Social Media, Privacy, and the Employment Relationship: The American Experience

Ariana R. Levinson*
Associate Professor of Law
Louis D. Brandeis School of Law
University of Louisville

Received: 16 August 2013 / Accepted: 1 October 2013

Abstract: This article posits that privacy issues arising in the United States from the use of social media and the employment relationship are similar to those that have arisen around the world. It suggests, however, that the patchwork of governing legal claims arising under different laws in different jurisdictions may be unique. After a brief introduction, the second section describes the recent passage of legislation in several states that may protect the privacy of job applicants' passwords to social-media sites. The third section describes the various claims employees may bring under the federal Electronic Communications Privacy Act, in tort for invasion of privacy, pursuant to the Fourth Amendment, or to enforce just cause provisions in collective bargaining agreements. The fourth section describes protection from overbroad discovery of social media when employers and former employees are involved in litigation. The article concludes by assessing the likelihood of further legal reform.

Keywords: social media, social networking, privacy, employment, electronic communications, hiring, discovery

1. Introduction

Electronic communications by employees and employer monitoring of those communications raise issues for both employers and employees. The problems created by social media as it relates to the employment relationship are a subset of these issues. Moreover, the issues facing employers and employees as a result of advancing technology are similar in the United States and around the globe. Boundaries between home and office have become blurred. Employees often socialize, including with those outside the workplace, perform personal tasks at work, and work during their off hours, including while at home. Employers express concern that employees are not working enough, or, worse, are engaging in inappropriate or unlawful behavior while they are on the clock. They worry that workers, even while at home, may be sharing confidential information or disparaging the employer in a public forum. On the other hand, employees are concerned that employers may abuse their technological ability to monitor the activities of their workers.

What may be unique about the experience in the United States is that, unlike some other countries, the United States has no comprehensive regulations governing the employment relationship. Laws differ depending upon, among other things, the type of claim involved, the state in which the work takes place, whether the work is performed for the government or a private employer, and whether the workforce is

*The author thanks Lauren Claycomb and Sharon Wright for research assistance, and Philip Heleringer, as well as two anonymous external reviewers, for editorial assistance. All views are solely those of the author, as are all errors.

unionized. Likewise, there exists no truly comprehensive scheme that regulates electronic communication or the protection of personal data.

Because so much depends upon the nature of the claim, the jurisdiction, and the particular circumstances, no generalized rules apply to every case. However, some predictive considerations emerge from a review of the cases decided to date. Protection is unlikely when the communication is with the public, or a large group of people. Protection is more likely when the communication is with a limited set of people and even more likely when with just one individual. Regardless of the number of people involved, however, social-media privacy protection is more likely when the social-media account is password protected. Privacy in social media is less likely to be protected when the media is used at work, and even less likely when on employer equipment. In particular, if the employer has notified the employee that it will monitor the social-media use, privacy is unlikely to be protected at all.

This article explores the various laws that come into play to protect employee privacy when an employee communicates via social media and an employer seeks to monitor or discover that activity. The article focuses on protection of privacy rather than the host of other related issues raised by the use of social media and the employment relationship. Among these other issues are the extent of the right to use social media to engage in advocating for a change in working conditions (Robert Sprague, 2012), the applicability of anti-discrimination laws in hiring screens (Nicolas P. Terry, 2012) and in online worlds, the right to free speech online (Mary-Rose Papandrea, 2012), the ways in which employers who are harmed by employee use of social media can be compensated, and, generally, whether and how employment rules apply to those working via avatar on social media sites such as Second Life (Alek Felstiner, 2012).

The article focuses on three broad topics regarding social media and privacy in the employment relationship. First is the issue of whether a potential employer can access a job applicant's social-media profile for use in making a hiring decision. Second is the issue of whether an employer can monitor a current employee's social media use, whether at work or not. Third is the issue of whether an employer can access a prior employee's social-media account, a question that generally arises within the context of a lawsuit.

2. Hiring

Social media provides an easy and inexpensive way for employers to gather information about job applicants to see if they will fit well in the workplace or do a good job. Employers also sometimes use social media to gather information about current employees, including those who are on disability leave, those who have filed workers' compensation claims, or those who have simply reported late to work. Employer monitoring of social-media use is nothing new (Nicolas P. Terry, 2012). However, a series of recent, highly publicized cases involving employer requests for social-media passwords led a number of states to enact legislation regulating the practice. In Maryland, the state Department of Public Safety and Correctional Services asked job applicants and employees returning from leave to provide their social-media passwords. The American Civil Liberties Union objected, and pressured the employer to cease asking potential hires and returning employees for passwords.

Maryland, Illinois, and California became the first three states to pass legislation prohibiting employer requests for social-media passwords. Nine states have since passed similar legislation, and legislation is currently pending in seventeen other states.[1] Two bills have been introduced at the federal

[1] On December 28, 2012, Michigan became the fourth state to pass such legislation. 2012 Mich. Pub. Acts 478, H.B. 5523 substitute, *available at* http://www.legislature.mi.gov/documents/2011-2012/publicact/pdf/2012-PA-0478.pdf; *Cyberlaw—Socialmedia: Michigan Employers May Not Ask for Passwords*, 81 U.S.L.W. 981, 2013 WL 68443 (Jan. 8, 2013). In 2013, Arkansas, Colorado, New Mexico, Nevada, Oregon, Utah, Vermont, and Washington passed statutes. As of July 2013, legislation remains pending in Georgia, Hawaii, Iowa, Kansas, Maine, Massachusetts, Minnesota, Missouri, Nebraska, New Hampshire, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Rhode Island, and Wisconsin. National Conference of State Legislatures, *Employer Access to Social Media Usernames and Passwords 2013*, NCSL.org, http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx (last updated July 31, 2013).

level during the current congressional term, although they are not likely to pass.[2] In the United States, a social-media site might also bring a breach-of-contract claim against a user—including an employer—who uses the site in an unauthorized manner. For instance, Facebook reacted to employer requests for applicants' passwords by clarifying that Facebook's Statement of Rights and Responsibilities prohibits soliciting a Facebook password. Facebook released a privacy statement emphasizing that it would take appropriate action against employers who violate the Statement, including shutting down the employer's Facebook account or initiating legal action.[3]

Other federal acts do not bear directly on privacy, but warrant brief mention. Federal anti-discrimination laws provide some measure of protection for at-will employees by prohibiting discrimination on bases including race, sex, disability, and age. To avoid liability, an employer who uses Facebook to screen potential hires, whether looking at public or private information, should have someone other than the person making the hiring decision conduct the initial screen and delete any data pertaining to protected characteristics.

The following sub-sections focus on the first three state laws that were passed in order to assess the extent to which different state laws protect the privacy of applicant and employee passwords. The review of the statutes discloses that the details of the text matter. Pertinent issues include the following: 1) Will these laws be equally effective in protecting applicants and employees from viewing of social media sites by employers? 2) Will some be more likely to reinforce an employer's ability to monitor because of the inclusion of broad exceptions? 3) Are the statutes equally effective in providing an enforcement mechanism or is a method of enforcement lacking? 4) Are remedies provided, and, if so, are they sufficient?

a. Viewing Social Media

The state laws differ as to whether they only prohibit acquiring the means to access a social media site, such as a password, or also prohibit viewing of a social media site. The Maryland statute defines "electronic communications device" broadly,[4] and the operative section states that "an employer may not request or require that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device."[5] Thus, the blog of a well-known, management-side employment firm noted that, subject, of course, to judicial interpretation, the law may not prohibit an employer from asking to view or obtain a print copy of an employee's social-media profile, as long as the employer does not ask for the employee's password or other protected means for accessing a protected account (Philip L. Gordon, 2012).[6]

---

[2] Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013), *available at* http://op.bna.com/tpif.nsf/id/mlon-94nrgd/$File/Social%20Networking%20Online%20Protection%20Act.pdf; Password Protection Act, H.R. 2077, 113th Cong. (2013), *available at* http://www.govtrack.us/congress/bills/113/hr2077.

[3] *Protecting Your Passwords and Your Privacy*, Facebook (Mar. 32, 2012, 5:32 AM), www.facebook.com/note.php?note_id=326598317390057.

[4] MD. Code Ann., Labor and Employment § 3-712 (West 2012) (effective Oct. 1, 2012).

(a)(3)(i) "Electronic communications device" means any device that uses electronic signals to create, transmit, and receive information.

(a)(3)(ii) "Electronic communications device" includes computers, telephones, personal digital assistants, and other similar devices.

[5] *Id.*

(b)(1) Subject to paragraph (2) of this subsection, an employer may not request or require that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device.

[6] As Philip L. Gordon states:

Passwords To Devices: While the Maryland law bars employers from requesting log-in credentials for "accessing a personal account or service," the law does not prohibit employers from requesting or requiring log-in credentials to access an employee's personal device, such as a smartphone or tablet. This distinction is critical as employers increasingly are implementing "Bring-Your-Own-Device" policies.

...

Because the Act's restrictions on its face arguably apply only to the disclosure of log-in credentials, it remains to be seen through judicial interpretation whether the Act's restrictions bar an employer from, for example, asking an employee or applicant

In contrast, the prohibition contained in the Illinois statute broadly bars viewing of social media sites by employers. The Illinois law was an amendment to a statute already in effect that prohibits employers from asking applicants about workers' compensation or safety claims. The law is more targeted toward social media than the Maryland law. Rather than using a broad definition of "electronic communication device" like the Maryland statute, the Illinois statute pertains only to an "employee's account or profile on a social networking website."[7] The Illinois law, in contrast to that of Maryland, however, clearly prohibits an employer obtaining access in any manner to an applicant or employee's social networking website. It prohibits an employer from demanding "access in any manner," so requesting to view the account or a paper printout clearly fall within the prohibition.[8]

California's law focuses on protecting employees' and applicants' use of social media but broadly encompasses the use of an electronic service or account, similar to the Maryland law.[9] The law prohibits an employer from requiring or requesting: 1) a user name or password "for the purpose of accessing personal social media"; 2) an applicant or employee to "access personal social media in the presence of the employer"; and 3) divulgence of "any personal social media."[10] Thus, like the Illinois law, and unlike the Maryland law, the California law clearly prohibits an employer from obtaining access to an applicant's or employee's personal social media site by any method, including viewing or printing its content.

b. Breadth of Exceptions

The statutes include a variety of exceptions for employer monitoring of social-media accounts. All the exceptions remain subject to court interpretation, but some statutes, such as the Illinois statute, appear to exempt more monitoring by employers than others, such as the Maryland statute.

In the Maryland statute, an exception is provided to permit an employer to require disclosure of means for accessing non-personal accounts "that provide access to the employer's internal computer or information systems."[11] Additionally, the statute provides that it does not permit employees to "download unauthorized employer proprietary information."[12] It further provides that the statute does not prevent an employer from:

---

to log into a personal account without disclosing the log-in credentials to the employer so the employer can observe the content of the personal account or asking an employee or applicant to print the content of a personal account. Before an employer chooses this route, they should speak with their employment counsel to educate themselves about the legal risks of doing so. While Maryland is the first jurisdiction to enact this legislation, it is not likely to be the last. Indeed, bills proposing similar restrictions currently are pending in various states, including but not limited to California, Illinois, Minnesota, New York, and Washington. In addition, U.S. Senator Richard Blumenthal (D–CT) has stated his plan to introduce similar legislation "in the very near future."

[7] 820 Ill. Comp. Stat. Ann. 55 / 10 (West 2013), *available at* http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2398&ChapterID=68.

[8] The Illinois statute may be amended to adopt the more narrow terminology used in the Maryland bill. *See* H.B. 1047, 98th Gen. Assemb., Reg. Sess. (Ill. 2013). *available at* http://www.ilga.gov/legislation/BillStatus.asp?DocNum=1047&GAID=12&DocTypeID=HB&LegId=71494&SessionID=85&GA=98.

[9] Cal. Labor Code § 980 (West 2012).

(a) As used in this chapter, "social media" means an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations.

[10] *Id.*

(b) An employer shall not require or request an employee or applicant for employment to do any of the following:

(1) Disclose a username or password for the purpose of accessing personal social media.

(2) Access personal social media in the presence of the employer.

(3) Divulge any personal social media, except as provided in subdivision (c). (d) Nothing in this section precludes an employer from requiring or requesting an employee to disclose a username, password, or other method for the purpose of accessing an employer-issued electronic device.

[11] MD. Code Ann., Labor and Employment § 3-712 (West 2012) (effective Oct. 1, 2012).

(b)(2) An employer may require an employee to disclose any user name, password, or other means for accessing nonpersonal accounts or services that provide access to the employer's internal computer or information systems.

[12] *Id.*

(d) An employee may not download unauthorized employer proprietary information or financial data to an employee's personal Web site, an Internet Web site, a Web-based account, or a similar account.

(1) based on the receipt of information about the use of a personal Web site, Internet Web site, Web-based account, or similar account by an employee for business purposes, from conducting an investigation for the purpose of ensuring compliance with applicable securities or financial law, or regulatory requirements; or
(2) based on the receipt of information about the unauthorized downloading of an employer's proprietary information or financial data to a personal Web site, Internet Web site, Web-based account, or similar account by an employee, from investigating an employee's actions...

A close reading of the statute reveals language that will be subject to interpretation. What does "based on the receipt of information" mean? Does permitting investigation allow an employer to view personal account information? Because the act has been in effect for only a short time, the answers remain to be seen.

The Illinois statute, while containing a broader prohibition on viewing social media, also includes broad exceptions stating:

(2) Nothing in this subsection shall limit an employer's right to:

(A) promulgate and maintain lawful workplace policies governing the use of the employer's electronic equipment, including policies regarding Internet use, social networking site use, and electronic mail use; and
(B) monitor usage of the employer's electronic equipment and the employer's electronic mail without requesting or requiring any employee or prospective employee to provide any password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking website.

Unfortunately, this last provision is very unclear—may an employer use a keylogger to monitor what an employee does on the employee's social networking site while on the employer's electronic equipment?[13] While the intent may be more limited, the law arguably permits intentional unauthorized monitoring of electronic communications that is potentially challengeable under the federal Stored Communications Act and raises the issue of a potential conflict with that act.

Like the Maryland law, the California law includes an exception for investigations. Unlike Maryland's law, however, California's exception clearly permits an employer to require an employee to divulge content of a personal social media site during the investigation. The exception reads:

(C) Nothing in this section shall affect an employer's existing rights and obligations to request an employee to divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding.

Because the exception relies on pre-existing employer rights, the law is unclear as to what type of evidence of misconduct might be required before the employer could use the exception to require access to an employee's personal social-media site.

c. Effectiveness of Enforcement Mechanisms

No matter how comprehensive a prohibition, a statute is only effective if it contains a mechanism of enforcement. Moreover, in the employment context, if a statute contains no anti-retaliation provision,

[13] A keylogger is available as hardware or software and monitors each keystroke that an employee makes. Keyloggers are sometimes used by employers to monitor their employees. Other software, such as SpectorSoft, that monitors everything a particular employee does on a computer is also available.

then its effectiveness will often be minimized because of the ability of an employer to discharge, or otherwise discipline, a complaining employee.

A close reading of the Maryland statute leaves the reader with one key question: how is the statute enforced? The Maryland statute contains no enforcement mechanism, likely rendering it primarily ineffective, unless amended to include one (Philip L. Gordon, 2012).[14]

The Maryland statute does include an anti-retaliation provision that prohibits an employer from refusing to hire, discharging, disciplining, or otherwise penalizing an employee who refused to disclose protected information.[15] While if it had been combined with an effective enforcement provision, the anti-retaliation provision would offer employees significant protection, questions would still remain. For instance, how can an applicant or employee prove that the reason she was denied employment or fired was a refusal to provide a password or other protected means for accessing a personal account?

In contrast to the Maryland statute, as part of a pre-existing statute, the Illinois law provides for enforcement by the Illinois Department of Labor and by civil action (Lynne Bernabei & Alan R. Kabat, 2012). Unlike the Maryland statute, however, the Illinois law contains no robust anti-retaliation provision prohibiting refusal to hire, discharge, or other discipline. A provision elsewhere in the act makes it a petty offense to retaliate against someone who complains or sues—for which a $1,000 fine is the maximum punishment.[16]

Similar to the Maryland statute, the California law is completely silent as to what enforcement mechanism, if any, is available. The California statute states that the Labor Commissioner "is not required to investigate or determine any violation of this act."[17] Some point to a potential, albeit untested, enforcement mechanism by civil suit under California's Private Attorneys General Act. Under that law, an employee could allege violations in a civil action. This remains to be tested in an actual suit (Gina Haggerty Lindell & L. Geoffrey Lee, 2012).[18]

---

[14] As Philip L. Gordon states:

Notably, the Maryland law contains no enforcement provision. The law does not authorize applicants or employees to sue. The law does not even delegate authority to the Maryland Department of Labor, Licensing and Regulation, or any other government agency, to enforce it. It is possible that an employee terminated in violation of the law might have a claim for wrongful discharge in violation of public policy. However, because that claim typically applies only to discharge, it is unclear whether an employee who is disciplined short of discharge would have a claim. It also is uncertain whether an applicant who is denied employment in violation of the law would be able to assert a claim.

[15] MD. Code Ann., Labor and Employment § 3-712 (West 2012) (effective Oct. 1, 2012).

(c) An employer may not:

(1) discharge, discipline, or otherwise penalize or threaten to discharge, discipline, or otherwise penalize an employee for an employee's refusal to disclose any information specified in subsection (b)(1) of this section; or

(2) fail or refuse to hire any applicant as a result of the applicant's refusal to disclose any information specified in subsection (b)(1) of this section.

[16] 730 Ill. Comp. Stat. Ann. 5/5-4.5-75 (West 2012).

[17] The Act states, "Notwithstanding any other provision of law, the Labor Commissioner, who is Chief of the Division of Labor Standards Enforcement, is not required to investigate or determine any violation of this act."

[18] According to the authors:

The Legislature did not provide for any specific penalties for violating this new law. As such, existing law under the Labor Code Private Attorneys General Act would likely allow an aggrieved employee to file a civil lawsuit, to receive a specific penalty amount, and to obtain an attorney's fee award.

Interestingly, the Department of Labor Standards Enforcement has disclaimed any desire or responsibility to investigate or enforce any alleged violations of this new law.

See Cal. Labor Code § 2698 (West 2012). The Private Attorneys General Act of 2004 provides:

(f) For all provisions of this code except those for which a civil penalty is specifically provided, there is established a civil penalty for a violation of these provisions, as follows:

(1) If, at the time of the alleged violation, the person does not employ one or more employees, the civil penalty is five hundred dollars ($500).

(2) If, at the time of the alleged violation, the person employs one or more employees, the civil penalty is one hundred dollars ($100) for each aggrieved employee per pay period for the initial violation and two hundred dollars ($200) for each aggrieved employee per pay period for each subsequent violation.

(g) (1) Except as provided in paragraph (2), an aggrieved employee may recover the civil penalty described in subdivision (f) in a civil action pursuant to the procedures specified in Section 2699.3 filed on behalf of himself or herself and other current or former employees against whom one or more of the alleged violations was committed. Any employee who prevails in any action shall be entitled to an award of reasonable attorney's fees and costs. Nothing in this part shall operate to limit an

Also like the Maryland law, the California law includes an anti-retaliation provision prohibiting discharge, discipline, or other retaliatory action against an employee or applicant for refusing to comply with an employer's request for protected social-media information. The California law, even more explicitly than the Maryland law, by including a statement specifying that the law does not prohibit an employer from taking adverse action if otherwise permitted by law, raises the unresolved issue of what method will determine whether discipline or a refusal to hire resulted from the prohibited conduct or for some lawful reason.[19]

d. Remedies

Even with an enforcement mechanism, a law will generally be used only if it provides an adequate remedy. The Maryland statute does not specify remedies for violating the prohibition on requesting a password or other means of accessing a social-media account. Additionally, the remedy available to an applicant or employee who suffers adverse consequences for refusing to disclose her password is not specified. Again, court interpretation will be necessary to determine the applicable remedies.

In contrast, the Illinois statute specifies the available damages. Damages available in a civil action are actual damages, and, where the violation is willful and knowing, attorney's fees and costs. The availability of attorney's fees often makes pursuit of claims easier for plaintiff employees.

If an applicant or employee in California can bring a civil action under California's Private Attorneys General Act, then a court would assess penalties based upon the number of aggrieved employees. A prevailing plaintiff could also receive attorney's fees. (Gina Haggerty Lindell & L. Geoffrey Lee, 2012).

Employer requests for applicant passwords provided the impetus for the states to pass privacy protective statutes, of which those first passed by Maryland, Illinois, and California are exemplary. But the statutes in the states that have passed such legislation also regulate the same behavior with regard to employees.[20] What, if any, other mechanisms regulate privacy and employee use of social media during the employment relationship in these states? What about states that have not passed—and may never pass—such regulations? These laws are the topic of the next section.

3. During the Employment Relationship

Because there exists such a patchwork of potentially applicable laws, claims in the United States arise under various state and federal statutes, common law, and pursuant to collective bargaining agreements. This section begins with a discussion of cases arising under the federal Electronic Communications Privacy Act (ECPA), particularly under the Stored Communications Act (SCA), and follows with

---

employee's right to pursue or recover other remedies available under state or federal law, either separately or concurrently with an action taken under this part.

Id. See also 2012 California Labor and Employment Legislative Update, Jones Day (Oct. 2012), http://m.jonesday.com/2012_california_labor/ (last visited Jan. 24, 2013).

The new law contains no enforcement provision. Potentially, an employee terminated for refusing to provide access to a social media username or password could bring a claim for wrongful termination. Additionally, it is possible that a violation of the new statute could result in a claim for penalties under the California Labor Code Private Attorneys General Act ("PAGA"), Cal. Labor Code section 2698 et seq.

Id.

[19] Cal. Labor Code § 980 (West 2012).

(e) An employer shall not discharge, discipline, threaten to discharge or discipline, or otherwise retaliate against an employee or applicant for not complying with a request or demand by the employer that violates this section. However, this section does not prohibit an employer from terminating or otherwise taking an adverse action against an employee or applicant if otherwise permitted by law.

Id. Often in the United States under discrimination statutes, courts will use what is termed a burden shifting paradigm where the employee must ultimately prove that the adverse action resulted from the protected conduct. Courts have borrowed this framework, which is rather confusing, for use in other employment contexts.

[20] The New Mexico statute may govern only applicants. S.B. 371, 51st Leg., 1st Sess. (N.M. 2013), *available at* http://www.nmlegis.gov/Sessions/13%20Regular/bills/senate/SB0371.pdf.

a review of state cases arising under state common law for invasion of privacy. It then turns to potential protections for public employees under the Fourth Amendment to the U.S. Constitution, and finally, discusses some cases decided in labor arbitration pursuant to a collective bargaining agreement.

a. ECPA

A few notable cases have arisen under the ECPA, particularly under Title II of the Act, the SCA. There is a strong argument that this statute should be interpreted to provide a high level of protection for employee privacy. Indeed, some courts have interpreted the statute to protect employees' password-protected social-media sites. The ECPA provides minimum statutory damages for each violation, including violations of the SCA, which provides for a minimum fine of $1,000 or, if greater, actual damages.[21]

The ECPA is a complex and outdated statute that was passed in the 1980s,[22] and its details are beyond the scope of this article. What is important to a discussion of social media and the employment relationship is that Title II, the SCA, prohibits intentional, unauthorized access to stored electronic communications. Several courts have held that an employee who provides a password to personal email or other online accounts in response to pressure from an employer has not truly given consent. Thus, the employer's access is not authorized.[23] A couple of courts have applied the same principle to password protected social-media sites. A related federal statute, the Computer Fraud and Abuse Act, similarly protects stored communications. No employee claims have been filed under that statute, however, presumably due to difficulties in proving the high level of required damages.

In 2009, two employees sued in a New Jersey federal district court after they were terminated for posts made in a MySpace chat group. The jury found the employer had unlawfully accessed the communications without user authorization. The court upheld the jury verdict. The employees had used their MySpace accounts and passwords to participate in an invitation-only chat group. A manager accessed the group after pressuring another employee to disclose her password. The court upheld an award of compensatory damages resulting from loss of work, as well as an award for punitive damages.[24] The result is especially interesting in an at-will employment context. Employment at will means an employer may normally terminate an employee for any reason or no reason at all, with some statutory and common law exceptions. Yet, in this case, a statute not particular to the employment relationship resulted in compensation for lost work.

Another case was decided in the Northern District of Illinois in 2011. In this case, an employee stored passwords to both her personal and work-related Facebook and Twitter accounts in a locked folder on the employer's server. While the employee was off work recovering from injuries sustained in a work-related accident, the employer accessed and used her personal accounts to promote its interior-design business. The court declined to grant summary judgment to the employer, finding that "there is undisputed evidence in the record that Defendants accessed [plaintiff's] personal Facebook account and accepted friend requests... [and] that Defendants posted seventeen Tweets to [plaintiff's] personal Twitter account... As such, there are disputed issues of material fact whether Defendants exceeded their authority in obtaining access to [plaintiff's] personal Twitter and Facebook accounts."[25]

---

[21] 18 U.S.C. § 2707(c) (West 2012).

[22] Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (West 2012).

[23] Brahmana v. Lembo, No. C-09-00106 RMW, 2009 WL 1424438, at *3 (N.D. Cal. May 20, 2009) (denying motion to dismiss ECPA claims for unlawfully intercepting and using employee's personal password); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 562 (S.D.N.Y. 2008) (an employee should have the opportunity to refuse or withdraw consent to monitoring); Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 928 (W.D. Wis. 2002) (reasoning that unauthorized access includes reading an employee's emails on a password protected web-based account, hotmail); Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010) (holding attorney-client privilege protects emails sent on company issued laptop through personal, password-protected, web-based email account).

[24] Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 WL 3128420, at *5 (D.N.J. Sept. 25, 2009) (jury could infer employee was pressured into providing a password and as such did not authorize employer's use of online chat group). The employer was a restaurant. *Id.*

[25] Maremont v. Susan Fredman Design Group, Ltd., No. 10 C 7811, 2011 WL 6101949 (N.D. Ill. Dec. 7, 2011).

While the aforementioned cases involved current employees, there is an argument that pressuring an applicant into providing a password for a social-media account would also result in unauthorized access. No case has yet tested this theory.

b. State Law and Invasion of Privacy Tort

As discussed in Section 2, many states have recently passed legislation protecting both applicants and employees from employer efforts to obtain social-media passwords. Most states also have enacted equivalents of the ECPA, including the SCA. Delaware and Connecticut require employers to notify employees that their electronic communications are being monitored. The requirement presumably extends to the monitoring of social-media activity.[26] Two other states, Michigan and Illinois, prohibit employers from gathering information on personal communications for inclusion in personnel records. This prohibition would, presumably, extend to gathering information about communications via social media.[27] Three states—New York, Colorado, and North Dakota—expressly protect lawful, off-duty conduct. In New York, protection extends only to recreational activity, a category that excludes dating, but presumably includes online activities such as blogging, chatting, or posting on Facebook.[28]

In states that have not enacted such legislation, the most likely claim would involve a common-law tort claim for invasion of privacy, often termed intrusion on seclusion.[29]

In the Illinois case involving the hospitalized interior designer, discussed in sub-section 3.a, in addition to the SCA claim, the plaintiff also brought an invasion-of-privacy claim. In Illinois, as in many other states, the claim requires a showing of: 1) unauthorized intrusion, that would be 2) highly offensive to a reasonable person, involving a 3) private matter, which, in many states, means a matter in which the plaintiff had a reasonable expectation of privacy, and 4) anguish and suffering. Because the plaintiff had 1,250 Twitter followers and numerous Facebook friends, and because she was promoting the employer design firm and linking to its page on her personal accounts, the court held that she had no reasonable expectation of privacy in her social-media accounts. The plaintiff did not try to keep the information private, and the information was not, in fact, private.[30]

As a federal district court in New Jersey has noted, courts normally find no reasonable expectation of privacy in social-media accounts without privacy settings limiting access to a few people. Accounts open to public view will not be considered private. On the other end of the spectrum, communications made to only one person will be considered private. In the middle, where the account is not public but is open to more than one person, however, different courts may rule differently. On the facts presented, the court denied a motion to dismiss the plaintiff's claim for invasion of privacy. The plaintiff was a nurse, as well as president of her union local. (Often, it is a union representative who brings a claim. This is not only because employers may retaliate against union activity, but also because the union is funding the litigation, while other non-union represented employees may not be able to afford filing suit.) Another nurse, who was Facebook "friends" with the plaintiff, accessed her friend's account and allowed the employer to view

[26] Connecticut requires notice of any monitoring that is not direct observation. *See* Conn. Gen. Stat. Ann. § 31-48d (West 2012). Delaware covers monitoring of telephone, internet, and email. Del. Code Ann. tit. 19, § 705 (West 2012).

[27] 820 Ill. Comp. Stat. Ann. 40 / 9 (West 2012); Mich. Comp. Laws Ann. § 423.508 (West 2012).

[28] Colo. Rev. Stat. Ann. § 24-34-402.5(1) (West 2012) (just termination); N.Y. Lab. Law § 201-d (McKinney 2012) (any type of adverse action); N.D. Cent. Code § 14-02.4-03 (West 2011) (any type of adverse action or lawful off-duty conduct).

[29] There have been several successful claims. *See, e.g.*, Fischer v. Mt. Olive Lutheran Church, 207 F. Supp. 2d 914 (W.D. Wis. 2002) (Hotmail might be entitled to reasonable expectation of privacy and may have been highly offensive for employer to go onto employee's personal account and read his emails); Restuccia v. Burk, No. CA 952125, 1996 WL 1329386 (Mass. Super. Ct. Aug. 13, 1996) (finding that there could be a reasonable expectation of privacy in a business email where the employee was told he could use email account for personal communications and he had his own password, but without his knowledge, employer had a separate password; court denied summary judgment). There have also been unsuccessful claims. *See, e.g.*, Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 WL 2066746 (D. Or. 2004) (no reasonable expectation of privacy when employee downloads inappropriate content from personal email at work and stores it in folder marked personal at work, if employee did not restrict with password, and not highly offensive for employer to monitor by investigating Internet hits, but not content); Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (finding no expectation of privacy when employee communicate with supervisor over company email, even if employee was assured his email would not be intercepted by manager).

[30] Maremont v. Susan Fredman Design Group, Ltd., No. 10 C 7811, 2011 WL 6101949 (N.D. Ill. Dec. 7, 2011).

her posts. In one post, the plaintiff had criticized paramedics for saving the life of an octogenarian who had open fired at the Holocaust Museum in Washington, D.C. The hospital reported the post to various regulatory boards. The court reasoned that the plaintiff "may have had a reasonable expectation that her Facebook post would remain private, considering that she actively took steps to protect her Facebook page from public viewing." The court noted that reasonableness and offensiveness are fact-specific inquiries, and that it was not evident how many Facebook "friends" the plaintiff had, or how many people could have viewed her post.[31] Notably, the employer did not move to dismiss the ECPA claim, probably because the employee allegedly had been coerced, and there was thus no user consent to access the stored communications.

c. Public Employees

The U.S. Constitution protects individuals, including government employees, from certain government actions. The Fourth Amendment in particular protects against unlawful searches and seizures. This protection has long been interpreted to apply to employees' privacy in items such as their private offices, desks, and locked cabinets.[32]

In 2010, the U.S. Supreme Court decided a Fourth Amendment case involving an employer that searched an employee's text messages sent on an employer-issued device.[33] The case received a great deal of publicity, and brought the issues of employer monitoring and employee privacy to prominence. The Court ruled that, even if there was a reasonable expectation of privacy in text messages sent on the employer-issued device, the search was for a reasonable purpose and was carried out by reasonable means. The Court declined to decide whether the employee, a SWAT Team officer, had a reasonable expectation of privacy in his messages, which pertained to a tryst involving his wife and another officer, reasoning that rapid advances in technology warranted reserving the expectation of privacy issue for a later case. The Court did, however, imply in a separate analysis about the reasonableness of the intrusion that the plaintiff did not have a reasonable expectation of privacy. As to the reasonableness of the employer's actions, the Court reasoned that the employer had a legitimate interest in determining the cause of excessive text messages for which the employer was being billed. Furthermore, the Court reasoned that reviewing the transcripts was an expedient and efficient way of meeting that objective. The Court further reasoned that the two-month scope of the review was also reasonable, especially in light of the employer's policy, which notified employees that text messages were subject to audit. Another interesting aspect of this case is that while the plaintiff lost the Fourth Amendment claim at the Supreme Court level, the Ninth Circuit held that the third-party service provider had violated the SCA when it released the text messages to the employer without the employee's consent. That aspect of the case stands as governing law, at least for now.

One article recently offered predictions for how courts are likely to treat social-media privacy under the Fourth Amendment (Alexander Naito, 2012). The article asserts that Fourth Amendment doctrine, which treats the disclosure of a communication to a third party as fatal to any reasonable expectation of privacy, leaves most social-media communications unprotected. At the same time, the article acknowledges that messages sent to one individual, via Facebook, for example, will likely be protected unless the recipient discloses them to an employer.[34] A more optimistic scenario for privacy advocates than that proposed in the article is that courts will adopt an approach that falls somewhere between the two extremes, finding a reasonable expectation of privacy in communications shared with a limited readership. This seems particularly likely where the communication is password protected or accessible by invitation only. Social-media communications shared with large numbers of people seem less likely to be protected because they are so easily shared and more easily accessed by an employer. The article expresses concern that the current focus on accessibility to physical workspace means an employee has no reasonable expectation of privacy in online communications, as long as the employer is physically

[31] Ehling v. Monmouth-Ocean Hospital Service Corp., No. 2:11-cv-03305 (WJM), 2012 WL 1949668 (D.N.J. 2012).

[32] O'Connor v. Ortega, 480 U.S. 709 (1987).

[33] City of Ontario v. Quon, 130 S. Ct. 2619 (2012).

[34] *Cf.* Romano v. Steelcase Inc., 907 N.Y.S.2d 650 (N.Y. App. Div. 2010) (discussing in discovery context how no reasonable expectation of privacy inheres in social media because a communication is not private once having reached a recipient and because terms of service do not guarantee privacy).

able to access its own equipment. Courts may, however, be more willing to easily analogize between physical space and virtual space. If a virtual space offers as much privacy as, say, a private office or desk, it also offers a reasonable expectation of privacy. The article also expresses concern that courts focus too much on whether an employer has notified workers of an intent to monitor, and not enough on whether an individual employee has taken reasonable steps—such as setting a password—to protect her privacy. While it is true that courts tend to focus on notice, it seems possible that policies in which employers reserve the right to monitor online activity will not vitiate the reasonable expectation of privacy in communications protected with personal passwords. Of course, if the employer is monitoring and obtaining personal communications without need for the password, and the employee is aware of the monitoring, then a reasonable expectation of privacy may not be found to exist.

A related non-privacy issue is whether First Amendment rights are violated when public employees are disciplined for opinions conveyed through social media. The United States generally provides strong protection for free speech, but that protection is curtailed in the employment context. An employee acting in an official capacity has no protection. If the employee is acting in an unofficial capacity, protection is afforded only where the statement is of public interest, and the need to make it outweighs the employer's interest in running an effective workplace. Many high-profile cases involve teachers who have been terminated for comments posted via social media. One author recently wrote an interesting piece suggesting that free-speech precedent should be overturned and interpreted to provide more protection for teachers posting via social media (Mary-Rose Papandrea, 2012).

d. Arbitration

In the United States, unionization is generally at the plant or store level. Unions often negotiate for contract provisions that say an employee can be terminated only for just cause, which provides some privacy protections for the use of social media, particularly during off-duty hours. Arbitration decisions provide particular insight into the issue, since arbitrators are more likely than courts to delve into the details of a specific employee's situation. Arbitrators consider factors including the employee's mental health, length of employment, and interaction with other employees.

Generally, arbitrators will uphold employer rules prohibiting personal use of employer equipment for electronic communications when the policy is enforced and progressive disciplinary steps are followed. Most will permit personal use to be limited to an employee's break time. But as to an employee's off-duty life, arbitrators will generally find it beyond an employer's control unless a direct nexus to the employment justifies disciplinary measures (Ariana R. Levinson, 2010).

Many arbitration decisions are unpublished, but a few published decisions address employee use of social media. One especially relevant case involved an employee's use of social media with his family outside work.[35] The employee was in the process of a divorce and worked at the same plant as his father-in-law. He sent his mother-in-law a profane Facebook message, saying that the mother-in-law would be judged by God and live in hell. The employee then sent a second message saying he would see the father-in-law at the plant. The employee had been incarcerated for 100 days on domestic-violence charges stemming from an incident involving his wife. The day after the employee returned to work, the father-in-law told the human resources department about the messages. As it happened, the employee had sent a third message, the day after sending the first two, apologizing for his previous statements and expressing an intention to turn his life around. He suffered from depression, anxiety, and insomnia, and was in therapy for eight months. The arbitrator decided that the first message had not been a threat. The second, while threatening, was not equivalent to an express threat of physical violence made during a confrontation at the plant. The arbitrator found the third message to have been a sincere apology. The in-laws had not been particularly troubled, had delayed informing the company, and contacted a prosecutor only at the company's suggestion. The arbitrator found that the off-duty conduct had not been sufficiently threatening to justify discharge, and imposed a 30-day suspension instead. The arbitrator further ordered that the employee be made whole for any additional losses.

[35] U.S. Steel Corp. v. Steelworkers, 130 Lab. Arb. Rep (BNA) 461 (2011) (Bethel, Arb.).

Another case not only involved privacy for off-work conduct, but also raised a hot topic in United States labor law—protected concerted activity. In this case, the arbitrator found just cause to terminate an employee for posts made in a closed Facebook group.[36] The four group members were co-workers but one shared a Facebook account with her husband. The husband relayed the communication, which eventually found its way to the employer. The grievant had made 10 of the 16 posts in the group, and had approved of a "racist" entry pertaining to a white manager. The arbitrator found that the conduct was not protected concerted activity, and that there was a sufficient nexus to work to justify discharge.

As to the privacy issue, the arbitrator recognized that another arbitrator reinstated another employee who had made only four posts.[37] But the grievant approved of two posts that constituted threats, and made numerous disparaging comments. The arbitrator thus found a sufficient nexus between the posts and employment to justify discharge. The case illustrated the ways in which boundaries between on- and off-duty conduct can become blurred. The grievant made all the posts from home or from her personal smart phone. While she asserted the posts from her phone were made during break, the arbitrator insinuated they were made during time she should have been working. In any event, the arbitrator reasoned that the posts undermined the working relationship with administration, co-workers, and parents. Thus, there was a sufficient nexus between the conduct and her employment.

As to the argument that the posts were protected concerted activity, the arbitrator reasoned first that the majority of the posts were not about terms and conditions of work at all. The arbitrator found only one comment was about work, and that post was about a supervisor arriving late and expecting the chat group members to be timely. The arbitrator reasoned the post was admittedly just griping and was not meant to induce action for mutual aid or protection. He held the employees were not acting together to address workplace concerns.

When employees are using social media in the way they would previously have conversed around the water cooler to discuss terms and conditions of employment, the National Labor Relations Act (NLRA) forbids the employer from taking negative action. This approach constitutes a straightforward application of the law governing protected concerted activity. Nevertheless, the National Labor Relations Board's (NLRB) rulings have generated a lot of attention from the press because employers are wary that Facebook is a more public and more easily accessible forum than the water cooler. Moreover, the law often renders unlawful employer rules and policies that are overbroad in prohibiting the use of social media and that would deter a reasonable employee from engaging in protected activity for fear of violating the rule (Robert Sprague, 2012). Generally, these claims would be brought to the NLRB, rather than an arbitrator, which would assess whether the conduct was concerted, either done as a group or as an outgrowth or impetus toward group activity; for mutual aid and protection, meaning conversation more than mere griping regarding terms or conditions of employment; and not so profane or disloyal as to lose the protection of the Act. Professor Bob Sprague recently reviewed approximately 100 charges filed with the NLRB, related to social-media use, and the thirty-six documents generated by the NLRB in these cases: twenty-one NLRB Office of the General Counsel Advice Memoranda, ten General Counsel reviews, four Administrative Law Judge decisions, and one Board decision. A related privacy issue that Professor Sprague recognizes the NLRB will likely have to address is that employers are prohibited by the NLRA from conducting surveillance of union activity.[38] Thus, an employer who tracks online organizing arguably has violated the NLRA. Since the Sprague review, the Board has issued another decision regarding the use of social media for protected concerted activity, which confirms that the standard analysis of protected concerted activity applies when employees are using social media.[39]

---

[36] Vista Nuevas Head Start (AFSCME MI local), 129 Lab. Arb. Rep. (BNA) 1519 (2011) (VanDagens, Arb.).

[37] *Id.* That arbitrator found the posts were private, the husband had breached their privacy, and the employer was responsible for sharing the posts with co-workers and parents. The arbitrator in the summarized case does not directly address that argument for breach of privacy, other than to mention that the employer did not seek out the posts but was justified in acting once it found out about them. The arbitrator instead reasoned that because the plaintiff invited co-workers to post, and the posts would disrupt the environment of teamwork and acceptance of all people and cultures, discharge was warranted.

[38] *Id.* at 1009.

[39] Hispanics United of Buffalo, Inc., 359 NLRB No. 37 (2012).

Turning back to the arbitration cases, another privacy-related issue arises when someone other than the employee posts information that reflects negatively on the employee. In one case, a high school teacher's estranged wife posted nude photos of the teacher on MySpace. The decision does not indicate whether access was restricted, but it does not appear to have been because children were able to access the photos. The arbitrator upheld the termination because the teacher had not taken reasonable steps to maintain custody and control of obscene photos.[40]

4. After the Employment Relationship

Discovery during litigation generally raises issues as to whether social-media communications are discoverable and, if so, to what extent. Many cases arise where an employer seeks to access a prior employee's social-media account. The Federal Rules of Civil Procedure permit discovery of any non-privileged information reasonably calculated to lead to relevant information.[41] This is a very low bar, considering that the Federal Rules of Evidence define "relevance" as any information that makes a fact in controversy more or less likely.[42] But the rules further provide that a discovery request must be made with reasonable particularity,[43] and must not be unduly burdensome.[44] The rule regarding requests for electronically stored information contains a similar requirement restricting unduly burdensome discovery.[45] Thus, some courts have disallowed wholesale discovery of social-media communications on these grounds. Whether generalized, applicable principles will develop via judicial precedent, and, if so, whether they will be codified, remains to be seen.

One case recently in the news presents the issue well. Home Depot is a large company and employer. It does some innovative things to foster good employment practices, such as anonymous hiring and promotion. Nevertheless, an employee sued the company, claiming she was terminated as a result of

---

[40] Warren City Bd. of Educ. v. Ohio Educ. Ass'n, 124 Lab. Arb. Rep. (BNA) 532 (2007) (Skulina, Arb.).

[41] Fed. R. Civ. P. 26(b). Discovery scope and limits:

(1) *Scope in General.* Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense—including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(C).

Id.

[42] Fed. R. Evid. 401. Evidence is relevant if:

(a) it has any tendency to make a fact more or less probable than it would be without the evidence; and

(b) the fact is of consequence in determining the action.

Id.

[43] *See* Fed. R. Civ. P. 34. Rule 34(a) permits discovery of information in party's custody, control, or possession, but must describe with reasonable particularity—show reasonable notice of what called for and what not. *Id.* Rule 34(b) provides:

(1) *Contents of the Request.* The request:

(A) must describe with reasonable particularity each item or category of items to be inspected . . . .

Id.

[44] FRCP 26(b)(2)(C) provides that [o]n motion or on its own, the court must limit the frequency or extent of discovery if it determines that:

(i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;...

(iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

[45] Rule 26(b)(2)(B) addresses "Specific Limitations on Electronically Stored Information." Fed. R. Civ. P. 26. According to Rule 26(b)(2)(B):

A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

Id.

her gender and a disability and that the company had failed to accommodate her disability, a condition known as vertigo (Declan McCullagh, 2012).[46]

The employer sought to discover four categories of social media:

(1) Any profiles, postings or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries) from social networking sites from October 2005 (the approximate date Plaintiff claims she first was discriminated against by Home Depot), through the present, that reveal, refer, or relate to any emotion, feeling, or mental state of Plaintiff, as well as communications by or from Plaintiff that reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state;
(2) Third-party communications to Plaintiff that place her own communications in context;
(3) All social networking communications between Plaintiff and any current or former Home Depot employees, or which in any way refer [or] pertain to her employment at Home Depot or this lawsuit; or
(4) Any pictures of Plaintiff taken during the relevant time period and posted on Plaintiff's profile or tagged or otherwise linked to her profile.

The court notes that, generally, discovery requests must be reasonably calculated to lead to the discovery of admissible evidence, and must describe the information requested with reasonable particularity. The court also noted that many cases involving social media require a threshold showing that the information sought is reasonably calculated to lead to the discovery of admissible evidence.

The court reasoned that the simple fact that the plaintiff had communicated was not relevant to her mental health—it was the content of the communications that mattered. The court found that the first and second requests had failed to meet the requirement for reasonable particularity because "any emotion" could cover anything from momentary frustration over the late arrival of a cable repairman to an emotional reaction to a movie or TV show. The court further reasoned that a request for photos covering a seven-year period was too broad. However, the court held that the request for communications with Home Depot employees was adequate to put plaintiff on notice as to what was requested, and ordered her to provide that information.

Another issue that sometimes arises is whether information stored in social media can be subpoenaed from a non-party service provider. One high-profile, non-employment case held that it cannot, because the SCA bars third-party providers from releasing information without the user's consent, and the SCA makes no exception for discovery (Robert L. Arrington, Aaron Duffy & Elizabeth Rita, 2012).[47] Commentators generally agree that the court correctly interpreted the SCA, and at least one other court has ruled accordingly (Bruce E. Boyden, 2012). Yet, at least one state court in a non-employment case has ordered that a plaintiff authorize the third-party service provider to grant the defendant access.[48] And courts deciding employment cases may follow suit.

For instance, the magistrate judge in one employment case stated that, if necessary, he would order that the plaintiff authorize the service provider to produce records the plaintiff herself could not

[46] Mailhoit v. Home Depot U.S.A., Inc., No. CV 11-03892 DOC (SSx), 2012 WL 3939063 (C.D. Cal. Sept. 7, 2012).

[47] The authors note that the SCA prohibits subpoenaing third parties who host social networking cites, but that courts use Rule 34 of the Federal Rules of Civil Procedure to require plaintiffs to produce the social networking pages and archives of deleted information for inspection. *Id.* at 22–24 (citing Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010)). *See also* Steven S. Gensler, *Special Rules for Social Media Discovery?*, 65 Ark. L. Rev. 7, 26–27 (2012).

[48] Romano v. Steelcase Inc., 907 N.Y.S.2d 650 (N.Y. App. Div. 2010). The case was a personal injury case where publicly available social media indicated the plaintiff was not being honest about the extent of injuries. *See id.* In two other personal injury cases where publicly available social media indicated the plaintiff was not being honest about the extent of injuries, the court ordered the plaintiff to turn over user name and password to counsel. *See* Largent v. Reed, No. 2009-1823, 2011 WL 5632688 (Pa. Ct. Com. Pl. Nov. 8, 2011); McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 WL 4403285 (Pa. Ct. Com. Pl. Sept. 9, 2010). In one, *Largent*, the plaintiff attacked the request as overbroad, burdensome, and embarrassing, and the court limited access to thirty-five days. *Largent*, 2011 WL 5632688. The governing rules in these state cases may differ slightly from the federal rules of procedure.

produce.[49] The plaintiff, a white, Jewish female, filed a retaliation and discrimination suit against her employer. The employer served a subpoena upon LivePerson, a "'web site that is a platform for online advice and professional consulting services,'" including sessions with online psychics. The employer sought to obtain the plaintiff's communications with LivePerson psychics, including excerpts of chat sessions she had forwarded to her work email account. In her communications with LivePerson, the plaintiff had discussed her "work performance, relationships with co-workers, views regarding her treatment by [defendant], emotional state before, during, and after her employment, efforts to mitigate damages, and personal beliefs about African-Americans." LivePerson moved to quash the subpoena, arguing that the plaintiff could readily access and produce the requested materials. The plaintiff, however, had deleted many of the chat remarks and, thus, claimed she could not produce them in discovery.

The court did not resolve the issue of whether the SCA prohibited LivePerson from producing the information. The court reasoned that there were questions as to whether the information was electronically stored and as to whether the plaintiff consented to disclosure via the site's initial terms of use. The court held that the plaintiff should create a new LivePerson account and request that LivePerson restore her deleted chats so that plaintiff could turn over copies of the chats to the defendant. Significantly, the magistrate also stated that it might order the plaintiff to authorize the release by LivePerson of any material she could not restore.

Professor Steven Gensler recently published an article arguing that no additional or specially tailored rules are necessary for the discovery of social media because existing rules adequately address the situation (Steven S. Gensler, 2012). The article argues that a party would have to prove the relevance of the entire account to properly obtain an entire Facebook account. The article acknowledges that two courts, in three cases, have erroneously ordered access to an entire social-media site,[50] but believes that will not develop as the governing rule. The article also argues that courts err in requiring a showing of publicly available social-media information before permitting discovery of relevant private information. The article expects courts to use protective orders, such as in-camera filings, to protect privacy.

Indeed, the Federal Rules of Civil Procedure suggest that even private social-media activity should be discoverable, as long as it is reasonably calculated to lead to the discovery of relevant evidence and is unprotected by attorney-client or other privilege. There is an argument, of course, that the rules that governed in a time of letters are inadequate for an era in which great quantities of private information are potentially accessible. As a practical matter, the sheer volume of information may make discovery difficult, though the rules already contain exemptions for requests that are unduly burdensome. Perhaps for these reasons, a new privilege should be developed to protect social-media activity in the absence of a higher threshold than one "reasonably calculated to lead to admissible evidence."

Alternatively, it might be argued that social-media information should remain private due to the unique nature of the employment relationship. Perhaps permitting discovery of social media in the employment context deters lawsuits and encourages discrimination and other bad conduct. However, such a result seems unlikely. To the extent that courts err by granting defendants access to entire social-media accounts, further rulemaking might be appropriate. Rules prohibiting access to entire social-media accounts would be particularly appropriate if courts were requiring particularized requests in certain types of cases, such as commercial suits, but not in others, such as employment suits.

5. Conclusion

Privacy protections for social-media use in the United States depend not only on whether one is an applicant, employee, or former employee, but also on a host of other considerations. Some predictive considerations do appear, however, from a review of the cases. Privacy in social media is unlikely when the communication is with the public, or a large group of people. Privacy in social

[49] Glazer v. Fireman's Fund Ins. Co., No. 11 Civ. 4374, 2012 WL 1197167 (S.D.N.Y. 2012).

[50] *See also* Bruce E. Boyden, *Oversharing: Facebook Discovery and the Unbearable Sameness of Internet Law*, 65 Ark. L. Rev. 39, 50 (2012) (noting these erroneous published case are just the "tip of an unseen iceberg of unreported cases").

media is more likely when the communication is with a limited set of people, and even more so when the communication is with an individual. Regardless of the audience, privacy is more likely to be protected when the social-media account is password protected. Privacy for social-media activity is less likely in the workplace than at home, and even less likely when employer equipment is used. Privacy protection is especially unlikely where the employer has notified the employee of its intent to monitor social-media use.

The most likely trajectory of reform involves the passage of more state laws similar to those in Maryland, Illinois, and California. If these future laws contain adequate provisions for enforcement, adequate remedies, and effective anti-retaliation provisions, they will arguably provide the highest level of protection for job applicants and employees of the available potential claims. Without those important provisions, the prevailing patchwork will remain. For those involved in post-employment litigation, rule reform does not appear likely. However, case law may develop rules that protect litigants from overly broad or unduly burdensome requests.

Arguably, the most sensible type of reform would be a comprehensive federal employment statute governing technology and privacy in the employment relationship (Ariana R. Levinson, 2010). A comprehensive federal law could alleviate some of the uncertainty for employers and employees that results from the current patchwork of laws. Additionally, a law that addresses social media as well as other technological advances eliminates concerns about ill-thought out differences in treatment of equally invasive technologies.

Some academics have, of course, suggested other innovative alternate approaches targeted at social-media use. For instance, one recent article in the American Business Law Journal proposes that, because social media makes it difficult to segregate audiences, U.S. law should incorporate principles of situational privacy (Patricia Sánchez Abril, Avner Levin, & Alissa Del Reigo, 2012). The authors propose creation of a right to designate as private certain areas within the workplace by tagging a photo "confidential" or by marking a folder "private." They also propose a right to delete information, and a rule prohibiting reliance on personal or off-duty conduct as a basis for adverse action. Three states have already enacted legislation protecting the privacy of lawful, off-duty conduct. The other proposals are unlikely to become law, at least in the near future.

References

Abril, Patricia Sánchez, Levin, Avner & Del Riego, Alissa, *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 Am. Bus. L.J. 63 (2012).

Arrington, Robert L., Duffy, Aaron & Rita, Elizabeth, *An Arbitrator's Guide to Social Networking Issues in Labor and Employment Cases*, 66-Jan Disp. Resol. J. 20 (2012).

Bernabei, Lynn & Kabat, Alan R., *Congress and State Legislatures are Properly Barring Employers' Demands for Social-Media Passwords*, Nat'l L. J. (July 23, 2012).

Boyden, Bruce E., *Oversharing: Facebook Discovery and the Unbearable Sameness of Internet Law*, 65 Ark. L. Rev. 39, 50 (2012).

Felstiner, Alek, *Regulating In-Game Work*, 16 No. 2 J. Internet L. 3 (2012).

Gensler, Steven S., *Special Rules for Social Media Discovery?*, 65 Ark. L. Rev. 7 (2012).

Gordon, Philip L., *Maryland "Facebook Law" Raises New Obstacles For Employers Vetting Applicants And Investigating Employees, But With Important Exceptions*, Workplace Privacy Counsel (Apr. 11, 2012), http://privacyblog.littler.com/2012/04/articles/social-networking-1/maryland-facebook-law-raises-new-obstacles-for-employers-vetting-applicants-and-investigating-employees-but-with-important-exceptions/.

Levinson, Ariana R., *Carpe Diem: Privacy Protection in Employment Act*, 43 Akron L. Rev. 331 (2010).

— *What Hath the Twenty First Century Wrought? Issues in the Workplace Arising from New Technologies & How Arbitrators Are Dealing with Them*, 11 Transactions: Tenn. J. of Bus. L. 9 (2010).

Lindell, Gina Haggerty & Lee, L. Geoffrey, *California Labor Code Will Limit An Employer's Right to Ask for Access to Personal Social Media*, Gordon & Rees LLP (Oct. 2012), http://www.gordonrees.com/publications/viewPublication.cfm?contentID=2874 (last visited Jan. 24, 2013).

Loatman, Michael O., *Congress May Limit Employer Access to Personal Social Media*, 28 Daily Lab. Rep. A-6 (Feb. 11, 2013).

McCullagh, Declan, *Judge: Home Depot Went Too Far in Seeking Worker's Social Posts*, CNet (Sept. 17, 2012, 9:54 AM), http://news.cnet.com/8301-1009_3-57514250-83/judge-home-depot-went-too-far-in-seeking-workers-social-posts/?tag=nl.t720&s_cid=t720.

Naito, Alexander, *A Fourth Amendment Status Update: Applying Constitutional Privacy Protection to Employees' Social Media Use*, 14 U. Pa. J. Const. L. 849 (2012).

Papandrea, Mary-Rose, *Social Media, Public School Teachers, and the First Amendment*, 90 N.C. L. REV. 1597 (2012).

Sprague, Robert, *Facebook Meets the NLRB: Employee Online Communications and Unfair Labor Practices*, 14 U. Pa. J. Bus. L. 957 (2012).

Terry, Nicolas P., *Fear of Facebook: Private Ordering of Social Media Risks Incurred by Healthcare Providers*, 90 Neb. L. Rev. 703 (2012).