I. SOCIAL MEDIA IN THE WORKPLACE

Social media creates “tremendous potential for generating buzz—both positive and negative.”¹ Often at the divide between work and play, social media “raises difficult questions as to whether and how rules regarding workplace confidentiality, loyalty, privacy, and monitoring apply to these new forums and, if so, how these rules are balanced against freedom of expression” and the at-will employment relationship.² As the boundary between work and play becomes less distinct, social media’s appropriate role in the workplace is receiving increasing attention.³

Questions presented by social media in the workplace are growing along with the accelerated progression of technology. The courts are being asked: Who owns a Twitter account, and who should reap the fruits of the account’s success?⁴ If an employee posts on Facebook about his daughter’s cancer progression, then what happens when his employer sees the post and fires the employee to save costs? If an employee’s LinkedIn account makes

---

connections and attracts clients to the employer, then who has the rights to these clients?

Because technology has advanced rapidly in recent years, courts have not answered many of these questions. Because courts and agencies have not, and likely will not, catch up for a few more years. Though little clear-cut legal authority on these social-media issues exists, employers should take steps to protect their growing interests and information. For Arkansas employers utilizing social media, the solution is simple: enact a policy covering employees’ use of social media.

The goal of this comment is to assist employers and practitioners by: (1) addressing the intricate employment, contract, privacy, and ownership rights associated with social media in key cases, statutes, and administrative decisions; and (2) providing guidelines and language needed to craft a clear and concise social-media policy.

II. DEFINING “SOCIAL MEDIA” AND “SOCIAL NETWORK SITES”

A. Social Media

To address social-media concerns, employers must have a basic understanding of what “social media” is. Essentially, social media is a category of media through which people talk, participate, share, network, and bookmark online. Most social-media services encourage discussion, feedback, voting, comments, and information sharing. Where traditional media facilitates only a one-way broadcast by delivering content directly to an individual, social media promotes a two-way conversation in which web sites, resources, and people connect, create, and develop content collectively.

5. Id. at 3.
6. Id.
7. Id.
9. Id.
10. Id.
Although the forms of social-media sites are constantly evolving, the most common types of sites are: social news; social sharing; social bookmarking; and social networks. Social-news sites allow users to read articles about news topics and vote or comment on the articles. On social-sharing sites, users “create, upload, and share videos or photos with others.” Social-bookmarking sites allow users to find, bookmark, and save items of interest. Finally, social-network sites allow users “to find and link” to other users. Once linked, users can access each other’s contact information, interests, posts, and more. These network connections and two-way communications test the traditional workplace structure because of the rapid speed at which social-networking content and communications develop. Because the challenges presented by social-network sites are so diverse, this comment focuses on how social-media policies can address issues raised primarily in this context.

B. Social-Network Sites

Conventionally, social-network sites are “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.” The nature and nomenclature of these connections has varied from site to site, but popular terms include: “Friends,” “Followers,”

11. Id.
12. Id. (citing examples of social-news sites such as Digg, Sphinn, Newsvine, and BallHype).
13. Jones, supra note 8 (citing examples of social-sharing sites, such as Flickr, Snapfish, YouTube, and Jumpcut).
14. Id. (citing examples of social-bookmarking sites, such as Delicious and Faves).
15. Id. (citing examples of social-network sites, such as Facebook, LinkedIn, MySpace, and Twitter).
16. Id.
17. See id.
“Contacts,” and “Fans.” Whether one is making friends or acquiring followers, “[w]hat makes social-network sites unique is not that they allow individuals to meet strangers, but rather that they enable users to articulate and make visible their social networks.” These visible profiles and articulated relationship lists are often an employer’s primary concern with social media.

C. The Rise of Social-Network Sites

Market research suggests that social-network sites are growing in popularity worldwide. This explosive growth has prompted many companies to invest time, money, and resources in social-media creation, promotion, and advertisement. Proskauer Rose LLP conducted an informal survey on emerging trends and practices with social-media use in the workplace and found that over seventy-six percent of companies surveyed were utilizing social media for business. Ironically, nearly forty-five percent of these companies lacked social-network policies.

The rise of these sites indicates a shift in the organization of online communities. Social-network sites are primarily organized around people, rather than interests. Given that social-network sites enable individuals to connect with one another, “they have become deeply embedded in user’s lives,” heavily integrated into the workplace, and increasingly problematic for the employer-employee legal relationship.

19. Id. at 213-14 (noting that SixDegrees.com, launched in 1997, was the first recognizable social-network site).
20. Id. at 211.
21. Id. at 213; see also Minehan, supra note 4, at 1-3 (describing the steps employers should take when their employees, who use social-media accounts to market the company's products or services, resign and then declare ownership of that account).
25. Id.
27. Id.
28. See id. at 221.
III. WHY A SOCIAL-MEDIA POLICY MATTERS

Whether posting pictures, commenting on statuses, tweeting their locations, or blogging about their days, users’ social-media activities often invite their employers’ concerns.29 Information posted on the web does not disappear easily; even “deleted” photographs may remain accessible through backup copies that linger indefinitely on servers.30 Although an understanding of social media may help alleviate these concerns, recent litigation suggests that social-media issues will likely continue to arise in the workplace.31

A clear social-media policy remains an employer’s best tool for countering social-media issues because it provides a starting place for courts when, not if, issues arise.32 To ensure policies apply to all types of lawsuits, employers should adopt policies that are not overly broad or restrictive, are respectful of employee privacy rights, and are unambiguous.33 Attorney Adam S. Foreman, an authority on issues related to technology in the workplace, suggests that employers determine the culture they seek to create and fashion a policy to their specific needs.34 Nonetheless, when developing such policies, employers must be cognizant of: (A) the potential legal pitfalls in social-media policies; and (B) their potential responses to social-media issues with employees.

29. See Minehan, supra note 4, at 1-2.
31. See Minehan, supra note 4, at 1.
32. See id.
34. Telephone Interview with Adam S. Foreman, Senior Principal, Miller, Canfield, Paddock & Stone, P.L.C. (Nov. 20, 2012). Mr. Foreman’s work in labor and employment law has been recognized by Michigan Super Lawyers, Best Lawyers in America, Chambers USA, and DBusiness. See Adam S. Foreman, MILLER CANFIELD, http://www.millercanfield.com/AdamForeman (last visited Nov. 11, 2013).
A. Potential Pitfalls Facing Social-Media Policies

Specifically, Arkansas employers developing social-media policies should familiarize themselves with the laws and potential legal pitfalls that present social-media issues, including: (1) the National Labor Relations Act (NLRA); (2) the Electronic Communications Privacy Act (ECPA); (3) the Federal Trade Commission Guidelines (Guides); (4) the Fair Credit Reporting Act (FCRA); (5) the Health Insurance Portability and Accountability Act (HIPAA); (6) the Genetic Information Nondiscrimination Act (GINA); (7) the Computer Fraud and Abuse Act (CFAA); (8) the common-law right to privacy; and (9) various state laws. The following sections address each of these legal areas respectively.

1. National Labor Relations Act

The NLRA—codified at 29 U.S.C. §§ 157-169 and enforced by the National Labor Relations Board (Board)—is the cornerstone of federal labor law. Section 157 of the statute explicitly defines the right of employees to engage in “concerted activities for the purpose of collective bargaining or other mutual aid or protection.” Section 158(a)(1) states that employers shall not “interfere with, restrain, or coerce employees in the exercise” of their section 157 rights. The NLRA protects activities such as: joining or forming a union; picketing; striking; pursuing a


36. 29 U.S.C. § 157; see also Protected Concerted Activity, NAT’L LAB. REL. BOARD, http://www.nlrb.gov/rights-we-protect/protected-concerted-activity (last visited Sept. 30, 2013) (“The law we enforce gives employees the right to act together to try to improve their pay and working conditions or fix job-related problems, even if they aren’t in a union.”).

grievance; and speaking with co-workers about a job issue.\footnote{kolko, supra note 35.} Courts, and the General Counsel of the Board, must now address whether activities such as “tweeting” and Facebook posting fall under these protected activities.\footnote{See id. at 1, 3-8.}


In 2011, the Board’s Acting General Counsel, Lafe Solomon, acknowledged that every regional office of the Board had encountered social-media cases.\footnote{Scott Faust, NLRB Issues Complaint in NY Facebook Case, PROSKAUER LAB. REL. UPDATE (May 20, 2011), http://www.laborrelationsupdate.com/nlrb/nlrb-issues-complaint-in-ny-facebook-case.} Although adverse-employment actions garner the most attention, employers must be mindful of the NLRA’s reach into all employment matters, including pertinent social-media issues like employee surveillance and an employee’s right to privacy.\footnote{See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 884 (9th Cir. 2002) (“Surveillance ‘tends to create fear among employees of future reprisal’ and thus, ‘chills an employee’s freedom to exercise his rights under federal labor law.’” (quoting Cal. Acrylic Indus. v. NLRB, 150 F.3d 1095, 1099 (9th Cir. 1998))); see also Flexsteel Indus., Inc., 311 N.L.R.B. 257, 257 (1993) (“The test for determining whether an employer has created an impression of surveillance is whether the employee would reasonably assume from the [employer’s] statement that [the employee’s] union activities had been placed under surveillance.”).}

\footnote{a. The First Intersection of the NLRA and Social Media}

In December 2009, the Board’s Division of Advice (Advice Division) first addressed the intersection of the NLRA and social media in an Advice Memorandum.
concerning a Sears social-media policy.\footnote{Advice Memorandum from Barry J. Kearney, Assoc. Gen. Counsel, Div. of Advice, Office of the Gen. Counsel, Nat’l Labor Relations Bd., to Marlin O. Osthus, Reg’l Dir., Region 18, Nat’l Labor Relations Bd., Sears Holdings (Roebucks), Case 18-CA-19081 (Dec. 4, 2009), 2009 WL 5593880, at *1 [hereinafter Sears Holdings].} In the Sears Holdings case, a union sought to organize Sears technicians who were scattered geographically.\footnote{Id.} As part of the campaign, the union created a website, Facebook and MySpace pages, and a Yahoo listserv, none of which were affiliated with Sears but which technicians “routinely use[d] . . . to discuss the [u]nion campaign and other work-related concerns.”\footnote{Id.}

Sears issued its first social-media policy in June 2009.\footnote{Id. at *2.} The policy prohibited associates from discussing “in any form of social media... [the d]isparagement of [the] company’s or competitor’s products, services, executive leadership, employees, strategy, and business prospects.”\footnote{Sears Holdings, supra note 43, at *2.} Once Sears issued the policy, technicians who participated on the listserv expressed concern that the policy, if applicable, infringed their freedom of expression.\footnote{Id. at *1; see supra notes 37-38 and accompanying text (describing the scope of section 158(a)(1).}

In response to the policy, the union filed an unfair-labor-practice charge, alleging that the policy chilled the exercise of protected activity in violation of section 158(a)(1) of the NLRA.\footnote{Sears Holdings, supra note 43, at *2.} The case was submitted to the Advice Division, but no evidence demonstrated the employer had used the policy for employee discipline or in response to the union campaign, the listserv, or any other protected activity.\footnote{Id. at *1-3. In reaching its decision, the Advice Division relied on Lutheran Heritage Village-Livonia, where the Board outlined the inquiry into a particular rule’s “reasonableness.” Id. at *2-3 (citing 343 N.L.R.B. 646, 647 (2004)).} The Advice Division dismissed the charge because the Sears social-media policy could not “reasonably be interpreted in a way that would chill Section [157] activity.”\footnote{Id. at *2.}
at issue did not violate the NLRA because: (1) the rule covered a wide variety of activities; (2) the rule’s stated purpose was to protect Sears rather than to restrict the flow of information; (3) the policy sufficiently apprised employees that it did not apply to section 157 protected activity; (4) employees used the listserv to discuss the union campaign and were not disciplined for doing so; and (5) no evidence demonstrated that Sears implemented the policy in response to protected activity.\textsuperscript{52}

b. NLRB Guidance for Social-Media Policies

Following the \textit{Sears Holdings} case, the Board has addressed more social-media issues.\textsuperscript{53} In light of the volume and outcome of recent cases, the Board is taking a broader view of what constitutes protected concerted activity and what is required in an employer’s social-media policy.\textsuperscript{54} The expanded definition of protected concerted activity is important because an employer’s social-media policy is not per se impermissible under the NLRA;\textsuperscript{55} an employer has every right to prohibit employees from engaging in non-protected activities, such as disloyal speech or insubordination.\textsuperscript{56} But if an activity is protected, a policy may violate section 158(a)(1) when: “(1) employees would reasonably construe the language to prohibit Section [157]
activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section [157] rights. Thus, employers must draw narrow guidelines that restrict harassing conduct without interfering with protected activity.

Furthermore, without including examples of prohibited conduct, an employer’s social-media policy will be overly broad because courts will construe any ambiguity in the policy against the employer. Without explanations, employees may reasonably interpret a policy’s prohibitions as applying to protected discussion about the employer’s labor policies or treatment of employees. Moreover, if the maintenance of a policy “reasonably tend[s] to chill employees in the exercise of their Section [157] rights,” it will violate the NLRA and be unenforceable. Thus, any policy should clarify and restrict its scope by including examples of unprotected conduct.

In September 2012, the Board issued its first two decisions specifically addressing employer social-media policies in Costco Wholesale Corp. and Karl Knauz Motors, Inc. In Costco, the Board found that employees could have reasonably construed the policy as prohibiting section 157 activity because its “broad” prohibitions against damaging Costco or any individual’s reputation extended to employees’ communications protesting how Costco treated

57. Lutheran Heritage Village-Livonia, 343 N.L.R.B. 646, 647 (2004) (explaining that an employer’s maintenance of rules that are likely to have a “chilling effect” on an employee’s section 157 rights may constitute an unfair labor practice).


59. See id. at 19-21.

60. See id.


its employees.65 The Board may have been looking for “greater contextual detail than was apparent with Costco’s policy.”66 The Board advised that the Costco policy’s broad language needed rules addressing conduct not protected by the NLRA, such as “verbal abuse,”67 “harassment,”68 and “conduct which is injurious, offensive, threatening, intimidating, coercing, or interfering with’ other employees.”69

Similarly, the Board found that the employer’s policy in Karl Knauz Motors violated section 158(a)(1) of the NLRA.70 The employer, a high-end car dealership, maintained a policy that stated:

   Courtesy is the responsibility of every employee. Everyone is expected to be courteous, polite and friendly to our customers, vendors and supplies, as well as to their fellow employees. No one should be disrespectful or use profanity or any other language which injures the image or reputation of the Dealership.71

The Board determined that because the policy did not contain language to limit its application, employees could reasonably interpret the policy as chilling protests or employment criticisms for fear they may be seen as “‘disrespectful or injurious] [to] the image or reputation of the Dealership.’”72 The crucial takeaway from Costco and Karl Knauz Motors is that context and specificity are essential to a policy’s lawfulness under the NLRA.73 Whether language will be considered overbroad is “not always clear,” and savings clauses will not always work.74

---

66. See Spognardi & Dill, supra note 64.
68. Id. (quoting Lutheran Heritage Village, 343 N.L.R.B. at 647-49).
69. Id. (quoting Palms Hotel & Casino, 344 N.L.R.B. 1363, 1367-68 (2005)).
71. Id.
72. Id.
73. Spognardi & Dill, supra note 64.
74. Id.
2. The Electronic Communications Privacy Act

The ECPA—"enacted in 1986, before cellphone and e-mail use was widespread, and before social networking was even conceived"—is outdated. The ECPA essentially prohibits unlawful monitoring of electronic communications.

Unfortunately, the ECPA’s failure to keep up with today’s technology means letters in a file cabinet receive more protection than e-mails on a server. The outdated ECPA has caused uncertainty for employers and inconsistency within the courts. Social media is only complicating the problem. Questions over the interaction between social media and the ECPA remain unanswered. Can employers compel employees to provide them access to the employees’ Facebook pages? Can employers peruse their employees’ Twitter feeds? Does performing a Google search on an employee constitute unlawful surveillance?

Facing this uncertainty, employers should implement safeguards and practices to ensure: (1) that any social-media monitoring is performed only by the employees’ authorized representatives “who have a legitimate interest in carrying out the monitoring”; (2) that “any data collected as a result of any monitoring is stored safely, not tampered with and not disseminated more widely than is necessary”; and (3) that “personal data is not stored for any longer than

---

78. See Justin Conforti, Comment, Somebody’s Watching Me: Workplace Privacy Interests, Technology Surveillance, and the Ninth Circuit’s Misapplication of the Ortega Test in Quon v. Arch Wireless, 5 SETON HALL CIRCUIT REV. 461, 464 (2009) (“If employers monitor communications on workplace technology and employees inadvertently divulge personal information, employees will often struggle to find any legal protection, as the American legal regime does not provide any generally applicable, affirmative protection for employee privacy.”); Helft & Miller, supra note 76.
79. Helft & Miller, supra note 76.
Employers should narrowly tailor social-media monitoring to ensure that it goes no further than is necessary to protect the employer’s specific business interests. Moreover, employers should discuss findings with employees before taking disciplinary action. Finally, when issues do arise, employers need to particularize and document any misuse of social-networking sites by employees.

3. Federal Trade Commission Guidelines

Employers seeking to harness social media to promote their products or services must also consider the Federal Trade Commission’s (FTC) authority to regulate “unfair or deceptive acts or practices in or affecting commerce.” The FTC has specifically expressed concern that employers’ use of social media in advertising has generated consumer confusion by blurring the line between what is “advertising” and what is “opinion.”

Section 5 of the Federal Trade Commission Act (FTCA) grants the FTC authority to enforce penalties against employers for using unfair and deceptive acts or practices. An act or practice is “deceptive” if: (1) it represents or omits information that will likely mislead a consumer who is acting reasonably under the circumstances; and (2) the representation or omission is

80 Social Networks Survey, supra note 2.
81 See id. at 4.
82 Id. at 8.
83 Id. at 4-5.
“material” or “likely to affect the consumer’s conduct or decision with regard to a product or service.” The FTC may deem an act or practice “unfair” under the FTCA if it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition.”

In light of these concerns over deceptive practices, 16 C.F.R. § 255.5—part of the FTC’s “Guides Concerning the Use of Endorsements and Testimonials in Advertising” (Guides)—requires advertisers to disclose material connections they have with endorsers promoting their products. Whether the advertiser-endorser relationship requires the advertiser to disclose such material connections depends on various factors, including: (1) whether the advertiser compensates the endorser; (2) the terms of any agreement between the advertiser and the endorser; and (3) the length of the relationship between the advertiser and the endorser.

The Guides make clear that an advertiser may be liable for false or unsubstantiated statements made through endorsements, as well as for failure to disclose a material connection between the advertiser and the endorser that might materially affect the weight or credibility of the endorsement. If endorsers make material statements in the course of their endorsements that are not adequately disclosed, the employer-advertiser may be liable. The FTC has indicated a clear intent to enforce the Guides in social-media contracts. For example, the FTC recently

---

87. Letter from James C. Miller, supra note 86, at 175.
89. FTC Guides Concerning Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255.5 (2009).
90. 16 C.F.R. § 255.5.
91. FTC Guides Concerning Use of Endorsement and Testimonials in Advertising, 16 C.F.R. § 255.1(d), 255.5 (2009).
92. 16 C.F.R. § 255.5. For example, an employee tasked with blogging for the employer-advertiser may serve as an endorser.

(“Depending on the circumstances, an advertiser’s provision of a gift to a blogger for
investigated the clothing store Ann Taylor concerning one of its promotion programs, which allegedly offered bloggers gift cards in exchange for event coverage. In response to the FTC’s increasing scrutiny of online advertising in social media, employers should make employees who manage work accounts aware of disclosure obligations.

4. Fair Credit Reporting Act

The FTC also enforces the FCRA, which imposes procedural requirements on employers who wish to use consumer-reporting agencies for conducting background checks or credit checks of employees and job applicants. For example, employers must provide written notice to and receive consent from the employee or applicant before requesting a consumer report. Furthermore, the FRCA requires employers to provide notice before and after taking any adverse action based on consumer-report information.

The FCRA defines “consumer reporting agency” to include “any person which . . . regularly engages in . . . the practice of assembling or evaluating consumer credit information . . . for the purpose of furnishing consumer reports to third parties, and which uses any means . . . of interstate commerce for the purpose of preparing or furnishing consumer reports.” Although this definition does not appear to extend to employers who run a Google search on an employee or access the employee’s Facebook profile, the definition is broad enough to reach social-posting blog content about an event could constitute a material connection that is not reasonably expected by readers of the blog.

94. Id.
96. 15 U.S.C. § 1681d; see also Using Consumer Reports, supra note 95.
97. 15 U.S.C. § 1681m; see Using Consumer Reports, supra note 95.
aggregator sites and data-mining services that compile information about users.\(^9\)

Several complaints filed in federal court and with the FTC against the company Spokeo illustrate this point.\(^{100}\) Spokeo prepares reports of anyone identified by name, e-mail address, or phone number, by running simultaneous searches across more than forty social-networking sites.\(^{101}\) The complaints against Spokeo alleged that the company violated the FCRA by offering inaccurate data about consumers without allowing the consumers to correct the reports.\(^{102}\) Spokeo argued that it is not a consumer-reporting agency and, thus, is not subject to the FCRA; nonetheless, at least one FCRA claim brought against Spokeo has already survived a motion to dismiss.\(^{103}\)

5. Health Insurance Portability and Accountability Act

HIPAA addresses health-data security and privacy by requiring healthcare providers, health-insurance plans, and employers to meet national standards for electronic healthcare transactions.\(^{104}\) Under HIPAA, employers, employer healthcare providers, and related practitioners must follow strict disclosure standards that prohibit the transmitting of a patient’s unencrypted medical information, including, among other things, a patient’s personal-identifying information, medical procedures, or treatments.\(^{105}\) An employer may be liable if an employee

---

99. See Adams v. Nat’l Eng’g Serv. Corp., 620 F. Supp. 2d 319, 328 (D. Conn. 2009) (explaining that staffing agency was a “consumer reporting agency” when it assembled and evaluated reports related to job candidates).


101. Complaint, supra note 100; Davis, supra note 100.

102. Davis, supra note 100.


posts on social-media sites confidential patient information in violation of HIPAA. To mitigate this exposure, employers should quickly correct these types of situations and discipline employees who post such information. For example, when a medical technician in Michigan posted on Facebook personal-identifying patient information, the hospital-employer immediately terminated her for violating HIPAA and the hospital’s privacy policy. In light of HIPAA, employers should train employees on proper use and protection of personal-identifying patient information. Employers should also clearly explain to employees their disciplinary policies regarding social-media HIPAA violations.

6. Genetic Information Nondiscrimination Act

Next, in light of GINA provisions, employers should not make employment decisions based solely on an employee’s DNA characteristics of which the employer may have learned through the employee’s social-media site. Under GINA, an employer may not “request, require, or purchase genetic information of an individual or family member of the individual.” However, an exception to this prohibition exists when an employer inadvertently obtains information, such as through a social-media outlet. For instance, if an employee voluntarily friends her supervisor on Facebook, and her profile interests discuss her mother and grandmother’s fight against breast cancer, then the employer will likely not be held liable for the acquisition of that information. But if an employer requires an employee to provide it access to the employee’s protected social-networking site and obtains

107. See Ray Lane, Health Care Employees: Privacy/Social Media Interplay is Key Issue in Hospital Tech’s Firing Over Facebook Post, DAILY LAB. REP. (BNA), Aug. 11, 2010, at A-4.
110. 29 C.F.R. § 1635.8(b)(1).
111. See 29 C.F.R. § 1635.8(b)(1)(ii)(D).
the employee’s family cancer history as a result, the employer may be liable for GINA damages.112

7. Computer Fraud and Abuse Act

As computer use has become increasingly interstate in nature, the reach of the CFAA has expanded.113 Although most early cases under the CFAA involved hacking activities, courts have extended the Act to employer-employee disputes.114 The CFAA most commonly applies in the workplace when an employee accesses and obtains information from the employer’s protected computer, either without or exceeding authorization.115 If an employee accesses the employer’s protected computer and disseminates the employer’s trade secrets to one of the employer’s competitors, then the competitor may be held liable for a CFAA violation.116

Because CFAA violations may turn on an employer’s own definition of the employee’s right to access computer systems, employers should specifically define computer authorization in pertinent policies.117 Within such a definition, employers should distinguish between “access” violations and “use” violations because courts may construe vague policies against the employer.118 To provide clarity and to put employees on notice, employers should explain the CFAA in the context of the employer’s own computer systems.119

112. See 29 C.F.R. § 1635.8(a).
117. See LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1137 (9th Cir. 2009) (holding the CFAA did not apply where former employee was authorized to access personal e-mails after employment had ended).
118. See United States v. Nosal, 676 F.3d 854, 863-64 (9th Cir. 2012).
119. See Garland & Katz, supra note 113.
Eagle v. Morgan illustrates how courts may apply the CFAA in social-media contexts.120 Linda Eagle—the co-founder of Edcomm, Inc., and a prominent figure in the fields of “banking training” and financial services—sold all outstanding shares of Edcomm to Sawabeh Information Services Company (SISCOM).121 After the sale, Edcomm initially retained Eagle as an executive but soon terminated her.122 Edcomm then appointed Sandi Morgan as the Interim Chief Executive Officer of Edcomm.123 Following her termination, Eagle tried to access a LinkedIn account she had established several years prior.124 When she could not access the account, a flurry of litigation followed.125

Eagle sued Edcomm and others, alleging that the defendants improperly accessed and continued to use her LinkedIn account.126 Eagle asserted that as a result of this “unauthorized access” to her LinkedIn account, individuals searching for her were routed to a LinkedIn page featuring Eagle’s honors, awards, recommendations, and connections, but with Morgan’s name and photograph.127 She further asserted that the alleged CFAA violation and “misappropriation of the account cost [her] time, money, loss of good will, damage to reputation, and diminution of the fair market value of her name.”128

The defendants alleged ownership of the LinkedIn account because Eagle received assistance in maintaining the account at work and shared her password with a co-worker.129 The defendants also countersued and alleged, among other claims, that Eagle misappropriated the LinkedIn “connections” associated with her account and

121. Id.
122. Id.
123. Id.
124. Id. (stating that Eagle created her LinkedIn account to promote her banking-education services; to foster her reputation as a businesswoman; to reconnect with family, friends, and colleagues; and to build social and professional relationships).
126. Id. at *2.
127. Id.
128. Id.
129. See id. at *1-2.
violated the CFAA by using the account information.\textsuperscript{130} The court rejected Edcomm’s CFAA claims because it did not recognize the alleged damages.\textsuperscript{131} The CFAA requires “loss related to the impairment or damage to a computer or computer system, any remedial costs of investigating or repairing computer damages, or costs incurred while the computers were inoperable.”\textsuperscript{132} Therefore, the court did not recognize Edcomm’s alleged damages resulting from its “loss of business relations” and costs associated with replacing its advertisements.\textsuperscript{133} Nonetheless, Eagle illustrates that employers should consider the CFAA when implementing social-media and computer policies.

8. The Common-Law Right to Privacy

Employees have a reasonable expectation of privacy in the workplace, but such an expectation does not, in many situations, extend to their Internet, e-mail, and social-media use via employer-supplied computers.\textsuperscript{134} The most common theory claimants use to allege an invasion of privacy is “[i]ntrusion upon [s]eclusion,” which requires as one element a claimant’s “solitude or seclusion of . . . private affairs.”\textsuperscript{135} An employee’s likelihood of recovery on an invasion-of-privacy claim is greater when the employee’s account is personal and password-protected, as opposed to being supplied or provided by an employer.\textsuperscript{136} For example, in Fischer v. Mt. Olive Lutheran Church, Inc., an

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{130} Eagle, 2011 WL 6739448, at *3-4.
  \item \textsuperscript{131} Id. at *9.
  \item \textsuperscript{132} Id.
  \item \textsuperscript{133} Id.
  \item \textsuperscript{134} See Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (holding no reasonable expectation of privacy existed in e-mail communications voluntarily made by an employee to his supervisor over the company’s e-mail system because the employee lost any reasonable expectation of privacy once he chose to make the unprofessional comments over the e-mail system).
  \item \textsuperscript{135} RESTATEMENT (SECOND) OF TORTS § 652B (1977). Intrusion upon seclusion claims require one to prove: (1) intentional intrusion; (2) physically or otherwise; (3) upon the solitude or seclusion of another of his private affairs or concerns; (4) liability to the other for the invasion of his privacy; and (5) intrusion would be highly offensive to a reasonable person. \textit{Id}.
  \item \textsuperscript{136} See Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 928 (W.D. Wis. 2002) (denying employer’s motion for summary judgment as to privacy claim because it was disputed whether a reasonable person would consider the former employee’s e-mail account private).
\end{itemize}
\end{footnotesize}
employer guessed the password to access an employee’s personal Hotmail account; thus, the employee alleged an invasion of privacy. The employer argued the employee had been accessing the account using an employer-supplied computer, but the court viewed the employer’s access of the account as an invasion of the employee’s privacy because the employee had taken reasonable steps to make his account private.

Considering *Fischer*, an employer should notify employees in its policy that electronic communications are solely for business purposes and that the employer may monitor or access all Internet usage. Employees, on the other hand, should understand that creating passwords will not, by itself, create a privacy expectation precluding an employer from reviewing tweets, “likes,” and messages transmitted over a company’s network.

### 9. State-Specific Laws

Employers must also be aware of trends in state legislation regulating social-media in the workplace. Recent state-law developments concerning social-media regulation include: (a) account-access statutes; and (b) off-duty conduct statutes.

#### a. Account-Access Statutes

One state-law development that employers must consider is regulation of employees’ personal accounts and online services through electronic-communications devices. Maryland and Illinois enacted the first state

---

137. *Id.* at 920-21, 927.

138. *Id.* at 928.

139. *See* Garrity v. John Hancock Mut. Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *1-2 (D. Mass. May 7, 2002) (holding employees did not have a reasonable expectation of privacy where they knew employer was able to look at e-mails and that message recipients might forward messages to others).

140. *Id.* at *2 (stating that employer’s instructions on how to create passwords and personal e-mail folders did not create privacy expectation that precluded employer from reviewing messages).

legislation of this kind in 2012. Maryland’s statute prohibits employers from requesting or requiring the “user name, password, or other means of accessing a personal account or service through an electronic communications device.” The Maryland statute prohibits employers from discharging, disciplining, or in any other way penalizing an employee for failing to disclose personal, social-media account information. Illinois’s amendment to its Right to Privacy in the Workplace Act mirrors the Maryland law and subjects employers who violate the law to penalties, including liability for actual damages.

Joining the trend, Arkansas enacted legislation in 2013 prohibiting employers from requesting access to an applicant or employee’s social-media account. Though the statute’s language is strong, many exceptions exist. If an employer inadvertently receives an employee’s login information, the employer is not liable for accessing the employee’s personal account. Furthermore, if an employee’s information is public, the employer has a right to such information. Finally, the Arkansas statute expressly reserves an employer’s existing right to request information if the employer reasonably believes the social-media account is relevant to a formal investigation. As password-protection legislation develops, employers must remain knowledgeable of both federal and state legislation.

142. 820 ILL. COMP. STAT. ANN. 55/10 (West 2013) (amended on Aug. 16, 2013); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2013).
143. MD. CODE ANN., LAB. & EMPL. § 3-712(b)(1).
144. MD. CODE ANN., LAB. & EMPL. § 3-712(c)(1)(2). The statute also prohibits an employer from refusing to hire a job applicant. MD. CODE ANN., LAB. & EMPL. § 3-712(c)(1)(2).
145. See 820 ILL. COMP. STAT. ANN. 55/10(b)(1).
146. 820 ILL. COMP. STAT. ANN. 55/15 (West 2013).
148. See ARK. CODE ANN. § 11-2-124(c).
149. ARK. CODE ANN. § 11-2-124(b)(1)(2).
150. ARK. CODE ANN. § 11-2-124(d).
b. Off-Duty Conduct Statutes

Several states have enacted statutes that prevent employers from taking action against employees based on off-duty conduct. These “lifestyle discrimination” laws are becoming more common as social media continues to grow; therefore, employers should examine their policies and practices to ensure compliance with these frequently overlooked statutes.

Lifestyle-discrimination laws exist in different forms; some laws address specific activities, but others encompass a variety of off-duty conduct. The most comprehensive statutes—such as those enacted by Colorado and New York—prohibit employers from discriminating against employees’ lawful activity occurring off the employers’ premises and during non-working hours.

Only slightly narrower in scope are statutes “prohibiting discrimination on the basis of an employee’s use of ‘lawful products’ or ‘lawful consumable products.’” Despite this broad language, exceptions often allow employers to consider such lawful conduct in employment decisions if:

1. doing so is related to a bona fide occupational requirement;
2. doing so is necessary to avoid a conflict of interest with the employer;
3. use of the product affects an employee’s ability to perform his job duties; and/or
4. the primary purpose of the organization is to discourage the use of the product at issue.

---

154. Id.
155. Id.
156. COLO. REV. STAT. ANN. § 24-34-402.5 (West 2013).
157. N.Y. LAB. LAW § 201-d (West 2013).
158. Burke & Roth, supra note 153.
159. See id. (discussing statutes in Illinois, Minnesota, Montana, Nevada, North Carolina, and Wisconsin that have adopted this language).
160. Id.
Most states’ lifestyle-discrimination laws regulate specific types of conduct, such as tobacco use. In fact, the American Civil Liberties Union (ACLU) reports that as early as 1988, six percent of employers were discriminating against off-duty smokers; moreover, the ACLU surmises that this figure has “almost certainly risen.” Other conduct protected by lifestyle-discrimination laws may include: marital status or sexual orientation; political activity or affiliation; and arrest record or certain minor criminal convictions.

Although an employer does not have the right to prohibit the use of social networks, employers might discipline employees for their misconduct on a social-networking site. When crafting a social-media policy, employers should first determine the scope of protections under their state’s laws. Arkansas does not currently have a lifestyle-discrimination statute. However, if employers may be subject to other states’ lifestyle-discrimination laws, they should check the applicable statutory exceptions. Assuming no exception applies, employers should treat discrimination based on these lifestyle characteristics the same as “discrimination based on other federal and state-protected characteristics.” Employers’ policies should address the protected lifestyle characteristics, and employers should investigate complaints about discrimination like they would investigate any other discrimination complaint.

161. Id.
163. Burke & Roth, supra note 153.
164. Social Networks Survey, supra note 2.
165. Burke & Roth, supra note 153.
166. Id.
167. Id.
168. Id.
B. Employer Responses

Employers have various methods for preventing social-media misuse by employees. Specifically, employers may claim: (1) breach of contract; (2) a violation of the Copyright Act; (3) a violation of harassment policy; and (4) a violation of a social-media policy. These theories allow employers to deter social-media misuse and prevent litigation.

1. Breach of Contract

Some employers may combat social-media misuse through employment contracts. Non-compete clauses may be especially useful. For example, in TEKsystems, Inc. v. Bolton, a technical-services and staffing firm sued a former employee for breach of his non-compete contract when the employee allegedly used information he obtained on the job to contact the employer’s current clients through networking sites such as CareerBuilder and LinkedIn. Although the employee claimed he made the connections after he left the firm, the court held the employee violated his contract because the firm’s success depended “overwhelmingly upon the ability of its employees to make and maintain personal connections with clients.” Furthermore, since the former employee was “instrumental in expanding the [firm’s] business,” the court granted the employer’s request for a permanent injunction and required the employee to abide by the non-compete contract for eighteen months. Social media has impacted many courts’ traditional geographic analysis of non-compete contracts; thus, employers should explicitly declare the importance of social media to their businesses and connect its use to attracting customers, making profits, and growing

---

169. See TEKsystems, Inc. v. Bolton, Civil Action No. RDB-08-3099, 2010 WL 447782, at *4-6 (D. Md. Feb. 4, 2010) (examining the scope of a “restrictive covenant” and requiring for enforcement that the covenant protects a legitimate business interest in a reasonable manner).
170. Id. at *2-3.
171. Id. at *3.
172. Id. at *6.
173. Id.
their businesses. If an employer can accomplish this, then the non-compete contract may be an effective response to an employee’s use of social-media to steal the employer’s clients.

2. The Copyright Act

Under the Copyright Act of 1976, work that employees prepare within the scope of their employment is “work made for hire.” Accordingly, an employer owns the copyright of such material. Employers may use this argument—rooted in principles of agency—to combat against employee theft and misappropriation conducted through social media.

From an intellectual property and a contractual perspective, actual user accounts offered by social-network sites appear to be the exclusive property of the sites, rather than the property of employee or employer users. Determination of ownership rights in the content posted by an employee, however, is an entirely different matter. One may determine ownership of social-media content by evaluating several factors, including the circumstances that imply ownership, an ownership agreement regarding social-media posts, and content entitled to copyright protection. Therefore, employers should proactively define their social-media rights.

In light of these considerations, Twitter provides a helpful example. Whether a “tweet” may qualify for copyright protection likely depends on a case-by-case analysis because each tweet is unique. “Although the ‘originality’ threshold is low under the law, [an employee’s] work must still embody some minimal level of creativity” to

---

178. See RESTATEMENT (THIRD) OF AGENCY § 1.01 (2006).
180. See id. at 52.
181. Id.
182. See id.
183. Id.
obtain ownership of the work—even in a 140 character tweet.\footnote{184} If content is not “original” and, therefore, not copyrightable, “no further examination as to whether the employer or the employee will own the copyright is necessary.”\footnote{185} An employer with a sound policy will retain ownership of this information.

In \textit{PhoneDog v. Kravitz}, the employer, PhoneDog, initiated a lawsuit against Noah Kravitz, a former employee, based on Kravitz's continued use of a PhoneDog Twitter account that contained a compilation of subscribers.\footnote{186} PhoneDog—an interactive, mobile-news web resource—encouraged its employees to use a variety of social-media sites, including Twitter, Facebook, and YouTube, to market its services.\footnote{187} Kravitz, while working for PhoneDog as a product reviewer and video blogger, “was given use of and maintained the Twitter Account ‘@PhoneDog_Noah’ (the ‘Account’).”\footnote{188}

As part of his employment, Kravitz submitted written and video content to PhoneDog, which PhoneDog transmitted to users through a number of mediums, including PhoneDog’s website and the Account.\footnote{189} Kravitz, on behalf of PhoneDog, accessed the Account with a password and used the Account to disperse information and to promote PhoneDog’s services to approximately 17,000 Twitter followers.\footnote{190} PhoneDog stated that “all @PhoneDog_Name twitter accounts used by its employees, as well as the passwords to such accounts, constitute[d] proprietary, confidential information.”\footnote{191}

When Kravitz ended his employment with PhoneDog in October 2010, PhoneDog requested that he stop using the Account.\footnote{192} “In response, Mr. Kravitz changed the Account handle to ‘@noahkravitz,’ and continue[d] to use

\footnote{185. Id.}
\footnote{186. No. C 11-03474 MEJ, 2011 WL 5415612, at *1 (N.D. Cal. Nov. 8, 2011).}
\footnote{187. Id.}
\footnote{188. Id.}
\footnote{189. Id.}
\footnote{190. Id.}
\footnote{191. \textit{PhoneDog}, 2011 WL 5415612, at *1.}
\footnote{192. Id.}
the Account.” Consequently, PhoneDog alleged it suffered at least $340,000 in damages. Based on these allegations, PhoneDog filed suit against Kravitz, asserting claims under California law for misappropriation of trade secrets, intentional interference with prospective economic advantage, negligent interference with prospective economic advantage, and conversion. PhoneDog eventually settled its claim, and Kravitz maintained sole custody of the Account.

3. Violation of Harassment Policy

Employers may be liable when their employees use social media to harass a co-worker by posting explicit or suggestive comments about the co-worker on a Facebook page, in a tweet, or in a blog post. Courts have provided guidance on employers’ responsibilities regarding these types of harassment issues, and the Equal Employment Opportunity Commission (EEOC) has developed extensive compliance information on such harassment. An employer may avoid liability in a harassment lawsuit if the court deems the employer’s handling of the workplace harassment reasonable. In determining the reasonableness of an employer’s reaction to harassment,

193. Id.
194. Id.
195. Id.
198. See Faragher v. City of Boca Raton, 524 U.S. 755, 807-08 (1998) (holding employer liable for harm because the employer failed to exercise reasonable care to prevent and correct promptly sexually harassing behavior by not disseminating its policy); see also Burlington Indus., Inc. v. Ellerth, 524 U.S. 742, 765-66 (1998) (holding that employee’s affirmative defense required showing of reasonable care to prevent and correct promptly any sexually harassing behavior and that employee unreasonably failed to take advantage of any preventive or corrective opportunities or to avoid harm otherwise).
courts consider whether: (1) the employer brought a “tangible employment action” against the harassing employee; (2) “the employer exercised reasonable care to prevent and correct promptly any harassing behavior”; and (3) “the employee unreasonably failed to take advantage of preventive or corrective opportunities provided by the employer or to avoid harm otherwise.”

Although this framework has worked in the past, the speed and ease with which harassment occurs through social media may complicate courts’ reasonableness determinations.

For employers, where a policy exists only in name, potential liability exists in fact. For example, if an employer has an express policy of monitoring its employees’ social-media use for harassment or of investigating employees through social-networking sites, but the employer fails to follow this policy, it may be liable to third parties for negligent-hiring or failure-to-investigate claims. Therefore, employers who monitor social-media use should proactively prevent harassing behavior and quickly discipline such behavior when it occurs.

4. Violation of Social-Media Policy

A clear social-media policy remains an employer’s best tool to prevent potential social-media misuse because policies provide more explicit parameters for employees and a starting place for courts to interpret social-media rights. Nonetheless, some employers refrain from enacting social-media policies, believing such policies improperly discourage employees’ social-media use. But even for these employers, the potential legal issues with employees’ social-media use warrants, at a minimum,
extending current communications policies to social media. 206

Employers should regulate the use of social media by amending current employee handbooks to dictate acceptable use of social-networking sites. 207 For social-media policies to work, employers, employees, and the court must understand the policies. 208 Again, courts construe confusing or ambiguous polices against the employer. 209 A coherent social-media policy is not overly broad or restrictive; it is respectful of employees’ privacy rights; and it is unambiguous. 210 Furthermore, a policy must not prohibit private employees from utilizing social media to engage in statutorily protected actions, and it must not prohibit public employees from exercising their constitutional rights. 211 The more specific a policy is, the more likely it will only prohibit unprotected actions. 212 If employers spend time proactively weighing the risks and benefits of using social media in their workplaces, they will set a desired social-media tone and establish policies better suited for their long-term needs. 213

An employer should strictly enforce any policies it implements. 214 A social-media policy that appears in an employer’s handbook may go unread and unheeded if the employer does not promote the policy. 215 In fact, in a 2009 study, twenty-three percent of surveyed employees stated

206. Id.
207. See Guard Publ’g Co., 351 N.L.R.B. 1110, 1114 (2007) (holding that employer’s policy prohibiting employees from using the e-mail system for “nonjob-related solicitations” did not violate section 158(a)(1) of the NLRA).
209. See id. at 397.
210. Telephone Interview with Adam S. Foreman, supra note 34.
211. See Guard Publ’g Co., 351 N.L.R.B. at 1110, 1114.
213. Telephone Interview with Adam S. Foreman, supra note 34.
215. Dexter, supra note 1, at 25.
that their employer did not have a social-media policy; eleven percent stated that their employer had a policy but admitted they did not know the policy; and twenty-four percent did not know whether a social-media policy existed in their workplace.\footnote{216} Based on these results, employers should require their employees to read and sign any policy issued.\footnote{217}

Moreover, discrepancies between the actual written policy and an employer’s day-to-day observance of the policy may cause significant problems when the employer defends claims arising from its actions against an employee’s misuse.\footnote{218} For example, where a policy addresses social-media harassment but does not discipline an employee’s harassing behavior, the employer may be liable for the harassment.\footnote{219} Even with these challenges, a social-media policy remains an employer’s best device because the impact of social media is increasing, and as a result, the issues are becoming more complicated.\footnote{220}

Nevertheless, many employers argue against creating social-media policies. These companies argue that a strict policy discourages employees from participating in social media.\footnote{221} If a company’s goal is to use or encourage social media, this worry is a roadblock.\footnote{222} Furthermore, others argue that strict policies strip authenticity from employees’ social-media use by removing the “personality” out of an employer’s brand.\footnote{223} An additional argument contends that too many rules become overwhelming and damage employee morale; therefore, employers may determine that the risks of a bureaucratic working environment outweigh

\footnote{217} Minehan, supra note 4, at 2.
\footnote{218} See Quon, 130 S. Ct. at 2629, 2931 (discussing the divergence between a supervisor’s statements and the official policy).
\footnote{219} See Heather Bussing, When Employers Are Liable for Harassment, HREXAMINER (June 24, 2012), http:www.hrexaminer.com/when-employers-are-liable-for-harassment.
\footnote{220} Telephone Interview with Adam S. Foreman, supra note 34.
\footnote{221} Kennedy, supra note 205.
\footnote{222} Id.
\footnote{223} Id.
the benefits of any social-media policy. Finally, companies without social-media policies argue that these policies erode the trust relationship between employers and employees. For many employers, the at-will relationship is sufficient. To these employers, if they cannot trust employees to use social media appropriately, then those employees should not work for them. But even these skeptical employers should not wholly ignore social-media issues. Instead of avoiding social-media policies, wary employers should revise current communication policies and educate employees on proper and effective social-media use. A social-media policy is not required to be an entirely new, delineated policy; rather, it may treat social media as just one of many forms of communication. Under this approach, employers should ensure that the policies for telephone, face-to-face, and e-mail communication apply evenly to social-media communication.

IV. PROPOSALS FOR A COHERENT SOCIAL-MEDIA POLICY

When deciding social-media cases, courts have looked at the employer’s proactive steps to specify its policy and to protect its information and image. Due to the tension between technology’s rapid progression and the slow development of the law, precedent provides little guidance for a declarative policy. Therefore, an employer’s best course of action is to consult with legal counsel to craft specific policies that clearly assert the employer’s rights regarding social-media use.

224. Id.
225. Id.
227. Kennedy, supra note 205.
228. Id.
229. Id.
231. Id.
232. Id. at 2-3.
To avoid enforceability issues, employers should craft social-media policies to meet particular needs. The key crafting consideration is the balancing of an employer’s legitimate interest in protecting its business against an employee’s right to privacy, both in relation to data and personal privacy. Specific steps employers should consider taking include: (A) addressing social-media use in well-defined and well-communicated policies; (B) actively managing social media; (C) defining violations; and (D) updating social-media-use agreements.

A. Addressing Social-Media Use in Policies

Employers can best safeguard their interests in social-media use through policy language that specifies how employees may appropriately use social-networking sites and the sanctions for non-compliance. This language should state that the employer monitors social-media use. Moreover, employers may include provisions concerning whether the employer or employee may create a social-media account for business marketing and branding; who has access to account settings and passwords; who may edit, add content, or comment on the employer account; examples of specific inappropriate social-media use; procedures to relinquish use of an account at the end of the employment period; and disciplinary actions enforced for misuse.

B. Actively Managing Social Media

One goal for a social-media policy is to establish an employer’s ownership rights to social media created and managed on its behalf. When an employee creates an account
account on an employer’s behalf and then leaves employment, the ownership of the created material will depend on several factors, including: (1) whether a contract governs such creations; (2) the name under which the employee created the account; and (3) what name the account holds out to the public. 239

For many employers, only employees who have been given permission should be allowed to create company social-media accounts. 240 If employers identify the scope of the social-media use, works created by the employee on behalf of the employer may be copyrightable and owned by the company. 241 Employers should be sure that, to the extent possible, they register all social-media accounts in the company’s name, not in an individual’s name. 242 Furthermore, employers should inform content-creating employees of restrictions, such as those enforced by the FTC. 243

Likewise, employees’ personal accounts should not include an employer’s name. While employers generally may not dictate or discriminate against off-duty conduct, they should separate themselves from such conduct. Employers should encourage employees to keep their personal lives at home and away from work resources. If employers are comfortable with setting a no-tolerance tone, they should inform employees that work resources are not available for personal social-media use. Otherwise, employers should inform employees that work resources used for social media are subject to monitoring.

Employers that use social media should dictate in their policies that the company’s social-media content is distinct and developed apart from an employee’s individual social-media personality. 244 Again, personal content should remain separate from anything that pertains to an

239. See Minehan, supra note 4, at 2.
243. Using Consumer Reports, supra note 95.
244. See Minehan, supra note 4, at 2.
Assigning to more than one person the task of communicating with customers and marketing via social media prevents one employee from dominating the social dialogue. By limiting work-related social-media use to individuals with marketing or public-relations duties, employers can more easily monitor social media, establish account ownership, and mitigate liability exposure. For example, where only an employer’s marketing department actively monitors social-media use, the hiring department can avoid claims of discrimination or retaliation based on social-media profiles.

C. Defining the Violations

Because the NLRB will strike a policy for being void or ambiguous, employers need clear, coherent policies. Moreover, because courts will construe ambiguity against the employer, the employer should consider how a reasonable person would interpret a clause. Next, the employer should inquire whether a particular clause will “chill” employees’ rights? By providing specific examples of both proper and improper social-media use, employers can better protect themselves and provide the courts with a starting point for analysis.

D. Updating Use Agreements

Employers should update policies in order to remain current with emerging technology and to acknowledge the progression of caselaw and administrative interpretation. Employers should remove irrelevant geographic limitations in non-compete contracts and strengthen duration restrictions.
V. CONCLUSION

Rapidly changing technology, the explosive growth of social media, and recent litigation illustrate the bottom line for employers—they need clear and concise social-media policies to which employees will consent. The advice given in *Sears Holdings*, *PhoneDog*, and *Eagle*, and statements from administrative agencies, illustrate the challenges of social media in the workplace. A written, enforceable agreement addressing the intricate employment, contract, privacy, and ownership-rights issues in social media reduces the risk of frustrating, flurried litigation. Through foresight, specificity, education, and proactivity, employers can harness the benefits of social media and mitigate the risks of expanding technology and new communication systems. This process starts, and hopefully ends, with a social-media policy.

*Bethany N. Whitfield*