INVASION OF THE SOCIAL NETWORKS:
BLURRING THE LINE BETWEEN PERSONAL LIFE
AND THE EMPLOYMENT RELATIONSHIP

Robert Sprague*

ABSTRACT

Over one-half billion people worldwide have registered accounts with Facebook, the most popular online social network. This Article addresses some of the more significant employment-related legal issues arising from the growing popularity of online social networks. First, the need for employers to investigate the background of prospective employees is examined from the context of employers using online social networks to conduct those investigations. In particular, this Article analyzes the degree to which job applicants have privacy rights in the information they post online. This Article then examines the interrelationship between online social networks and employees, focusing on limitations faced by employers in taking adverse actions against employees based on their online activities. This Article also examines the rights of employers to access employee online communications, as well as potential liabilities for employers based on employee online communications. This Article concludes with a set of best practices recommendations to assist employers in keeping pace with the changing legal landscape associated with online social networks.

I. INTRODUCTION

In 2010, the number of worldwide registered users of Facebook, the online social network site,1 reached one-half billion.2 Facebook is certainly

---

* J.D., M.B.A. Associate Professor, University of Wyoming College of Business, Department of Management & Marketing.

1 Social network sites have been defined as "as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system." danah m. boyd & Nicole B. Ellison, Social Network Sites: Definition, History, and Scholarship, 13 J. COMPUTER-MEDIATED COMM. 210, 211 (2008). In case you were wondering, danah boyd chooses to not capitalize her name for personal and political reasons. See danah boyd, what’s in a name?, DANAH.ORG, http://www.danah.org/name.html (last visited Oct. 10, 2011). Online social network sites are a subset of online social media, which include social networking attributes accompanied by different media, such as photos (e.g., Flickr.com) or videos (e.g., YouTube.com).

not the only one of its type, meaning that a substantial number of people are connected through online social networks. As boyd and Ellison point out, what makes online social network sites unique is not that people are meeting strangers, but that they are articulating and making visible their social connections. “The public display of connections is a crucial component of [online social network sites].” Individuals use online social network sites to create “intimacy, community, and identity-building through selective disclosure.” Ultimately, online social network “members craft highly detailed digital identities that are displayed for all expected, as well as some unexpected, audiences.”

---

1. SixDegrees.com, launched in 1997, is considered to be the first true online social network site. See boyd & Ellison, supra note 1, at 214. Friendster was launched in 2002 as a social compliment to the business-focused Ryze.com, launched in 2001. Id. at 215. Friendster, though, had difficulty coping with its growing popularity, and in 2003, MySpace was launched, in part, to attract frustrated Friendster users. Id. at 215–17. Although Facebook initially limited access to college students, id. at 218, once it opened access to the general public, it soon eclipsed MySpace as the most popular social network site. See Aaron Prebluda, Facebook vs. MySpace: Tale of the Tape, COMPETEPULSE.COM (Feb. 26, 2009, 1:00 PM), http://blog.compete.com/2009/02/26/facebook-myspace/ (noting that Facebook overtook MySpace in February 2009 in terms of the number of unique visitors to their respective sites). It should be pointed out that some social network sites practically unknown in the United States are very popular in other countries, such as Google’s Orkut (principally in Brazil) and Microsoft’s Windows Live Spaces. boyd & Ellison, supra note 1, at 216.

2. See James Grimmelmann, Saving Facebook, 94 IOWA L. REV. 1137, 1142 n.4 (2009) (describing, in particular, the difference between a social network, i.e., the “map” (Facebook), and social networking, i.e., the “territory” (the relationships among people)). Though they recognize that the terms “social networking sites” and “social network sites” are used almost interchangeably, boyd and Ellison use the latter because “‘networking’ emphasizes relationship initiation,” which is not the primary practice of sites such as Facebook. See boyd & Ellison, supra note 1, at 211.

3. boyd & Ellison, supra note 1, at 211.

4. Id. at 213.

5. Patricia Sánchez Abril, Recasting Privacy Torts in a Spaceless World, 21 HARV. J.L. & TECH. 12 (2007). Online social network users register with a site and create a profile, which usually consists of the user’s name, country, zip code, gender, date of birth, a list of friends, a list of groups with shared interests, pictures, videos, links to Internet pages, as well as updates of personal information, such as dating/marital status, sexual preference, etc. See id. at 13–14 (describing a typical MySpace profile). See also Samantha L. Millier, Note, The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet, 97 KY. L.J. 541, 544 (2008/2009) (describing the type of information used to create a typical Facebook profile).

6. Sánchez Abril, supra note 7, at 14. “[F]or teenagers, the online realm may be adopted enthusiastically because it represents ‘their’ space, visible to the peer group more than to adult surveillance, an exciting yet relatively safe opportunity to conduct the social psychological task of adolescence[, including] . . . floating communicative norms and other risk-taking behaviours.” Sonia Livingstone, Taking Risky Opportunities in Youthful Content Creation: Teenagers’ Use of Social Networking Sites for Intimacy, Privacy and Self-expression, 10 NEW MEDIA & SOC’Y 393, 396–97 (2008). “Indeed, it seems that even normatively valued online activities are correlated in practice with risky activities regarding online content, contact and conduct, suggesting that what for an adult observer may seem risky, is for a teenager often precisely the opportunity that they seek.” Id. at 397.
Businesses—and, hence, employers—are now beginning to discover the value of the visibility of those online social connections. In just a few short years, employers have gone well beyond just Googling job applicants to learn more about their prospective employees than what is revealed in résumés or job interviews. Employers are able, either on their own or with the aid of specialized services, to mine a broad array of personal data from online social network sites, particularly Facebook.

Businesses are also beginning to avail themselves of the benefits of, as well as suffer some negative consequences from, social networks. On February 15, 2011, a Red Cross employee accidentally used the Red Cross Twitter account to send a message about finding more beer to drink, concluding, “when we drink we do it right #gettngslizzerd.” Red Cross was praised for how it used Twitter and its blog to admit the mistake and make fun of itself, resulting in donations from fans of the beer in question. In contrast, after being sued for allegedly misrepresenting the content of beef in its food, Taco Bell was criticized for trying to “buy back” its customers with a Facebook promotion. And some businesses have discovered the negative public relations that can arise through the viral aspects of social media. For example, in 2009, two Domino’s Pizza employees uploaded to YouTube a video made in a Domino’s kitchen in which one of them made sandwiches for delivery while violating a number of health codes. Within days, the video had been viewed more than a million times. One commentator labeled the incident a “nightmare” for Domino’s, and a Domino’s spokesperson stated, “We got blindsided by two idiots with a video camera and an awful idea . . . . Even people who’ve been with us as loyal customers for 10, 15, 20 years, people are second-guessing their relationship with Domino’s, and that’s not fair.”

---

9 One industry analyst noted that in 2010, fifty-nine of the global Fortune 100 companies were “recruiting staff specifically assigned to core social media duties that include customer outreach, PR and marketing support and internal communications.” *The State of Social Media Jobs 2010 – A Special Report*, SOCIALMEDIAINFLUENCE.COM (June 14, 2010, 2:13 PM), http://socialmediainfluence.com/2010/06/14/the-state-of-social-media-jobs-2010-a-special-report/.


11 Id.

12 Id. But see Craig Daitch, *Taco Bell Uses Humor, Social Media to Dig Itself out of Beef Scandal*, ADVERTISINGAGE (Feb. 4, 2011, 9:41 AM), http://adage.com/digitalnext/post?article_id=148675 (arguing that Taco Bell is engaged in an effective, proactive social media campaign).


14 Id.

15 Id.
employees are publicly complaining on Facebook about customers and supervisors, as well as suing employers based on their colleagues’ Facebook postings.

Online social networks have arrived in the workplace and their presence raises a number of legal issues that have yet to be fully addressed by the courts or lawmakers. Part II of this Article addresses one of the most significant impacts of online social networks on the employment relationship—vetting potential employees. One recent survey reveals that nearly eighty percent of individuals involved in hiring and recruiting use the Internet to investigate candidates. Part II explores why potential employers find online social network data so valuable, as well as the risks posed by searching out and using that data. Part III of this Article focuses on online social networks and the employment relationship, particularly possible limitations on employers’ abilities to discipline or terminate employees as a result of their online postings. Part III also explores additional interrelationships between employers and employee online postings, exploring employer discovery rights to employee online social network content, as well as potential employer liability for employee online postings. Part IV provides a concluding analysis, including recommendations for employers in controlling online social networks within the employment context.

II. SEARCHING ONLINE REPUTATIONAL INFORMATION TO VET JOB APPLICANTS

According to a 2010 survey commissioned by Microsoft Corporation, nearly eighty percent of surveyed United States hiring and recruiting professionals research applicants online. The survey focused on online reputation, which it described as “the publicly held social evaluation of a person based on his or her behavior, what he or she posts, and what others

---

16 See, e.g., Eric Frazier, Facebook Post Costs Waitress Her Job, CHARLOTTEOBSERVER.COM (May 17, 2010), http://www.charlotteobserver.com/2010/05/17/1440447/facebook-post-costs-waitress-her.html (reporting on a waitress who was fired after posting a complaint about customers on her Facebook account). When someone publishes content online, it is generally referred to as “posting.”
18 See, e.g., Amira-Jabbar v. Travel Serv., Inc., 726 F. Supp. 2d 77 (D.P.R. 2010) (dismissing plaintiff’s discrimination claim which was based, in part, on photos of a company outing and associated comments uploaded by an employee to his Facebook account).
Recruiters are using online reputational information to discover if there is something about a candidate’s lifestyle that might be questionable or that might go against the core values of the hiring company. As a camp counselor recruiter noted, “You really get a lot of information that you can’t ask for in a job interview, but you go on the Web and it’s all there . . . .”

While search engines remain the most prevalent source of online data (used by 78% of surveyed hiring and recruiting professionals), online social network sites are also frequently searched (by 63% of respondents), as are photo and video sharing sites (59%), professional and business network sites (57%), personal websites (48%), blogs (46%), online forums and communities (34%), and even online gaming sites (27%).

The same survey also reported that 70% of hiring and recruiting professionals in the United States have rejected a candidate based on data found online. Fifty-eight percent of surveyed hiring and recruiting professionals reported that lifestyle concerns reflected online influenced a decision to reject a candidate. Lifestyle concerns were followed closely by inappropriate comments and text written by the candidate (influencing a rejection 56% of the time) and unsuitable photos, videos, and information (55%). Other online information which was a factor in rejecting a candidate: inappropriate comments or text written by friends and relatives (influencing a rejection 43% of the time); comments criticizing previous employers, co-workers, or clients (40%); inappropriate comments or text written by colleagues or work acquaintances (40%); membership in certain groups and networks (35%); discovering that information the candidate shared was false (30%); and displaying poor communication skills online (27%).

One concern with vetting job applicants using online reputational information is context: “The [Internet] is a virtual landscape of ex parte communications that could prove damaging to careers and academic

21 Id. at 3.
23 Pam Belluck, Young People’s Web Postings Worry Summer Camp Directors, N.Y. TIMES, June 22, 2006, at A16 (internal quotation marks omitted).
24 CROSS-TAB, supra note 20, at 8.
25 Id. at 5. Interestingly, only seven percent of U.S. consumers surveyed believe information about them online affected their job search. Id.
26 Id. at 9.
27 Id.
28 Id.
opportunities, if viewed outside their original social context. 29 While recruiters generally understand an applicant may be merely posturing when outlandish statements are unearthed online, it still leads them to question the person’s judgment. 30 So while a majority of recruiters who use online reputational information to evaluate a candidate recognize that much of the information may be inaccurate, it is nonetheless still often used to reject a candidate. 31

Investigating employee lifestyles is not new. In 1914, the Ford Motor Company instituted a profit sharing plan which imposed significant conditions on workers to qualify to participate in the plan, including “age, sex, character, habits and behavior, home conditions, matrimony, dependents, wage rating, and, later on length, of service.” 32 As a result, investigators visited the homes of employees “in order to examine home conditions, to find out whether a man drinks, how he spends his evenings, whether he has a bank account, dependents, etc.” 33 A Ford worker was entitled to the additional wages through the profit sharing plan only after the company was satisfied he would “not debauch the additional money he receive[d].” 34 Critics charged these investigations, conducted by the company’s “Sociological Department,” were merely a means by which the Ford Motor Company could pry into the private affairs of its workers and compel them to comply with Henry Ford’s rigid code of conduct. 35

29 David Rosenblum, *What Anyone Can Know: The Privacy Risks of Social Networking Sites*, 5 IEEE SECURITY & PRIVACY 40, 46 (2007) (“Because so many profiles contain third-party comments or communications, the temptation to condemn an individual for uncensored or injudicious posts to friends is great.”).

30 Finder, *supra* note 22 (describing one recruiter who discovered an applicant’s online boasting of “smokin’ blunts” (cigars hollowed out and stuffed with marijuana), shooting people and obsessive sex; while recognizing it was simple posturing, the recruiter also eliminated the applicant from consideration due to lack of judgment).

31 *Cross-Tab, supra* note 20, at 9–10.

32 Samuel M. Levin, *Ford Profit Sharing, 1914–1920: I. The Growth of the Plan*, in *HENRY FORD: CRITICAL EVALUATIONS IN BUSINESS AND MANAGEMENT* 160, 163 (John C. Wood & Michael C. Wood eds., 2003). The plan was a bit unique, in that it was designed to distribute some $10,000,000 in anticipated profits for the year and was not contingent upon the company earning a particular amount of profit, nor initially on the employees’ length of service or level of output. *Id. at* 163. The principal goal of the plan was to establish a base minimum wage of $5.00 per day. *Id.*

33 *Id.*

34 *Stephen Meyer III, The Five Dollar Day: Labor Management and Social Control in the Ford Motor Company 1908–1921* 125 (1981). Every Ford employee who earned less than $200 per month (i.e., all but high level managers and supervisors) was investigated. *Id. at* 129–30. The investigations focused on three distinct aspects of the lives of the workers: social and biographical information; economic and financial conditions of the workers and their families; and morality, habits, and lifestyle. *Id. at* 130.

The twenty-first century equivalent issue is whether employers have the legal right to investigate the online lives of their job applicants. Fundamentally, it rests on the degree to which job applicants enjoy a right to informational privacy. In the employment context, individual rights of informational privacy are balanced against an employer’s legitimate need to discover the information. As such, before discussing the parameters of informational privacy, it is necessary to understand the informational needs of the employer.

A. Why Employers Need to Investigate Job Applicants

Beyond managerial concerns of whether a new employee is competent and will fit within the organization, there is potential legal liability facing employers arising from negligent hiring. To establish liability due to an employer negligently hiring an employee, a third-party plaintiff must first establish the employer owed a duty to that particular plaintiff “arising out of the relationship between the employment in question and the particular plaintiff, owed to a plaintiff who is within the zone of foreseeable risks.”

provided protection to the non-unionized workers against arbitrary actions by foremen and supervisors. Id. at 71. The investigations created uneasiness among Ford’s workers and were scaled back in 1917. MEYER III, supra note 34, at 165 (noting the department’s name was changed to the “Educational Department,” investigators were renamed “advisors,” and the department no longer investigated employees with more than one year’s service with the company). A combination of worker disgruntlement with the program and an economic recession led to the Ford Motor Company ending the profit sharing plan, and its attendant investigations, in 1920. Id. at 197.

Information privacy addresses control and handling of personal data. Daniel Benoliel, Law, Geography and Cyberspace: The Case of On-line Territorial Privacy, 23 CARDOZO ARTS & ENT. L.J. 125, 128 (2005). See also ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (“Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”); Charles Fried, Privacy, 77 YALE L.J. 475, 482 (1968) (describing privacy as “not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves”). Commentators and courts use the terms “information privacy” and “informational privacy” interchangeably.

See, e.g., Ann Marie Ryan & Marja Lasek, Negligent Hiring and Defamation: Areas of Liability Related to Pre-Employment Inquiries, 44 PERS. PSYCHOL. 293, 293 (1991) (citing WAYNE F. CASCIO, APPLIED PSYCHOLOGY IN PERSONNEL MANAGEMENT (1982)) (noting the rationale behind past-employment and background checks is that “past performance is the best predictor of future behavior”); id. at 304 (discussing “screen-in”—looking for desirable characteristics—and “screen-out”—looking for reasons to reject a candidate—selection procedures to determine fitness); Carolyn Wiley & Docia L. Rudley, Managerial Issues and Responsibilities in the Use of Integrity Tests, 43 LAB. L.J. 152, 152 (1991) (discussing overt integrity tests which are designed to “measure an applicant’s attitudes toward a wide range of counterproductive on-the-job behaviors,” particularly theft and other forms of dishonesty). See generally Chris Piotrowski & Terry Armstrong, Current Recruitment and Selection Practices: A National Survey of Fortune 1000 Firms, 8 N. AM. J. OF PSYCHOL. 489 (2006) (discussing survey data on recruitment and employment selection methods, particularly the nexus between personality factors and personnel selection and placement).
created by the employment.” 38 Once the duty is established, the plaintiff must show the employer breached that duty in hiring the employee by showing that:

(1) the employer was required to make an appropriate investigation of the employee and failed to do so; (2) an appropriate investigation would have revealed the unsuitability of the employee for the particular duty to be performed or for employment in general; and (3) it was unreasonable for the employer to hire the employee in light of the information he knew or should have known. 39

For example, where an employee was hired to perform outdoor landscaping work and would have only incidental contact with tenants, the employer had no duty to make an investigation into the employee’s background. 40 But when the employer, after three weeks, gave a passkey to the employee so he could perform work inside residences managed by the employer, the employer had a duty to investigate the employee’s background. 41

Foreseeability is the most important element of the breach-of-duty component, creating a significant burden for employers. 42 Although most negligent hiring cases have involved plaintiffs suffering physical harm at the hands of an employee, 43 courts have held employers liable for the negligent hiring of dishonest employees whose crimes of deceit have caused damage to third parties. 44 The major dilemma facing employers is that “courts have been inclined to take a rather sweeping view of the range of outcomes that should be considered foreseeable risks, yet have provided few guidelines to aid employers in defining the elements of employee ‘fitness’ or in deciding just how probing a ‘reasonably sufficient’

---

39 Garcia, 492 So. 2d at 440 (citations omitted).
41 Id. but see Garcia, 492 So. 2d at 442–43 (holding that employee’s responsibilities of driving a truck gave the employer no reason to investigate whether the employee was a “dangerous character”).
42 Byford, supra note 38, at 360.
44 Byford, supra note 38, at 362.
This leaves open the issue of just how extensively employers can investigate applicants’ backgrounds.

B. Limits on Employer Background Checks

There are very few bright-line legal restrictions on employers’ abilities to investigate applicants’ backgrounds. One specific restriction is found in Title VII of the Civil Rights Act of 1964, which prohibits employers from making employment-related decisions, including hiring decisions, on the basis of a person’s race, color, religion, sex, or national origin. The Americans with Disabilities Act prohibits employers from discriminating against qualified individuals on the basis of disability in regard to job application procedures or hiring. Employers are also prohibited from discriminating against potential hires if they are forty years or older. Prospective employers would very easily be able to discern whether an applicant was a member of a protected class by reviewing the applicant’s online social network profile. While employers are generally prohibited from asking certain discriminatory questions during the application or interview process, even when an applicant volunteers information the employer is otherwise prohibited from asking, the employer still cannot use that information in the hiring decision.

Employers are also beginning to see limits on their ability to perform credit checks on applicants. Employers are permitted to perform credit

45 \textit{Id.} at 360 (footnote omitted).


49 \textit{See, e.g.}, Gaskell v. Univ. of Ky., No. 09-244-KSF, 2010 U.S. Dist. LEXIS 124572, at *27–30 (E.D. Ky. Nov. 23, 2010) (denying prospective employer’s motion for summary judgment of candidate’s religious discrimination claim based on evidence plaintiff was the top candidate for a position until the search committee became aware of the candidate’s religious views through an Internet search).


51 \textit{See, e.g.}, Phillip M. Perry, \textit{Your Most Dangerous Legal Traps When Interviewing Job Applicants,} 20 LAW. PRAC. MGMT., Mar. 1994, at 50, 54.
checks of job applicants under the Fair Credit Reporting Act, though employers must notify an applicant in writing if a report is to be obtained and if a resulting report is used in making an adverse decision, such as deciding not to hire an applicant. Four states prohibit employers from using credit history reports without a bona fide occupational justification, while over one dozen additional states are considering similar legislation. And the EEOC has filed suit against one employer, claiming the use of credit history information has had a significant disparate impact on black job applicants, where the use of the information was not job-related and not a business necessity.

As discussed more fully below, employers may also be prevented from deciding whether to hire someone based on their consumption of lawful products. The majority of these statutes prohibit employers from making an employment decision based on an applicant’s tobacco use. However, seven states prohibit employers from making an employment decision based on the broader concept of the applicant’s consumption of lawful products, while two additional states protect even broader non-work-related activities. While there have been no cases applying any of these statutes to job applicants’ online social network activities, employers considering employees within these states must realize that although what they view online may be objectionable, if it is legal and not directly related

52 15 U.S.C. §§ 1681–1681x (2006). However, H.R. 321, introduced in the 112th Congress on January 19, 2011, would prohibit the use of credit background checks against employees and prospective employees, except when required by law as well as for managerial and executive positions at financial institutions.


54 Id. at § 1681m (2006 & Supp. 2010).


56 Fourteen States Now Seek Limits on Employment-Related Credit Checks, 79 U.S.L.W. 2067 (Feb. 15, 2011).


58 See infra notes 138–39 and accompanying text.


60 See id. at 641 n.87 (listing statutes protecting consumption of lawful products).

61 As discussed more fully infra, New York protects prospective applicants’ lawful consumption of products as well as legal recreational and political activities from consideration. See infra notes 147–49 and accompanying text. North Dakota prohibits prospective employers from considering applicants’ participation in lawful activities. See infra notes 150–52 and accompanying text.
to the job in question, it cannot be a factor in the decision whether to hire an applicant.

Beyond these specific restrictions, are employers free to delve into any other information about applicants that is posted on the Internet, either by the applicants themselves or by others? More specifically, what information privacy rights do job applicants have?

C. Testing the Boundaries of Information Privacy Rights on the Internet

Courts have found that, in extreme cases, employers can violate applicants’ rights to privacy in the hiring process. For example, in Soroka v. Dayton Hudson Corp., the defendant required security personnel applicants to complete a 704-question psychological test. However, the California Court of Appeals characterized some of the questions as pertaining to the applicants’ religious attitudes, as well as their sexual orientation. The Soroka court concluded that the religious and sexual orientation portions of the psychological test were not job related and therefore violated the applicants’ privacy.

As a general matter, employers are allowed, up to a point, to investigate the private lives of applicants. While the United States Supreme Court has found a constitutional privacy interest in avoiding disclosure of personal matters, that privacy interest is tempered against a government employer’s legitimate interests in managing its operations. In NASA v. Nelson, the Supreme Court assumed that government employees may have some constitutional right to informational privacy. But as Justice Scalia argued in his concurrence, the Court has always assumed, without deciding, that

---

63 Id. at 79. The defendant argued that the purpose of the test was “to screen out [security] applicants who [were] emotionally unstable, who may put customers or employees in jeopardy, or who [would] not take direction and follow [employer] procedures.” Id.
64 For example, applicants were required to answer True/False to questions such as: “Everything is turning out just like the prophets of the Bible said it would . . .” and “I believe there is a God . . . .” Id. at 79–80.
65 For example, applicants were required to answer True/False to questions such as: “I am very strongly attracted by members of my own sex . . . .” and “I like to talk about sex . . . .” Id. at 80.
66 Id. at 86 (applying CA. Const. art. I, § 1, which relates to an individual’s right to privacy). See also Phillips v. Smalley Maint. Servs., Inc., 435 So. 2d 705, 711 (Ala. 1983) (finding that employer’s repeated inquiries as to the nature of sex between employee and her husband violated the employee’s privacy).
68 Id.
69 Id. at 756.
such a privacy interest exists. 70 Regardless of whatever privacy interest someone may have in his or her private life, though, it may still be revealed through a reasonable employment background check. 71

The focus in NASA v. Nelson was on undisclosed private matters. One can certainly argue that information posted by individuals about themselves on online social network sites is not undisclosed—indeed, it may be voluntarily disclosed. 72 Courts have already expressed a disinclination to find rights to privacy in online information. As one court stated, “the concept of [I]nternet privacy is a fallacy upon which no one should rely.” 73 Internet postings are not considered private since they are often available to the general public and the right to privacy protects only that which people seek to preserve as private. 74 At present, most courts consider the right to

70 Id. at 766 (Scalia, J., concurring).
71 Id. at 763–64. Although NASA v. Nelson involved a government employer and potential constitutional rights of government employees, its standards can generally be applied to private employers. See, e.g., infra note 94. Further, according to Justice Scalia, “[a] federal constitutional right to ‘informational privacy’ does not exist.” NASA, 131 S. Ct. at 764 (Scalia, J., concurring).
72 One would naturally consider that online social network users can set their privacy settings in order to prevent unintended disclosures of personal information. But for a “generation raised with blogging, webcams, and icons of smiley faces that act as digital proxies for personal interactions, the distinction between private conversation and public disclosure has become increasingly blurred.” Rosenblum, supra note 29, at 40. Online social networking sites are the “currency of social validation and, to ensure that that currency is not counterfeit, the testimonials contained must be public . . . [and] uncensored. Indeed, the very rationale of these sites encourages exaggerated or outlandish self-expression . . . .” Id. at 42. See also Finder, supra note 22 (noting that Facebook and MySpace “have attracted millions of avid young participants, who mingle online by sharing biographical and other information, often intended to show how funny, cool or outrageous they are”). Another issue is the degree to which online social network users are allowed to keep information private. For example, Facebook is subject to an FTC complaint for forcing users to publicly disclose information that previously could be kept private. See In re Facebook II, EPIC.ORG, http://epic.org/privacy/facebook/in_re_facebook_ii.html (last visited June 25, 2011).

The Court is convinced that placing information on the information superhighway necessarily makes said matter accessible to the public, no matter how many protectionist measures may be taken . . . . [I]t strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, without taking any measures to protect the information.

privacy as binary—what is not kept secret is not considered private. 75 As individuals live more of their lives through online applications, they leave a trail of individual bits of data that can be accumulated into a near-complete picture of who they are, what they do, where they go, and with whom they associate.76 Because individual pieces of information are revealed in what is considered a “public” sphere,77 they are not afforded privacy protection.78 Nor is the accumulation of that information, even when it reveals an intimate portrait of an individual.79

Although someone posting personal information on his or her online social network profile may only intend that it be shared with a close circle of individuals, the fact that it may be viewed by a large segment of the public may render it “disclosed” and not subject to protection. But privacy rights have been recognized in information disclosed only to a few individuals.80 This raises issues such as what is the boundary between public and private—at what point does something that is private become public?81 Can there be seclusion in cyberspace?82


75 See, e.g., Leaving ‘Friendprints’: How Online Social Networks Are Redefining Privacy and Personal Security, KNOWLEDGE@WHARTON (June 10, 2009), http://knowledge.wharton.upenn.edu/article.cfm?articleid=2262; see also United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010) (stating that “prolonged GPS monitoring reveals an intimate picture of the subject’s life that he expects no one to have . . . ”); In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., No. 10-MC-0897, 2010 U.S. Dist. LEXIS 136053, at *12 (E.D.N.Y. Dec. 23, 2010) (finding a reasonable expectation of privacy in cell phone location records because they “can effectively convey details that reveal the most sensitive information about a person’s life . . . ”); Mike Elgan, ‘Pre-crime’ Comes to the HR Dept., DATAMATION (Sept. 29, 2010), http://itmanagement.earthweb.com/entdev/article.php/3905931/Pre-crime-Comes-to-the-HR-Dept.htm (discussing one particular service that searches job applicants’ social networking activities to reveal the “real” applicant).

76 See, e.g., Gill v. Hearst Publ’g Co., 253 P.2d 441, 444–45 (Cal. 1953) (holding that a couple photographed at a farmer’s market had no cause of action against the photograph’s publisher).

77 See Solove, supra note 74, at 1432–33.

78 See generally Solove, supra note 74, at 1432.

79 For example, the U.S. Supreme Court recognized a right of privacy in a private telephone conversation, even though the contents are naturally revealed to the party at the other end of the conversation. See Katz v. United States, 389 U.S. 347 (1967); see also W.A. Parent, Privacy, Morality and the Law, 12 Phil. & Pub. Aff. 269, 270 (1983) (discussing considerations of private information disclosed within a limited circle of friends, relatives, or professional associates).

80 See Lior Jacob Strailevitz, A Social Networks Theory of Privacy, 72 U. Chi. L. Rev. 919, 920 (2005). See also Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862–63 (Cal. Ct. App. 2009) (wherein a local newspaper published a student’s “ode” to the town, which she had previously published on and removed from MySpace, and the California Court of Appeal held that her expectation of privacy was lost because the potential audience was so vast, even though “[p]rivate is not equivalent to secret” and the author expected a limited audience); Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 44 (Minn. Ct. App. 2009) (holding that privacy is lost when private information is posted on a publicly accessible
Sanders v. American Broadcasting Cos.\textsuperscript{83} can provide some guidance in addressing these issues. In Sanders, an undercover reporter covertly videotaped her conversations with several coworkers.\textsuperscript{84} The California Supreme Court held that “a person who lacks a reasonable expectation of complete privacy in a conversation because it could be seen and overheard by coworkers (but not the general public) [can] nevertheless have a claim for invasion of privacy by intrusion based on a television reporter’s covert videotaping of that conversation.”\textsuperscript{85} Fundamentally, Sanders stands for the proposition that a person does not have to have an absolute or complete expectation of privacy and rejects the notion of binary privacy rights.\textsuperscript{86} According to the California Supreme Court, “[t]here are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law.”\textsuperscript{87}

California, though, appears to be the only jurisdiction that recognizes a limited right to privacy. For example, in Nader v. General Motors Corp., the Court of Appeals of New York ruled that General Motors investigators, who obtained personal information about Nader by interviewing his acquaintances, did not invade his privacy since Nader had disclosed the information to the interviewees.\textsuperscript{88} More recently, the Ninth Circuit Court of Appeals concluded that the Arizona Supreme Court would not recognize as

\begin{footnotesize}
\item[\textsuperscript{83}] 978 P.2d 67 (Cal. 1999).
\item[\textsuperscript{84}] Id. at 69.
\item[\textsuperscript{85}] Id. at 71.
\item[\textsuperscript{86}] Id. at 72.
\item[\textsuperscript{87}] Though the court did later state it was holding “only that the possibility of being overheard by coworkers does not, as a matter of law, render unreasonable an employee’s expectation that his or her interactions within a nonpublic workplace will not be videotaped in secret by a journalist.” Id. at 77.
\item[\textsuperscript{88}] 255 N.E.2d 765, 770 (N.Y. 1970). See also Myrick v. Barron, 820 So. 2d 81, 81 (Ala. 2001) (en banc) (Houston, J., concurring) (“[S]ince at least 1997, the invasion-of-privacy claim based upon wrongful intrusion in Alabama has been limited to one’s dwelling, papers, and private records.”).
\end{footnotesize}
broad an interest in limited privacy as the California Supreme Court has
done.89

Another issue raised by online social networks is the role of “place” in
privacy protection. Historically, privacy has been conceptualized as a
function of physical space and location.90 But in cyberspace, “there are no
physical spaces or clear boundaries delineating behavior and propriety.”91
In addition, as made clear in the Sanders court’s analysis, not only must
there be some degree of a reasonable expectation of privacy,92 but the
intrusion must also be highly offensive to a reasonable person.93 In the
workplace context, whether an intrusion is highly offensive is generally
related to the legitimacy of the employer’s need for the information.94

The historical nature of the right to privacy, with its emphasis on
secrecy, concealment, and space, leaves little protection to job applicants
who are revealing digital personas online. While individuals may believe
they are communicating with only a relatively small circle of friends—and
intend their communications only for that small circle—the open nature of
online social networks deprives them of meaningful rights to privacy for the
information they share. But are there other circumstances in which they
may find protection for personal information?

expectation of limited privacy in a communication . . . is reasonable only to the extent that the
communication conveys information private and personal to the declarant.” Id.
90 See Sánchez Abril, supra note 7, at 12. Sánchez Abril notes that concepts of space, subject matter,
secrecy, and seclusion have served as proxies for the legal definition of privacy. Id. at 17. See also Kyllo
v. United States, 533 U.S. 27, 37 (2001) (“In the home . . . all details are intimate details . . . .”).
91 Sánchez Abril, supra note 7, at 12.
92 See Sanders, 978 P.2d at 74–76 (reviewing cases in which there was no reasonable expectation of
privacy in the workplace, particularly because of the open nature of the workplace in question).
that while an employee may have had a reasonable expectation of privacy in personal information stored
on a company-provided computer, as a matter of law any intrusion would not be highly offensive
because the employer’s search of the computer was motivated by a desire to protect its confidential
information); Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1078, 1082 (Cal. 2009) (holding that while
the employer’s surreptitious video recording of employees in an office intruded upon their reasonable
expectation of privacy, the intrusion was not highly offensive due to the limited nature of the
surveillance and the employer’s legitimate business concerns); McLaren v. Microsoft Corp., No. 05-97-
00824-CV, 1999 Tex. App. LEXIS 4103, at *13 (Tex. Ct. App. May 28, 1999) (holding that even if the
employee could establish a reasonable expectation of privacy in e-mail messages sent across and stored
on the employer’s computer system, the employer’s interception of those messages was not highly
offensive).
Some privacy protection may be found in the Electronic Communications Privacy Act (ECPA). While, as noted above, many of the online disclosures an employer may review in the hiring process are published by the candidates themselves, the ECPA can provide privacy protection where the applicants have taken steps to restrict access to the information. Title I of the ECPA, commonly referred to as the Wiretap Act, prohibits the unauthorized interception of wire, oral, and electronic communications, while Title II, the Stored Communications Act (SCA), prohibits unauthorized access to stored wire and electronic communications and transactional records. While, as discussed below, the ECPA has been applied by a few courts to protect employee communications from unauthorized access by employers, the same principles can be applied to prospective employees as well.

One of the first challenges to interpreting and applying the ECPA in the workplace is found in Konop v. Hawaiian Airlines, Inc. Konop, a Hawaiian Airlines pilot, had restricted access to his personal website to only pre-approved individuals, mostly pilots and other employees of Hawaiian Airlines. A Hawaiian Airlines vice-president (Davis) asked for, and received access information for, Konop’s website from two pilots Konop had pre-approved, and then used that information to access and read Konop’s website. Konop argued that Davis’ conduct constituted an interception of an electronic communication in violation of the Wiretap Act. The Konop court held, however, that for a website such as Konop’s to be “intercepted” in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage (i.e., presumably not after the contents have been uploaded to and stored on the website for later reading). In contrast, the SCA protects stored electronic

---

97 Id. §§ 2701–12. The ECPA also includes a Title III, which regulates the use of pen registers and trap and trace devices. Id. §§ 3121–27. A pen register device records outgoing address or routing information regarding a communication, id. § 3127(3), while a trap and trace device records incoming address or routing information. Id. § 3127(4).
98 302 F.3d 868, 874 (9th Cir. 2002).
99 Id. at 872.
100 Id. at 873.
101 Id. at 876. 18 U.S.C. § 2511(1)(a) makes it an offense to intentionally intercept any wire, oral, or electronic communication.
102 See Konop, 302 F.3d at 878.
communications. Konop had also claimed that Davis accessed his website, a stored electronic communication, without authorization in violation of the SCA.103

While Davis did not have direct authorization from Konop to access the website, Section 2701(c)(2) of the SCA allows a person to authorize a third party’s access to an electronic communication if the person is (1) a user of the service and (2) the communication is of or intended for that user.104 The Konop court noted some indication in the legislative history that Congress believed addressees or intended recipients of electronic communications would have the authority under the SCA to allow third parties access to those communications.105 Therefore, Davis would not have violated the SCA if he gained access to Konop’s website by using information obtained from authorized users. However, the individuals from whom Davis obtained the access information had never actually used Konop’s website. The court therefore ruled they were never “users” under the language of the SCA, concluding that Davis’ access was indeed unauthorized and in violation of the SCA.106

Pietrylo v. Hillstone Restaurant Group107 is similar in facts to Konop. In Pietrylo, a supervisor “coerced” an employee to provide access information to a restricted communications area within a MySpace account in which employees were making comments critical of their employer and management; the court ruled the supervisor’s repeated access to the restricted area was unauthorized and violated the SCA.108

Can an employer request access to job candidates’ social network profiles, particularly by requiring applicants to “friend” the employer, which would grant the employer access to information that may not otherwise be publicly disclosed? The City of Bozeman, Montana, attempted to do so as part of its background check of City employee applicants. The City’s consent for a criminal background and reference check included a request for “all current personal or business websites, web pages or memberships on any Internet-based chat rooms, social clubs or forums, to include, but not limited to: Facebook, Google, Yahoo, YouTube.com, MySpace, etc.”109 The City quickly dropped the request after public

---

103 See id. at 879.
105 Konop, 302 F.3d at 880 (citing H.R. REP. NO. 99-647, at 66–67 (1986)).
106 Id. at 880.
108 Id. at *9–11.
criticisms, stating the request “appears to have exceeded that which is acceptable to our community.” More recently, it was alleged that the Maryland Division of Corrections was requiring applicants to disclose their social media account usernames and passwords. In a letter addressed to Maryland’s Department of Public Safety and Correctional Services, the American Civil Liberties Union of Maryland argued the request violated job applicants’ personal privacy rights, citing Pietrylo for the argument that such a request constitutes unauthorized access in violation of the SCA because it is a “forced authorization” due to the disparate bargaining power between an employer and employee or applicant. The Department subsequently suspended the practice and stated that requests for user names and passwords had been voluntary and had not been taken into account when evaluating job applicants. One could argue that coercing a job candidate to reveal personal information that is otherwise restricted in exchange for being considered for a job would not be an authorized nor freely-given disclosure and, hence, a possible violation of the SCA.

III. SOCIAL MEDIA AND THE EMPLOYMENT RELATIONSHIP

Businesses and employees are using social media in a number of ways that can impact the employment relationship. This Part focuses on the interrelationship between online social networks and the employment relationship, with particular emphasis on the ability of employers to fire

\[\text{man.pdf (last visited Oct. 10, 2011).} \]

\[\text{110 Matt Gouras, City Drops Request for Internet Passwords, MSNBC.COM (June 19, 2009, 8:42 PM), http://www.msnbc.msn.com/id/31446037/ns/technology_and_science-security/.} \]


\[\text{112 See supra note 108 and accompanying text.} \]


\[\text{114 Aaron C. Davis, Md. Corrections Department Suspends Facebook Policy for Prospective Hires, WASH. POST BREAKING NEWS BLOG (Feb. 22, 2011, 9:58 PM), http://www.washingtonpost.com/wp-dyn/content/article/2011/02/22/AR2011022207486.html. The Maryland Attorney General Douglas Gansler reportedly believes that requesting usernames and passwords from job applicants is legal, though current employees should not be required to do the same. Neal Augenstein, Md. AG: Requiring Employees’ Personal Passwords Is Legal, WTOP.COM (Feb. 23, 2011, 6:45 PM), http://wtop.com/?nid=46&sid=2282721. Gansler asserts that requesting access information from corrections applicants is critical to screening those applicants for gang affiliations. Id. A bill has since been introduced in the 2011 Maryland Legislative Session which would prohibit employers from requiring an employee or job applicant to disclose user names or passwords for specified Internet sites or Web-based accounts. S.B. 971, 2011 Leg., 428th Sess. (Md. 2011), available at http://mlis.state.md.us/2011sr/billfile/sb0971.htm.} \]
employees based on the content they publish online.115 This Part also addresses two additional interrelationships—the ability of employers to access employee online content through the discovery process and potential liabilities employers may face as a consequence of employee online content.

A. Firing Employees for Online Content

The online privacy rights of job applicants discussed earlier are no greater than those of employees. Under the employment-at-will doctrine, employers are generally free to terminate the employment relationship at any time, with or without cause.116 Therefore, employers who discover information about, or statements made by, current employees through their online social network activities have wide latitude in dismissing those employees. But there are some restrictions on employers.117

Section 7 of the National Labor Relations Act (NLRA) guarantees employees the right to engage in concerted activities for the purposes of mutual aid and protection.118 Fundamentally, Section 7 protects employees’

115 This Article does not specifically address employer work-related monitoring of employees. See generally Ariana R. Levinson, Carpe Diem: Privacy Protection in Employment Act, 43 AKRON L. REV. 331 (2010) (providing a comprehensive analysis of employee privacy in relation to employer monitoring).

116 See, e.g., Guz v. Bechtel Nat’l, Inc., 8 P.3d 1089, 1095 (Cal. 2000) (describing employment at will as allowing either party to terminate the employment relationship for any or no reason); Lobosco v. N.Y. Tel. Co./NYNEX, 751 N.E.2d 462, 464 (N.Y. 2001) (“Where the term of employment is for an indefinite period of time, it is presumed to be a hiring at will that may be freely terminated by either party at any time for any reason or even for no reason.”) (citation omitted). With the exception of Montana, every state in the union and the District of Columbia recognizes the employment-at-will doctrine. See Scott A. Moss, Where There’s At-Will, There Are Many Ways: Redressing the Increasing Incoherence of Employment At Will, 67 U. PITT. L. REV. 295, 299 (2005). By statute, Montana requires cause to terminate employees who have completed any probationary period. MONT. CODE ANN. § 39-2-904(1)(b) (LEXIS through 2010 Regular & Special Sess.). While there are no exact statistics reflecting how many U.S. employees are at-will, trends can be extrapolated from the number of employees working under collective bargaining agreements, as they represent the largest class of employees not considered at-will. The Department of Labor’s Bureau of Labor Statistics reports that in 2010, 14.7 million workers belonged to a union, representing 11.9% of the workforce. Economic News Release, Dep’t of Labor Bureau of Labor Statistics, Union Members Summary (Jan. 21, 2011), available at http://www.bls.gov/news.release/union2.nr0.htm. One could surmise, therefore, that a vast majority of employees are at-will.

117 There are a number of exceptions to the employment at will doctrine that are not directly discussed in this Article. For a general discussion of exceptions to the employment law doctrine, see generally Moss, supra note 116.

118 29 U.S.C. § 157 (2006). The NLRA applies to all but a few specifically excluded employers, particularly federal and state governments. See id. § 152(2). The National Labor Relations Board has adopted a rule that it will not assert jurisdiction over nonretail enterprises unless they have annual sales of at least $50,000 to firms engaged in interstate commerce. Blankenship & Assocs., Inc. v. NLRB, 999
rights to communicate amongst themselves for the purpose of improving working conditions. As such, an employee’s Facebook posting complaining about her supervisor may be a protected activity.

In December 2009, American Medical Response of Connecticut, Inc. (AMR) terminated an employee after she criticized her supervisor in a posting on her personal Facebook profile. In October 2010, the National Labor Relations Board (NLRB) filed a complaint against AMR, alleging that the employee’s termination violated her Section 7 rights. AMR’s Blogging and Internet Posting Policy prohibited employees “from making disparaging, discriminatory or defamatory comments when discussing the Company or the employee’s superiors, co-workers and/or competitors.” The NLRB alleged, in part, that AMR’s Blogging and Internet Posting Policy interfered with its employees’ Section 7 rights. In contrast, also in December 2009, the NLRB’s Office of the General Counsel issued an Advice Memorandum concluding that Sears Holdings’ Social Media Policy, which prohibited employees from disparaging the “company’s or competitors’ products, services, executive leadership, employees, strategy, and business prospects,” did not interfere with employees’ Section 7 rights. This raises the inference that the NLRB’s complaint against AMR is a retreat from its earlier advice to Sears Holding, as well as an argument that an overly broad prohibition against criticizing management online is a violation of Section 7.

Certain facts were not included in the AMR Complaint—i.e. that the employee’s negative remark about the supervisor posted on her personal Facebook page drew supportive responses from her co-workers and led to

F.2d 248, 250 (7th Cir. 1993). The NLRA’s protection for concerted activities applies not just to union employees; it applies as well to non-union (i.e., at-will) employees, particularly because they lack any form of designated bargaining representative. Citizens Inv. Servs. Corp. v. NLRB, 430 F.3d 1195, 1197 (D.C. Cir. 2005).

See, e.g., Citizens, 430 F.3d at 1197 (finding the employer had violated a financial consultant employee’s Section 7 rights by dismissing him after he had voiced complaints on behalf of himself and other consultants regarding a new commission payment structure); Valley Hosp. Med. Ctr., Inc., 351 N.L.R.B. 1250, 1252 (2007). Section 7 rights are enforced through 29 U.S.C. § 158(a)(1) (2006), which makes it an unfair labor practice for an employer “to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in [S]ection 7.” See Citizens, 430 F.3d at 1197.


Id. at para. 7.

Id. at para. 16.


further negative comments about the supervisor from the employee. The NLRB’s Press Release also specified that particular provisions of AMR’s Blogging and Internet Posting Policy “contained unlawful provisions, including one that prohibited employees from making disparaging remarks when discussing the company or supervisors and another that prohibited employees from depicting the company in any way over the internet without company permission.” In contrast, the NLRB’s Office of the General Counsel concluded Sears Holdings’ Social Media Policy did not interfere with Section 7 rights because it contained “sufficient examples and explanation of purpose for a reasonable employee to understand that it prohibits the online sharing of confidential intellectual property or egregiously inappropriate language and not Section 7 protected complaints about the Employer or working conditions[.]” and because the Policy was not implemented in response to protected activities.

The AMR Complaint does appear to represent a shift in attitude towards social media policies and concerted activities. The challenged prohibitions in AMR’s and Sears Holding’s policies are nearly identical—in concept, if not exact wording. And while the NLRB’s Office of the General Counsel warned against interpreting portions of policies in isolation, that is fundamentally the approach taken in the AMR Complaint. A substantial focus in the AMR case was the company’s Blogging and Internet Posting Policy. In settling the case, the NLRB noted that AMR had “agreed to revise its overly-broad rules to ensure that they do not improperly restrict employees from discussing their wages, hours and working conditions with co-workers and others while not at work, and that they would not discipline or discharge employees for engaging in such discussions.” The AMR Complaint and subsequent settlement imply that the NLRB will consider not just whether a social media policy is used to suppress Section 7

---

126 Id.
128 Id. at 5. See, e.g., Cintas Corp. v. NLRB, 482 F.3d 463, 471 (D.C. Cir. 2007) (Henderson, C.J., concurring) (noting that the company’s confidentiality provision’s restriction on disclosing employee information must be read in light of its associated references to legitimately protected business information”).
129 News Release, NLRB, Settlement Reached in Case Involving Discharge for Facebook Comments (Feb. 8, 2011) (emphasis added), available at http://www.nlrb.gov/news/settlement-reached-case-involving-discharge-facebook-comments. “The company also promised that employee requests for union representation will not be denied in the future and that employees will not be threatened with discipline for requesting union representation.” Id.
rights, but also whether the existence of an overly-broad social media policy in and of itself can interfere with Section 7 rights.\footnote{See, e.g., Guard Publ’g Co. v. NLRB, 571 F.3d 53, 58 (D.C. Cir. 2009) (reiterating that a valid no-solicitation rule applied in a discriminatory manner or maintained for discriminatory reasons may not be enforced against union solicitation). In \textit{Guard Publishing Co.}, the company’s communications systems policy prohibited use of the e-mail system for non-job-related solicitations, yet one employee was disciplined after sending a union-related message while other employees who had sent non-job-related solicitations were not disciplined. \textit{Id}.}

Just as an employer may not use an otherwise valid communications policy in a discriminatory manner to suppress Section 7 activities,\footnote{Guard Publ’g Co., 571 F.3d at 58.} it cannot also use it to discriminate against a protected class under Title VII. For example, when an employee was terminated after sending e-mail messages containing “sexually suggestive and otherwise inappropriate jokes or picture attachments” in violation of the employer’s Information Security and Sexual Harassment policies, the employee brought a claim against the employer for discrimination.\footnote{Williams v. Wells Fargo Fin. Acceptance, 564 F. Supp. 2d 441, 443 (E.D. Penn. 2008).} The district court denied the employer’s motion for summary judgment, holding that the former employee had established a \textit{prima facie} case of racial discrimination by introducing sufficient evidence from which a jury could reasonably infer the employer

---

\footnote{See, e.g., Martin Luther Mem’l Home, Inc., 343 N.L.R.B. 646, 647 (2004) (stating that a workplace rule “can be unlawful if employees would reasonably read it to prohibit Section 7 activity”) (cited with approval by Int’l Union, U.A.W. v. NLRB, 520 F.3d 192, 197 (2d Cir. 2008)). The AMR complaint will most likely not be the last word on this issue. On May 9, 2011, the NLRB filed a complaint against Hispanics United of Buffalo, a nonprofit that provides social services to low-income clients, after the nonprofit fired five employees who had criticized another employee through Facebook communications. News Release, NLRB, Complaint Issued Against New York Nonprofit for Unlawfully Discharging Employees Following Facebook Posts (May 18, 2011), \url{http://nlrb.gov/news/complaint-issued-against-new-york-nonprofit-unlawfully-discharging-employees-following-facebook}. The NLRB complaint alleged Hispanics United unlawfully discharged the employees in violation of Section 7 because the Facebook postings “involved a conversation among coworkers about their terms and conditions of employment, including their job performance and staffing levels.” \textit{Id}. It has also been reported that the NLRB is considering filing a Section 7 complaint against Thomson Reuters after it allegedly disciplined an employee who sent a Twitter message criticizing management. See Steven Greenhouse, \textit{Labor Panel to Press Reuters over Reaction to Twitter Post}, \textit{N.Y. TIMES}, Apr. 7, 2011, at B3. The NLRB’s Office of the General Counsel has issued a memo which includes a requirement that regional offices addressing complaints involving employers’ social media policies must seek advice from the NLRB’s Division of Advice before taking any action. See Memorandum from NLRB Office of Gen. Counsel, A.9. (Apr. 12, 2011), \url{http://www.laborrelationsupdate.com/GC%20Memorandum%202011-11.pdf}. On August 18, 2011, the NLRB’s Acting General Counsel issued a report discussing recent cases involving social media in the workplace wherein the General Counsel’s office provides its reasoning in determining whether employees were engaged in protected concerted activities in certain cases when using social media, as well as the office’s position regarding social media policies. Memorandum OM 11-74 from NLRB Office of Gen. Counsel (Aug. 18, 2011), \url{http://mynlrb.nlrb.gov/link/document.aspx/09031d458056e743}.}
selectively enforced its policies. In particular, Williams, an African-American, was terminated as a result of his prohibited conduct, while it was commonplace for all employees to send personal e-mails through the company’s system during work hours, including messages with sexual or pornographic content, and receive only counseling or warnings. The court concluded that a jury “could reasonably infer that the defendant [employer] selectively enforced its email policies and used the most severe discipline available because it would result in the termination of a disproportionate number of African-American employees.”

There are also selected state statutes which prohibit employers from taking adverse employment actions based on employees’ and prospective employees’ off-premises conduct during nonworking hours. Initially, the focus of a majority of these state statutes was to protect employees’ and prospective employees’ rights to use tobacco. However, some statutes are a bit broader, preventing employers from discriminating against employees and prospective employees based on their consumption of lawful products off the premises during nonworking hours. Four states—California, Colorado, New York, and North Dakota—have even broader statutes, prohibiting adverse employment actions based on lawful activities off the premises during nonworking hours.

California’s statute, on its face, appears to be the most expansive, addressing “loss of wages as the result of demotion, suspension, or discharge from employment for lawful conduct occurring during nonworking hours away from the employer’s premises.” However, California’s statute is merely procedural—assigning claims by employees to the Labor Commissioner; it does not provide employees any substantive rights. And while the statute makes no reference to employer interests,
legitimate employer interests can still justify a dismissal even when 
employees are engaged in lawful activities, such as dating.\textsuperscript{142} 

Colorado’s statute prohibits employers from terminating the 
employment of any employee “due to that employee’s engaging in any 
lawful activity off the premises of the employer during nonworking 
hours . . . ”\textsuperscript{143} The statute does not apply to activities related to a bona fide 
occupational requirement, reasonably and rationally related to the 
employment activities, or which create a conflict of interest.\textsuperscript{144} While the 
Colorado Court of Appeals has held the statute applies to lawful, off-duty 
conduct, whether or not work-related,\textsuperscript{145} the Colorado District Court has 
ruled that an employee’s public letter criticizing management is a breach of 
loyalty, which falls within the exceptions provided in the statute.\textsuperscript{146} 

While New York’s statute specifies protections for employees’ and 
prospective employees’ lawful consumption of products during nonworking 
hours while off the employer’s premises, it also protects against legal 
recreational activities, as well as political activities during nonworking 
hours while off the employer’s premises.\textsuperscript{147} Similar to Colorado, the New 
York statute does not apply to any activity which “creates a material 
conflict of interest related to the employer’s trade secrets, proprietary 
information or other proprietary or business interest.”\textsuperscript{148} The majority of 
cases brought so far under the New York statute involve terminations 
arising from romantic relationships, in which the courts have concluded that 
“dating” is not a recreational activity protected under the statute.\textsuperscript{149} 

North Dakota’s statute prohibits discrimination on the basis, in part, of 
“participation in lawful activity off the employer’s premises during 
nonworking hours which is not in direct conflict with the essential business- 
related interests of the employer.”\textsuperscript{150} North Dakota’s lawful activities 
provision was initially enacted to “expand the law prohibiting employment 

\textsuperscript{142} Id. at 411 (recognizing that employers have legitimate interests in avoiding conflicts of interest 
between work-related and family-related obligations).

\textsuperscript{143} COLO. REV. STAT. § 24-34-402.5(1) (LEXIS through 2010 Legis. Sess.). Colorado’s statute also 
only applies to employees.

\textsuperscript{144} Id. at §§ 24-34-402.5(1)(a)–(b).

claim by an employee that she was terminated after making a complaint during nonworking hours while 
off the employer’s premises to the Occupational Safety and Health Administration).

\textsuperscript{146} Marsh v. Delta Air Lines, Inc., 952 F. Supp. 1458, 1463 (D. Colo. 1997) (applying § 24-34- 
402.5(1)(a)).

\textsuperscript{147} N.Y. LAB. LAW § 201-d (LEXIS through 2011 Released Chapters).

\textsuperscript{148} Id. § 201-d(3)(a).

\textsuperscript{149} See, e.g., McCavit v. Swiss Reinsurance Am. Corp., 237 F.3d 166, 167 (2d Cir. 2001); Hudson v. 

\textsuperscript{150} N.D. CENT. CODE § 14-02.4-01 (LEXIS through 2011 Legis. Sess.).
discrimination and preclude employers from inquiring into an employee’s non-work conduct, including an employee’s weight and smoking, marital, or sexual habits.” The North Dakota legislature subsequently amended the lawful activities language to activity “‘which is not in direct conflict with the essential business-related interests of the employer’” to clarify possible conflicts between the protected status of lawful activity off the employer’s premises and the employment-at-will doctrine,” in order to “provide an employer with some assurance that the employee’s conduct is not deleterious to the well-being of the employer’s mission.”

While these lawful consumption and lawful activity statutes, on their face, appear to restrict employers’ abilities to take actions against employees based on off-duty, off-premises conduct, for the most part, they permit employers wide latitude as long as, similar to general employee privacy concerns, employers can demonstrate a legitimate business interest in their decision. In addition, to date, there has not been a published court decision applying any of these statutes to employee online social network activities.

B. Using Discovery to Access Employee Online Social Network Communications

Another emerging area involving employee use of social network sites involves workers’ compensation claims. For example, Alexis Muniz had testified before a workers’ compensation board that she was unemployed while receiving workers’ compensation benefits for a job-related injury while working for a previous employer. Muniz was subsequently arrested and convicted of fraud after investigators discovered a posting on her Facebook page where she boasted about her salary and job as an apartment complex manager.

152 Id. (citations omitted). It should also be noted that Connecticut prohibits employers from disciplining or discharging employees resulting from their exercise of their First Amendment rights or certain rights under the Connecticut state constitution (right of religious liberty, liberty of speech and the press, and right to assemble and petition), provided “such activity does not substantially or materially interfere with the employee’s bona fide job performance or the working relationship between the employee and the employer.” CONN. GEN. STAT. § 31-51q (LEXIS through 2010 Legis. & 2011 Supp.).
153 Workers’ compensation laws are state-based no-fault systems designed to provide employees with compensation for job-related injuries through an efficient mechanism for claims resolution. Jaclyn S. Millner & Gregory M. Duhl, Social Networking and Workers’ Compensation Law at the Crossroads, 31 PACE L. REV. 1, 3 (2011).
155 Id.
Fundamentally, employers can use any publicly-available, employee-created social network information as long as it is relevant to a workers’ compensation claim, as well as other employee-plaintiff litigation. Employers can obtain evidence informally by just searching the Internet for information posted by the employee in question, as such information would be publicly available. It is also possible for employers to obtain even more information by requesting username and password information through formal discovery. As long as it is relevant to the litigation, whether directly or peripherally, a party may obtain discovery regarding any unprivileged matter.

While, as noted earlier, courts have recognized some online privacy rights through the Stored Communications Act when employees take efforts to limit access to posted information, these concerns do not necessarily apply to discovery requests. At least one court has held that since it is understood that social network site operators can view and disclose posted information, that information cannot be considered confidential. Since most social network communications are based on friendships and social relationships, not attorney-client, physician-patient, or psychologist-patient types of relationships, they cannot be considered privileged.

Even when communications are based on an attorney-client relationship, an employee may waive any privilege by using the employer’s

---

156 See generally, Millner & Duhl, supra note 153, at 10–11.
157 See, e.g., Romano v. Steelcase, Inc., 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010). In Romano, the plaintiff claimed her injuries were the fault of the defendant, and that due to those injuries she was confined to her house and bed. Id. at 654. The Romano court granted the defendant’s request for access to the plaintiff’s private postings on Facebook and MySpace after the defendant observed that the plaintiff’s public profile page on Facebook revealed she had an active lifestyle and had traveled to Florida and Pennsylvania during the time period she claimed that her injuries prohibited such activity. Id. at 653–54. The court characterized privacy as a reasonable expectation in the age of online social networks as “wishful thinking.” Id. at 657.
158 See id. at 656–57.
160 See supra notes 106 & 108 and accompanying text.
162 Id. at *10.
communications system. For example, in *Holmes v. Petrovich Development Co.*, the employee used her employer’s e-mail system to communicate with her attorney regarding a possible sexual harassment action against the employer.  

The *Holmes* court concluded that because the employee had been notified through the employer’s policies that all e-mail messages could be monitored and that they were not private, any privilege was lost, stating that it was akin to the employee consulting her attorney in one of the employer’s conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by the employer would be privileged.  

Similarly, in *Lenz v. Universal Music Corp.*, the plaintiff’s communications became subject to discovery as a result of her blog postings, e-mail messages with family, and electronic chats with friends regarding her conversations with counsel.

### C. Employer Liability for Employee-Created Content

Employers must also be aware of company-related materials employees publish online. Through Section 5 of the Federal Trade Commission Act (FTCA), the Federal Trade Commission (FTC) is authorized to challenge unfair or deceptive acts or practices.  

To establish liability under Section 5 of the FTCA, the FTC must establish that (1) there was a representation; (2) the representation was likely to mislead customers acting reasonably under the circumstances, and (3) the representation was material.

Statements posted online by individuals praising a company’s products or services can generally be considered to be endorsements.  

The FTC defines an endorsement as an advertising message that “consumers are likely to believe reflects the opinions, beliefs, findings, or experience of a party other than the sponsoring advertiser.” If there is a connection between the endorser and the sponsor that may materially affect the weight or credibility of the endorsement, then the connection must be disclosed.  

Consumers naturally consider comments by an independent consumer as more credible than from someone who receives some form of

---

164 *Id.* at 896. *But see* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010) (holding that an employee had a privacy interest in e-mail correspondence with her attorney stored on a web-based third party service provider).
168 16 C.F.R. § 255.0(b) (2009).
169 *Id.* § 255.5.
compensation or benefit, whether direct or indirect, from the seller of the product or service. Failing to disclose a connection between an endorser and sponsor can be deceptive. For example:

An online message board designated for discussions of new music download technology is frequented by MP3 player enthusiasts. They exchange information about new products, utilities, and the functionality of numerous playback devices. Unbeknownst to the message board community, an employee of a leading playback device manufacturer has been posting messages on the discussion board promoting the manufacturer’s product. Knowledge of this poster’s employment likely would affect the weight or credibility of her endorsement. Therefore, the poster should clearly and conspicuously disclose her relationship to the manufacturer to members and readers of the message board.\(^{170}\)

To date, enforcement actions have involved fairly blatant misrepresentations of the connection between the sponsor and the endorser. For example, in 2010, the FTC settled charges with a public relations agency hired by video game developers that engaged in deceptive advertising by having employees pose as ordinary consumers posting game reviews at the online iTunes store and not disclosing that the reviews came from paid employees working on behalf of the developers.\(^{171}\) Statements published on social networks by employees promoting the products or services of their employers can be considered endorsements, even if the employees are not directed by the employer to publish such statements. There are two levels of liability associated with product or service endorsements—the employer-sponsor is subject to liability for: (1) false or unsubstantiated statements made through endorsements; and (2) failing to disclose material connections made through endorsements; and (2) failing to disclose material connections between itself and its endorsers.\(^{172}\) As such,

\(^{170}\) Id. at Ex. 8.


\(^{172}\) 16 C.F.R. § 255.1(d) (2011).
employers must ensure that if employees are making endorsements—even voluntarily—the endorsements are accurate and there is disclosure that the authors of the endorsements are employees of the sponsor.

Employers can face other types of potential liability arising from employee-generated online communications. As a general matter, employers should not allow social network sites to be used to display and communicate objectionable material throughout the workplace. An employee may establish a violation of Title VII of the Civil Rights Act by proving that discrimination based on sex has created a hostile or abusive work environment.173 Whether a work environment is “hostile” or “abusive” can be determined only by looking at all the circumstances, including: “the frequency of the discriminatory conduct; its severity; whether it is physically threatening or humiliating, or a mere offensive utterance; and whether it unreasonably interferes with an employee’s work performance.”174 The vast majority of cases addressing hostile work environments involving electronic communications, especially e-mail, have found only isolated events that did not give rise to a hostile or abusive environment—e.g., a single offensive e-mail message;175 viewing twelve allegedly obscene e-mail messages over a period of seventeen months received by a supervisor that were not addressed to the plaintiff;176 a barrage of offensive e-mail messages addressed to the plaintiff sent over a three week period;177 and catching a glimpse of nude bodies on computer screens three to five times.178 However, in Coniglio v. City of Berwyn, a district court denied the employer’s motion for summary judgment for an employee’s claim that a hostile environment was created by a supervisor repeatedly viewing pornography on his computer monitor, which was only twelve feet from the employee’s desk and could be seen through a glass partition.179 And in Blakey v. Continental Airlines, Inc., the Supreme Court of New Jersey recognized that an employer could be liable for a hostile

work environment created by employees through an electronic bulletin board system not directly maintained by the employer.\textsuperscript{180}

As a general matter, employers will not be liable for purely personal social network communications published by employees,\textsuperscript{181} even when using the employer’s computer system.\textsuperscript{182} However, at least one court has found an employer potentially liable for an employee’s conduct through the workplace computer system. In \textit{Doe v. XYC Corp.},\textsuperscript{183} computer technicians and supervisors were aware that an employee was using the employer’s computer system to visit pornographic web sites while at work, but took no action due to the employer’s policy to not monitor the Internet activities of its employees.\textsuperscript{184} The employee’s wife sued the employer on behalf of her ten-year-old daughter, “Jill Doe,” after the employee “transmitted three . . . clandestinely-taken photos of Jill Doe over the Internet from his workplace computer to a child porn site in order to gain access to the site.”\textsuperscript{185} In reversing the lower court’s granting of the employer’s motion for summary judgment, the New Jersey Superior Court held:

\begin{quote}
[A]n employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee’s activities and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third-parties. No privacy interest of the employee stands in the way of this duty on the part of the employer.\textsuperscript{186}
\end{quote}

\textsuperscript{180} 751 A.2d 538, 549 (N.J. 2000) (noting that harassment by a supervisor that takes place outside of the workplace can be actionable because the conduct arises out of the employment relationship and can permeate the workplace).

\textsuperscript{181} See \textit{Tomka v. Seiler Corp.}, 66 F.3d 1295, 1317 (2d Cir. 1995) (“[A]n employer is not liable for torts committed by the employee for personal motives unrelated to the furtherance of the employer’s business.”) (citation omitted).

\textsuperscript{182} See, e.g., \textit{Booker v. GTE.net LLC}, 350 F.3d 515, 519 (6th Cir. 2003) (holding that the employer was not vicariously liable for a highly offensive e-mail message sent through a third-party provider by an employee through the employer’s computer system where the messages did not advance the interests of the employer); \textit{Delfino v. Agilent Tech., Inc.}, 52 Cal. Rptr. 3d 376, 396 (Cal. Ct. App. 2006) (holding that the employer was not liable for threatening e-mail messages and Internet posting sent by an employee using the employer’s computer system because the messages were sent “out of personal malice, not engendered by the employment”) (citation omitted).


\textsuperscript{184} Id. at 1158–60.

\textsuperscript{185} Id. at 1160. The employee also later acknowledged that he stored child pornography (over 1,000 images), including nude photos of Jill Doe, in his workplace computer. Id.

\textsuperscript{186} Id. at 1158.
Doe’s holding presents a strong argument that employers cannot turn a blind eye to what employees are doing online, at least while they are in the workplace.

IV. CONCLUDING ANALYSIS AND BEST PRACTICES RECOMMENDATIONS

Employers can avoid some of the legal minefields presented by online social networks by adopting certain best practices:

When vetting job applicants online, limit inquiries to publicly-available information and consider only information that relates to legitimate business needs.

NASA v. Nelson and the majority of informational privacy cases indicate that employers are free to inquire into the backgrounds of job applicants as long as there is a legitimate business need for the information. Information disclosed to the public, as well as to third parties, is not currently considered private. But privacy is based on societal norms. As more and more individuals interact socially through online social networks, courts may begin to recognize a more nuanced zone of privacy—that what may be intended for a limited audience only may be subject to a right to privacy. To paraphrase the California Supreme Court and extend limited privacy expectations from media disclosure to cyberspace, society is beginning to develop new degrees and nuances of expectations of privacy—“the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law.”

When vetting job applicants online, know the legal limitations.

Courts are beginning to separate password-protected communications sent through personal accounts with other forms of online communications. The Stored Communications Act prohibits unauthorized

---

188 Katz v. United States, 389 U.S. 347, 361 (1967) (Douglas, J., concurring) (stating that a person’s reasonable expectation of privacy must be one that society is willing to recognize as reasonable).
190 See, e.g., Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) (holding that an employee had a reasonable expectation of privacy in personal e-mail messages stored on a third party’s service, although the employee had accessed that outside service while at work, using employer-provided equipment); Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010) (holding that an employee had a privacy interest in e-mail messages stored on a web-
access to stored electronic communications. Circumventing protections or coercing access to protected areas will, in all likelihood, result in an Stored Communications Act violation. The two publicized incidents in which employers have requested social network access information from job applicants have resulted in quick reversals by the employers due to adverse publicity. Clearly, the public considers being required to turn over usernames and passwords in order to be considered for a job a violation of personal privacy.

By searching job candidates’ online social network postings, potential employers can easily learn information that they may otherwise be prohibited from requiring from applicants, especially related to protected class characteristics. Social network searches should be conducted by someone who will not be making the hiring decision so that protected class characteristics that may be discovered can be removed from any information considered by the decision maker.

*Think twice before firing employees due to their online postings.*

Section 7 of the National Labor Relations Board protects employees’, union as well as at-will, right to engage in concerted activities—to communicate amongst themselves for the purpose of improving working conditions. When an employee “gripes” online about a supervisor or overall working conditions, that will probably be concerted activity if other employees participate.

In addition, seven states protect employees from adverse employment actions based on their consumption of lawful products off the premises during non-working hours, and another four states offer the same protection for employees’ lawful activities. These statutes do allow an employer to take action, however, if the consumption or activities have a direct bearing on the employer’s legitimate interests. As such, if employers do learn through online social networks of what they consider to be objectionable conduct by their employees, they should ensure there is a legitimate business interest at stake before taking any action.

---

191 See supra notes 106 & 108 and accompanying text.
Regulate and monitor employees’ work-related online conduct, but not too much.

Formerly, a workplace policy prohibiting employees from using the Internet to criticize the firm, its managers and executives, and its customers was permissible as long as it was not enforced in a way that infringed on employees’ Section 7 right to concerted activities. With the 2011 American Medical Response of Connecticut, Inc. settlement, however, the National Labor Relations Board has clearly signaled that if such a policy merely has the potential to infringe on Section 7 rights, it violates the National Labor Relations Act. The safest course for companies, while requesting that employees maintain civility in their online postings and not criticize customers, is to not prohibit criticism of the firm or its supervisor or executives.

The courts have indicated a clear bias against any form of employee right to privacy in electronic communications transmitted through the employer’s computer and communications systems. This is true even when the employee engaged in what would otherwise be privileged communications with her attorney.192 Courts have, however, drawn the line when employers have accessed password-protected messages stored on private e-mail accounts maintained by employees—even when employees have accessed those accounts using the employer’s systems.193

Employers also need to be aware of what their employees post online, particularly if those publications relate to the employers’ products or services. Any time an employee promotes the employer’s products or services, not only must the endorsement be accurate, but it also must contain a disclosure of the employee’s connection to the employer. And while the majority of cases that have considered objectionable communications by employees through employers’ computer systems have either found the conduct was not severe enough to create a hostile environment or was so personal to be outside the scope of employment, Doe v. XYC Corp. serves as a warning that employers cannot turn a blind eye to their employees’ online activities.194

---

192 See supra notes 163–64 and accompanying text.
193 See supra note 190.
194 See supra notes 183–86 and accompanying text.
Regulate and monitor employees’ work-related online conduct, with clear prior notice to your employees.

An employee’s awareness that the employer is capable of monitoring the employee’s communications is alone not enough to imply consent to monitoring.195 However, when the employee acknowledges receiving an employee manual which states, in part, that “electronic mail messages sent and received on Company equipment are not private and are subject to viewing, downloading . . . and archiving by Company officials at all times,” and the manual defines electronic mail messages as including “personal/private/instant messaging systems,” then the employee is on actual notice and has no complaint when his messages are reviewed by management.196

Regulate and monitor employees’ work-related online conduct, and take consistent action when necessary.

When objectionable, particularly potentially harassing, content is posted online, prompt, remedial action by the employer is imperative to reduce, if not eliminate, potential liability. For example, if an employee posts objectionable content on his Facebook profile, promptly instructing the IT department to block access to that Facebook page from workplace computers could be considered adequately remedial.197 But the employer’s actions must be consistent. Selectively enforcing its policies could raise the specter of illegal discrimination.198

V. CONCLUSION

Online social networking is becoming more ingrained into the personal lives of individuals, as well as being adopted as a communications tool by businesses. As the use of online social networks matures, so should their associated legal issues. Employers will need to maintain vigilance as the online social network landscape evolves and the legal system adjusts to its presence in the workplace.

195 See, e.g., Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992).