (EEOC Intake).

AQ 14

24. *Ibid.*
25. *Equal Employment Opportunity Comm’n v. Shell Oil Co.*, 466 U.S. 54, 69 (1984).
26. www.eeoc.gov/eeoc/plan/upload/2011par.pdf (accessed 18 September 2012).
27. With some exceptions, the ensuing discussion does not examine state (U.S.) anti-discrimination law, but focuses on pertinent federal law.
28. To be codified at Md. Code Ann., Lab. & Empl. § 3-712.
29. Illinois HB 3782 amends the state’s Right to Privacy in the Workplace Act.
30. H.R. 5050, 112th Cong., 2d Sess. (Apr. 27, 2012).
31. S. 3074, 112th Cong., 2d Sess. (May 9, 2012).
32. www.govtrack.us/congress/bills/112/hr5050 (accessed 10 November 2012); www.govtrack.us/congress/bills/112/hr5684 (accessed 10 November 2012).
33. 15 U.S.C. §§ 1681–1681t (2000 & Supp. 2003).
34. 18 U.S.C. §§ 2510–2522
35. 18 U.S.C. Chapter 121 §§ 2701–2712.
36. In *Crispin v. Christian Audigier Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010), a federal district court decided that the SCA applies to social media posts, provided that a posting had established privacy settings, was content electronically stored within the meaning of the SCA and thus could not be accessed without authorization.
- See also *Pietrylo v. Hillstone Rest. Group*, 2008 WL 6085437; and *Konop v. Hawaiian Airlines, Inc.*, 236 F.3d 1035 (2001) (D.N.J. July 24, 2008), making it clear that under some circumstances unconsented access to private media sites may constitute a violation of the SCA.
37. 18 U.S.C. § 1030.
38. 42 U.S.C. §§ 2000e-2 (2000).
39. 42 U.S.C. §§ 2000e-2(a)(1).
40. 42 U.S.C. §§ 12101–12213 (2000).
41. 29 U.S.C. §§ 621–634 (2000).
42. Many of such questions are not explicitly prohibited by the language of the aforementioned anti-discrimination laws (except for the ADA), but in some cases have been de facto made

unlawful by federal regulations and EEOC guidance. It is beyond the scope of this article to discuss specific federal regulations and EEOC guidance regulating such inquiries.

43. 29 U.S.C. §§ 621–634 (2000).
44. 15 U.S.C. §§ 1681–1681t (2000 & Supp. 2003).
45. *Ibid.*
65. *Ibid.*

References

Bick J (2009a) Proceed with caution: social networking websites and blogs. *Labor Law Reports*, 27 May. Available at: www.bicklaw.com/Publications/LAWFULMININGOFSOCIALNETWORKS.htm (accessed 1 June 2012).

Bick J (2009b) Lawful mining of social networks. *New Jersey Law Journal*, 16 February.

Cross-Tab (2010) Online reputation in a connected world 5-6. Available at: www.microsoft.com/privacy/dpd/research.aspx (follow hyperlink labeled ‘Online reputation research overview PDF’) (accessed 8 September 2012).

Curtis M (n.d.) Want a job? Password, please! Available at: www.aclu.org/blog/technology-and-liberty/want-job-password-please (accessed 8 July 2012).

Education Week (2003) State policies on sexual misconduct between educators and students. 30 April.

AQ 15 Epstein RA (2008) *Cases and Materials on Torts*, 9th edn.

Kluemper DH, et al. (2012) Social networking websites, personality ratings, and the organizational context: more than meets the eye? *Journal of Applied Social Psychology* 42(5): 1143–1172.

AQ 16 Langbein JH (1985) The German advantage in civil procedure. *University of Chicago Law Review* 52: 823.

AQ 17 Larson LK (2010) *State-by-State Analysis, Employment Screening (MB)*.

Mooney DE (2010) Comment, employer on the web wire: balancing the legal pros and cons of online employee screening. *Idaho Law Review* 46: 733.

AQ 19 Peebles KA (2012) Negligent hiring and the information age: how state legislatures can save employers from inevitable liability. *William & Mary Law Review* 53: 1397.

AQ 20 Resnik J (1982) Managerial judges. *Harvard Law Review* 96: 374.

Resnik J (2000) Money matters: judicial market interventions creating subsidies and awarding fees and costs in individual and aggregate litigation. *University of Philadelphia Law Review* 148: 2119.

AQ 22 Rubenstein WB (2002) The concept of equality in civil procedure. *Cardozo Law Review* 23: 1865.

AQ 23 Seligman MEP, et al. (2001) Why lawyers are unhappy. *Cardozo Law Review* 23: 33.

Webley A (2011) How one teacher’s angry blog sparked a viral classroom debate. Time/CNN, 18 February. Available at: www.time.com/time/nation/article/0,8599,2052123,00.html#ixzz1Fz9Ba0fz (accessed 1 September 2012).

AQ 25 Wertheimer A (1988) The equalization of legal resources. *Philosophy & Public Affairs* 17: 303.