Legal Implications of Employee Social Media Use

By Corey M. Dennis

Corey M. Dennis is an associate in the Boston office of Morrison Mahoney LLP, where he practices defense-side civil litigation

> "Bored Boston government workers are goofing off on Facebook and other popular social networking sites on taxpayer time, boasting of napping during meetings, playing 'Mafia Wars,' creating anagrams of their names and planning Halloween costumes… . 'Amy Derjue is going to sit in the [Boston City] Council meeting and nap,' she wrote on Facebook at 11:49 a.m. last Wednesday. And she was apparently eager to punch out [another] day, writing at 4:40 p.m.: '20 minutes and I am OUT. Gone. No longer present. Do not contact unless you want to drink, shop, or watch sporting events.'"[1]

I. Introduction

The use of social networking sites, also known as social media, is exploding. Currently, two-thirds of Americans use social media, including Facebook, Twitter, MySpace, Linkedin, Plaxo and other social and professional networking sites. Since 2007, use of social media has increased 230% percent. In addition, 43% of users are visiting these sites more than once a day.[2] Social networking websites allow members to create profiles that contain personal information (e.g., age, school attended, employer, gender, religion, musical interests, hobbies) and to share their profiles with other individuals known as their "friends."[3] These sites are now being used by employers and employees, both inside and outside the workplace.[4]

SixDegrees.com, the first recognizable social network site, launched in 1997. The site allowed users to create profiles, list their friends, and surf the friends' lists. The next major social networking website was Friendster, which launched in 2002. However, social networking websites did not hit the mainstream until 2003, when MySpace and LinkedIn (which is geared towards professionals) launched. Facebook was introduced as a Harvard-only social networking site in early 2004, but subsequently became accessible to all college students and later to high school students, professionals inside corporate networks, and, eventually, to everyone.[5] See below for a chart depicting this history.

SixDegrees.com	Friendster	LinkedIn MySpace	Facebook (limited)	YouTube	Facebook (everyone)
1997	2002	2003	2004	2005	2006

Employees' use of the internet, particularly social media, has resulted in productivity problems in the workplace.[6] For instance, employees often spend time reading and sending personal emails, bidding on auction sites, reading news and blogs, playing online games, and interacting with friends on social networking sites.[7]

1. Jessica Heslam and Dave Wedge, *Hacks hooked on Facebook: Some spend workday on social sites*, The Boston Herald (October 28, 2009).

2. Alison Diana, *Social Media Up 230% Since 2007*, InformationWeek (June 28, 2010), *available at* http://www.informationweek.com/news/software/web_services/showArticle.jhtml?articleID=225701600&subSection=News; *2010 Social Networking Report*, Experian Simmons, http://www.smrb.com/web/guest/2010-social-media-report; Teddy Wayne, *Social Networks Eclipse E-Mail,* The New York Times (May 17, 2009), *available at* http://www.nytimes.com/2009/05/18/ technology/internet/18drill.html?_r=1.

3. Richard Raysman and Peter Brown, *Behavioral Ads: Social Networks' Latest Legal Pitfall?,* Law Technology News (March 25, 2008), *available at* http://www.law.com/jsp/lawtechnologynews/ PubArticleLTN.jsp?id=900005506762; Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship, Social network sites: Definition, history, and scholarship*, J. Computer-Mediated Comm., 13(1), *available at* http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (defining social networking websites).

4. Molly DiBianca, *The [Many] Roles of Online Social Networks in the Workplace,* The Delaware Employment Law Blog (January 19, 2009), http://www.delawareemploymentlawblog.com/2009/02/ the_many_roles_of_online_socia.html. As of October 30, 2010, Facebook reports that it has "[m]ore than 500 million active users," 50% of which log on in any given day. Facebook "Press Room," http://www.facebook.com/press/info.php?statistics. "The fastest growing demographic is those 35 years old and older." *Id.; see also* Molly DiBianca, *The Number of Adults Who Use Online Social Networking Sites Is Skyrocketing*, The Delaware Employment Law Blog (January 19, 2009), http://www.delawareemploymentlawblog.com/2009/01/the_number_of_adults_who_use_o.html ("the number of adults who utilize these sites has quadrupled since 2005").

5. Boyd & Ellison, *supra* note 3.

6. Sharon Gaudin, *Study: Facebook use cuts productivity at work,* ComputerWorld (July 22, 2009), *available at* http://www.computerworld.com/s/ article/9135795/Study_Facebook_use_cuts_ productivity_at_work. However, at least one study has found that the use of social media at work, for short periods of time, can actually increase employee productivity. Miral Fahmy, *Facebook, YouTube at work make better employees: study,* Reuters (April 2, 2009), http://www.reuters.com/article/idUST RE5313G220090402.

7. *Web Browsing at Work*, Employee Privacy Rights, http://www.employeeprivacyrights.co.uk/web-browsing-work.html.

Given the rapid growth of social networking sites and the fact that users post personal information online using these sites, privacy has also become a major concern.[8] In fact, in September 2009, Facebook settled a class action over its controversial Beacon advertising program, which posted personal information about Facebook users, such as movies they were renting online, without their permission.[9] Facebook agreed to stop the program and contribute $6 million to "set up a non-profit foundation that will award grants to projects that "promote the cause of online privacy, safety and security."[10]

Not only is employee use of social media growing rapidly, but employers are also now using these tools in ways that span the entire employment relationship, from pre-employment (recruiting), to potential employment (screening), and then all the way through the employment relationship (monitoring), and termination.[11] "Numerous reports are appearing of job candidates not being hired and employees being fired because of information found about them on social networking sites. There's even a term for people who get fired for what they put on their web sites: 'dooced.' This comes from Dooce.com, the blog of Heather Armstrong, who was terminated after writing about her employer on her blog."[12] The use of social media by both employers and employees in each stage of the employment relationship—pre-employment, employment, and post-employment—and the legal implications of this use will be discussed below.

II. Pre-Employment Use of Social Media by Employers in the Hiring Process

Forty-five percent of employers now use social media to research applicants.[13] There have been "dozens of articles in recent months about employers using social networking sites such as MySpace and FaceBook to find personal information about job candidates including drinking habits, nudity, general sleaziness, and criminal behavior ranging from shoplifting to violent assaults."[14]

Whether employers should use social media in making their hiring decisions is up for debate. Some believe that "employers must make efforts to screen candidates before making their final hiring decision."[15] In fact, some commentators have even suggested that "an employer has a duty to mine blogs of potential and existing employees," and "an employer who does not search social networks for readily available information may be negligent in their hiring practices."[16]

The potential liability risks to employers that result from using social media to research applicants seem low. An applicant's invasion of privacy action would fail in many cases because while many applicants believe they have a reasonable expectation of privacy regarding their social networking activity, this is a difficult argument to support where the information on social networking sites is voluntarily disclosed and posted in the public domain.[17] Moreover, although a lawsuit could bring negative publicity, "short of issuing a subpoena to check browser records on an interviewer's computer, it could be very difficult to discover if an employer had checked on the candidate online."[18]

However, despite increased employer use of social networking sites, most experts advise employers against the practice for the following reasons.[19] First, there is "no way to verify the accuracy of the information that is posted on these sites, nor is there a way to confirm that the applicant actually posted such information."[20] Concerns about the accuracy of applicant information posted online are

8. Raysman and Brown, *supra* note 3 (noting privacy concerns); Amy Miller, *Facebook GC Tells Lawyers He's Looking for a Fight,* Law.com (Feb. 2, 2010), http://www.law.com/jsp/article.jsp?id=1202441887703&src=EMCEmail&et=editorial&bu=Law.com&pt=Law.com%20Newswire%20Update&cn=LAWCOM_NewswireUpdate_20100202&kw=Facebook%20GC%20Tells%20Lawyers%20He%27s%20Looking%20for%20a%20Fight&hbxlogin=1 (noting ambiguity with regard to law on social media user's privacy).

9. Tomio Geron, *Judge Approves Facebook's Privacy Settlement,* Wall St. J. (March 19, 2010), *available at* http://online.wsj.com/article/SB10001424052748703580904575131742105971382.html.

10. Zusha Elinson, *Facebook Privacy Settlement Hits Bumps*, Law.com (February 12, 2010), http://www.law.com/jsp/article.jsp?id=1202443234965&src=EMCEmail&et=editorial&bu=Law.com&pt=LAWCOM%20Newswire&cn=NW_20100212&kw=Facebook%20Privacy%20Settlement%20Hits%20Bumps; Geron, *supra* note 9.

11. Molly DiBianca, *The [Many] Roles of Online Social Networks in the Workplace,* The Delaware Employment Law Blog (January 19, 2009), http://www.delawareemploymentlawblog.com/2009/02/ the_many_roles_of_online_social.html.

12. LaJean Humphries, *The Impact of Social Networking Tools and Guidelines to Use Them*, LLRX.com (January 15, 2007), http://www.llrx.com/features/goodgoogle.htm.

13. Molly DiBianca, *New Statistics on Employers Using Social Media to Research Applicants*, The Delaware Employment Law Blog (September 9, 2009), http://www.delawareemploymentlawblog.com/2009/09/new_statistics_on_employers_us_1.html; *see also* Sheila Marikar, *After Years of Telling All, 20-Somethings Start to Clam Up*, ABC News (March 1, 2007), http://abcnews.go.com/US/print?id=2912364.

14. LaJean Humphries, *The Impact of Social Networking Tools and Guidelines to Use Them*, LLRX.com (January 15, 2007), http://www.llrx.com/features/goodgoogle.htm; *see also* Samantha L. Millier, *Note, The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 Ky. L.J. 541, 545 (2008) ("Facebook is well known to employers, and the network is commonly used to conduct 'background checks' on potential new hires.").

15. Molly DiBianca, *Top 10 Reasons Why Employers Should Screen Their Applicants*, The Delaware Employment Law Blog (August 11, 2008), http://www.delawareemploymentlawblog.com/2008/08/top_10_reasons_why_employers_s.html; *see also* Molly DiBianca, *How to Conduct Online Background Searches With Google*, The Delaware Employment Law Blog (August 18, 2008), http://www.delawareemploymentlawblog.com/2008/08/how_to_conduct_online_backgrou.html ("Especially where the job pool is largely college graduates, the internet can be a great tool for applicant screening."). This author argues that using social media to screen applicants provides employers with more information when they have limited access to information, eliminates the need for costly background checks, and helps to prevent resume fraud, bad hiring decisions, and workplace violence.

16. Jonathan Bick, *Lawful Mining of Blogs on Social Networks*, New Jersey Law Journal (February 19, 2009), http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202428377614&hbxlogin=1 ("Internet social networks provide employers with a low-cost, easy-to-use, high availability screening tool for job applicants.").

17. Ian Byrnside, *Note: Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants*, 10 Vand. J. Ent. & Tech. L. 445, 461 (2008); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) ("Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting.").

18. Elizabeth Millard, *Online Background Checks As social networking sites grow, so does the ability of employers to discriminate*, ABA Journal (January 2007), *available at* http://www.abajournal.com/magazine/next.

19. Carolyn Elefant, *Do Employers Using Facebook for Background Checks Face Legal Risks?,* Law.com Legal Blog Watch (March 11, 2008), http://legalblogwatch.typepad.com/legal_blog_watch/2008/03/do-employers-us.html.

20. Daniel A. Schwartz, *Using Social Networking Sites for Employment Screening; Is there a Right Answer?*, Connecticut Employment Law Blog (September 19, 2008), http://www.ctemploymentlawblog.com/2008/09/articles/hr-issues/using-social-networking-sites-for-employment-screening-is-there-a-right-answer.

valid, given that on social networking sites and blogs, destructive groups have published lies and doctored photographs of vulnerable individuals, sent damaging statements about victims to employers, and manipulated search engines to highlight those statements for business associates and clients to see.[21]

One of the primary risks associated with using social media to screen applicants is discrimination lawsuits. When viewing an applicant's social media profile, an employer may discover information identifying an applicant's disability, religion, age, national origin, race, sexual preference, or membership or other protected class.[22] While an employer's lack of awareness of the applicant's membership in a protected class may serve as a defense to a discrimination claim, such an argument would be unavailing where the employer has discovered this information by reviewing the applicant's online profile.[23]

In short, although reviewing an applicant's social networking site "may satisfy an employer's curiosity, the time-worn principles of checking references, conducting interviews and, if necessary, background screening, should typically satisfy most employer's need to hire the best candidate."[24] As explained by one commentator: "frankly, an employer's hiring decisions should come down to who is best qualified for the job; knowing that someone's favorite show is *Heroes* may be interesting, but irrelevant."[25]

Most job applicants are now aware that many employers investigate applicants using social media, and as a result, they modify their Facebook or MySpace privacy settings to shield their profiles from public view.[26] Some have suggested that employers can circumvent these privacy protections by asking employees to acquire access to applicants' profiles.[27] However, this is not advisable and could lead to liability.[28]

It has been suggested that, if an employer or recruiter chooses to use the Internet to research or screen applicants, an attorney should be consulted to develop a written policy and a fair and non-discriminatory procedures designed to locate information that is a valid predictor of job performance.[29] Job applicants should either remove all potentially negative information from online profiles, restrict privacy settings so that third-parties cannot view their profiles, or both.[30]

III. Use of Social Media During Employment—Employers' Risks

There are undoubtedly significant benefits to allowing employees to use social media. Notably, employers are beginning to find that social media is an effective and inexpensive marketing tool.[31]

Proponents of using social media to assist in hiring decisions respond that "concerns about the accuracy" of such information can be allayed by simply *asking* the candidate about whatever it is that the employer found that may acting as a barrier to employment." Molly DiBianca, *New Study Shows Increase in Online Applicant Screening*, The Delaware Employment Law Blog (September 18, 2008), http://www.delawareemploymentlawblog.com/2008/09/new_study_shows_increase_in_on.html ("Just as with criminal backgrounds, employers should not make a *per se* decision without first giving the candidate an opportunity to explain the results of the report and any circumstances surrounding the arrest and/or conviction. The same interactive discussion should occur if an employer finds something on the candidate's social-networking site that gives them concerns.").

21. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. Rev. 61, 64 (2009).

22. Schwartz, *supra* note 20 (noting that there are "several landmines employers need to avoid" when "using social networking sites as a screening device"); Daniel Abasolo, *Fired for Facebook: Employers should not look up Internet profiles*, The Battalion Online (June 28, 2006), http://media.www.thebatt.com/media/storage/paper657/news/2006/06/28/Opinion/Fired.For.Facebook-2118962.shtml (noting employer may obtain information regarding "an applicant's race, religion, sexual orientation or past sexual partners . . . at their discretion by researching an applicant or employee on Facebook or MySpace"); Les Rosen, *Caution!–Using Search Engines, MySpace or Facebook for Hiring Decisions May Be Hazardous to Your Business*, Employment Screening Resources (June 2008), http://www.esrcheck.com/articles/Caution-Using-Search-Engines-MySpace-or-Facebook-for-Hiring-Decisions-May-Be-Hazardous-to-Your-Business.php (noting problem of "Too Much Information").

23. Rivera Concepcion v. Puerto Rico, 682 F. Supp. 2d 164, 174-75 (D.P.R. 2010) ("Many courts have determined that a plaintiff cannot sustain a prima facie case of disability discrimination without showing that an employer had actual or constructive knowledge of the plaintiff's disability."); Welch v. Ciampa, 542 F.3d 927, 938 (1st Cir. 2008) (explaining public employee's First Amendment "political discrimination" claim requires a showing that employer had knowledge of employee's political affiliation); Hedberg v. Indiana Bell Telephone Co., Inc., 47 F.3d 928, 932 (7th Cir. 1995) ("an employer cannot be liable under the ADA for firing an employee when it indisputably had no knowledge of the disability").

24. Schwartz, *supra* note 20; *see also* Elefant, *supra* note 19 ("I think it's unlikely employers are going to learn a good deal of job-related information from a Facebook page they won't learn in the context of a well-run interview, so the potential benefit of doing this sort of search is outweighed by the potential risk.").

25. Schwartz, *supra* note 20; *see also* Byrnside, *supra* note 17, at 475 ("In all likelihood, most of the negative information on an applicant's social networking profile is irrelevant to job performance, and if the applicant believes this information to be private, it may be more beneficial to the employer to respect this expectation of privacy, whether or not it is reasonable."); Ashley Cerasaro, *Employers defy privacy by using Facebook*, Tennessee Journalist (April 8, 2008), http://tnjn.com/2008/apr/08/employers-defy-privacy-by-usin (explaining "information on Facebook not relevant to the job may be used inappropriately by employers to assess a candidate," and "'online background checks' are unfair and invasive"); George Lenard, *Employers Using Facebook for Background Checking, Part I,* George's Employment Blawg (December 5, 2006), http://www.employmentblawg.com/2006/employers-using-facebook-for-background-checking-part-i/ ("I would advise employers to cut applicants and employees some slack. You were once young too . . . Ask yourself how relevant the information creating the negative impression is to job performance.").

26. *See* Cerasaro, *supra* note 25 (explaining Facebook users are now utilizing one of the "multiple privacy settings" Facebook provides).

27. Jonathan Bick, *Lawful Mining of Blogs on Social Networks*, New Jersey Law Journal (February 19, 2009), http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202428377614&hbxlogin=1("Employers can access potential hires' social networking profiles in a variety of ways.").

28. Rosen, *supra* note 22 (explaining creating fake identities to attempt to investigate applicant or employee's use of social media "is overly intrusive and invades too deeply into private matters").

29. Rosen, *supra* note 22. For legal protection, employers should considering obtaining consent so that applicants are on notice that their web persona is fair game. *Id;* Molly DiBianca, *Are You Monitoring Your Employees' Facebook Pages?*, The Delaware Employment Law Blog (June 15, 2010), http://www.delawareemploymentlawblog.com/2010/06/are_you_monitoring_your_employ.html.

30. Rosen, *supra* note 22.

31. *See Workplace Blogging: The Good, The Bad and the Ugly*, Sherrard Kuzz LLP Client Alert (May 2005), available at http://www.sherrardkuzz.com/pdf/Workplace_Blogging.pdf; Stephen D. Lichtenstein & Jonathan J. Darrow, *Employment Termination for Employee Blogging: Number One Tech Trend for 2005 and Beyond, or a Recipe for Getting Dooced?*, 2006 UCLA J.L. Tech. 4 (2006), available at http://www.lawtechjournal.com/articles/2006/04_061117_lichtenstein_darrow.pdf; ("An increasing number of employers including Microsoft,

Additionally, a growing number of businesses, government organizations, and educational institutions are using blogs to manage and improve the flow of information among employees.[32] On the other hand, employees' use of social media may expose employers to liability.[33]

A. Employer's Duty to Monitor Employees' Internet Activity

Doe v. XYC Corp.[34] illustrates the potential liability exposure to employers resulting from employees' computer use. In *Doe*, the New Jersey Superior Court, Appellate Division, held that where an employer is aware that an employee is using a workplace computer to access pornography, the employer has a duty to investigate the employee's activities and to prevent unauthorized activity and harm to innocent third parties, and that the employee's privacy interest does not trump this duty.[35]

Jane Doe, on behalf of her ten-year old daughter, brought a negligence action against XYC Corp. claiming that XYC Corp. should be held liable for the activities of one of its employees ("Employee"), who was Jane's husband and the stepfather of Jill. Employee had used his workplace computer to access pornography and send nude photographs of Jill to a child porn site on numerous occasions. He was arrested following a search of his work space and work computer based on a search warrant.[36]

XYC Corp.'s IT Department had conducted limited investigations of Employee's computer use and had determined that he was visiting pornographic websites, including child pornography websites, and had reported the findings of these investigations to high-level management. However, although Employee's supervisor told him to stop his inappropriate computer usage on one occasion, he recommenced these activities shortly thereafter and was not prevented from continuing this usage.[37]

The court found that XYC Corp. had the ability to monitor Employee's internet activities and that he had no legitimate expectation of privacy that would prevent the company from accessing his computer to determine whether he was using it to view adult or child pornography. Accordingly, the court concluded that because XYC Corp. had knowledge that Employee was viewing child pornography on his computer, it had a duty to act by terminating Employee or reporting his activities to law enforcement authorities, or both.[38] This decision demonstrates that an employer may face civil liability where the employer has become aware of the employee's unauthorized computer use and a third party is harmed by that use.[39]

B. Employees' Defamation of Employers and the Communications Decency Act

Aside from the problems associated with employees conducting inappropriate or illegal activities using social media, there are other concerns. Social media users may post material that is protected by trademarks or copyrights to their sites and may post photographs of yet-to-be-released products.[40] Further, employees may disparage and defame their employers on anti-employer blogs or Facebook.[41] The rapid rise of anti-employer blogging is further compounded

Google, Sun Microsystems, General Motors, and Yahoo! provide blog sites for employees or encourage them to create their own blogs."); Carolyn Elefant, *From Small Tweets, Big Firm Clients Grow*, Legal Blog Watch (August 25, 2009), http://legalblogwatch.typepad.com/legal_blog_watch/2009/08/from-small-tweets-big-firm-clients-grow.html (noting "many large firm lawyers" are beginning to realize "big time benefits" in the form of business development from the use of social media).

32. William O'Shea, *Blogs in the Workplace*, The New York Times (September 14, 2003), available at http://www.nytimes.com/2003/07/07/technology/07NECO.html (noting private blogs "archive data that would have otherwise been lost" and may be used to quickly access such information).

33. *See* Thomas J. Benedict, *Internet Law—Employee Blogs Pose Potential Problems for Businesses*, Internet Business Law Services (March 6, 2007), http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1629 (explaining employers may be liable for "an employee's defamatory private blog on topics that fall within the scope of the employee's employment or within the employee's actual or apparent authority" or for "sexual harassment and hostile work environment claims based on an employee's private blogging activities, if a supervisor authors inappropriate comments about an employee or if the employer had knowledge that an employee authored harassing blogs about a co-employee"); *Can Workplace Policies Minimize Your Organization's Potential Risk from Employee Blogs?*, Jackson Lewis Legal Updates (February 8, 2006), http://www.jacksonlewis.com/legalupdates/article.cfm?aid=895 (noting blogging "may expose employers to charges of defamation or to liability for other unlawful speech or content that is later attributed to the employer").

34. 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005).

35. *Doe v. XYC Corp.,* 887 A.2d 1156, 1158 (N.J. Super. Ct. App. Div. 2005).

36. *Id*. at 126, 130.

37. *Id*. at 127-29.

38. *Id*. at 140.

39. William A. Herbert, *The Electronic Workplace: To Live Outside the Law You Must Be Honest*, 12 Empl. Rts. & Employ. Pol'y J. 49, 71-72 (2008), *available at* http://works.bepress.com/cgi/viewcontent.cgi?article=1003&context=william_herbert; *cf.* Curtis v. Citibank, *N.A.,* 70 Fed. Appx. 20, 22 (2d Cir. 2003) (holding the employees' hostile work environment claims failed because coworkers' "objectively offensive" "'Ebonics' email" could not "be imputed" to the employer, given that "no supervisors had any role in the incident," the employer "swiftly investigated the plaintiffs' complaint about the email," and "[w]ithin three weeks of [the employees'] complaint, [the employer] disciplined the employees who had sent or forwarded the email with termination or final warning, installed a banner on its email system warning against such abuses, and notified all of its employees of the incident, the disciplinary penalties given, and the company policy against offensive conduct").

40. Stephanie Armour, *Warning: Your clever little blog could get you fired*, USA Today (June 14, 2005), *available at* http://www.usatoday.com/money/workplace/2005-06-14-worker-blogs-usat_x.htm; *Can Workplace Policies Minimize Your Organization's Potential Risk from Employee Blogs?*, Jackson Lewis Legal Updates (February 8, 2006), http://www.jacksonlewis.com/legalupdates/article.cfm?aid=895 ("blogging raises significant challenges for employers concerned about the broadcast of trade secrets and confidential and insider information, disclosure of which may subject the company to liability under federal or state securities laws"). For example, "an associate product manager at Google" was fired in 2005 for blogging about "future potential products." Armour, *supra*.

41. Konrad Lee, *Anti-Employer Blogging: Employee Breach of the Duty of Loyalty and the Procedure for Allowing Discovery of a Blogger's Identity before Service of Process is Effected*, 2006 Duke L. & Tech. Rev. 2, 2 (2006); *Workplace Blogging: The Good, The Bad and the Ugly*, *supra* note 38 ("Disgruntled, disenfranchised, angry employees have much to say about their employers," and "blogged information carries with it enormous potential to harm the employer"); *cf.* Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1346, 1367 (2003) (holding employee who "sent as many as 200,000 e-mail messages to Intel employees" "criticizing Intel's employment practices to numerous current employees on Intel's electronic mail system" not liable for trespass to chattels). To prevail on a claim of defamation under Massachusetts law, a plaintiff must establish that the defendant was at fault for the publication of a false statement regarding the plaintiff, capable of damaging the plaintiff's reputation in the community, which either caused economic loss or is actionable without proof of economic loss. White v. Blue Cross & Blue Shield of Mass., 442 Mass. 64, 66 (2004). While a statement's truth is generally an absolute defense to a claim of libel (written defamation), a plaintiff may recover for libel under Massachusetts law when the statement is published with "actual malice." Noonan v. Staples, Inc., 556 F.3d 20, 26 (1st Cir. 2009).

by the fact that bloggers often post defamatory material anonymously[42] and Section 509 of the Communications Decency Act of 1996 (CDA) "immunizes providers of interactive computer services against liability arising from content created by third parties," such as blog postings from a third party on an employee's blog.[43] For instance, in *Dimeo v. Max*,[44] the plaintiff's defamation claim against a website operator was barred by that statute.

In *Dimeo*, Anthony DiMeo III, a blueberry farm heir and operator of the publicity firm Renamity, sued Tucker Max who used his website (www.tuckermax.com) to "share [his] adventures with the world." Max's Web site hosted a number of message boards, some of which contained disparaging statements about DiMeo stemming from a New Year's Eve party that had gone awry.[45] Renamity held the party at Le Jardin, a restaurant located in the Philadelphia Art Alliance gallery. Twice as many people appeared than were expected, and the alcohol and food ran out well before midnight. The guests became angry and destructive, and ultimately, two pieces of art were stolen from the museum. The police arrived shortly thereafter and dispersed the crowd.[46]

DiMeo filed an action in the Court of Common Pleas of Philadelphia County, Pennsylvania. He asserted claims of defamation and violation of 47 U.S.C. § 223(a)(1)(C), the Communications Act of 1934. Max removed the lawsuit to the U.S. District Court for the District of Pennsylvania.[47] The district court dismissed DiMeo's defamation claim, holding that it was barred by § 509 of the Communications Decency Act,[48] which provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider," and "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." [49] The court also dismissed the 47 U.S.C. § 223(a)(1)(c) claim because, among other things, that statute is a criminal statute that does not provide a private right of action.[50]

DiMeo appealed to the U.S. Court of Appeals for the Third Circuit, challenging the dismissal of his defamation claim.[51] The Third Circuit concluded that the requirements of the statute were satisfied because Max's website was an "interactive computer service" and the relevant website posts constituted information furnished by "third party information content providers." On that basis, the Third Circuit affirmed the dismissal of DiMeo's defamation claim.[52]

C. Social Media Use as Protected Activity Under Labor Laws

When monitoring employees' social media use, employers should be aware that such use may constitute protected, concerted activity under state and federal labor laws if the activity involves the promotion of common goals of a group of employees relating to wages, hours, or working conditions.[53] *Konop v. Hawaiian Airlines, Inc.*[54] illustrates this principle. In *Konop*, Robert Konop, a pilot for Hawaiian Airlines, Inc., created and maintained a website where he posted bulletins critical of his employer, its officers, and the incumbent union, Air Line Pilots Association ("ALPA"). Access to the website was limited to those who had a username and password. Pilots Gene Wong and James Gardner were given access.[55]

Konop programmed the website to allow access when a person entered the name of an eligible person, created a password, and clicked the "SUBMIT" button on the screen, indicating acceptance of the terms and conditions of use, which prohibited any member of Hawaiian's management from viewing the website and prohibited users from disclosing the website's contents to anyone else. Hawaiian vice president James Davis asked Wong, who had not yet accessed the website, for permission to use his name to access the website, and Wong agreed. Davis also logged in with using Gardner's name as well after Gardner had given him consent to do so. Davis later accessed the website on numerous occasions.[56]

Konop subsequently brought suit against Hawaiian alleging

42. *See* Doe v. Individuals, 561 F. Supp. 2d 249, 250-51 (D. Conn. 2008); Dimeo v. Max, 433 F. Supp. 2d 523, 524 (E.D. Pa. 2006); *see also* Brendan L. Smith, *Meet John Doe Internet defamation plaintiffs are itching for the chance,* ABA Journal (Jan. 1, 2010), http://www.abajournal.com/magazine/article/meet_john_doe ("Masked by the Web's anonymity, Internet users feel free to flame celebrities, blast politicians, or blow the whistle on employers for corporate misdeeds."); Richard Raysman and Peter Brown, *Online Defamation and Anonymous Defendants*, Law Technology News (February 10, 2010), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202443014665&Online_Defamation_and_Anonymous_Defendants (outlining "emerging standards courts employ before allowing a plaintiff to discover the identity of anonymous defendants in online defamation cases").

43. Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008); *see also* 47 U.S.C. § 230(c) (2010) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."); Darrow & Lichtenstein, *supra* note 31 ("Another potential major area of concern for the employer is where third parties post comments on the employee's blog that contain defamatory, obscene or pornographic material, violate the employer's legal rights or interests, or constitute an invasion of the employer's privacy."). Some have suggested that, given courts' interpretations of the CDA and the number of people now communicating over the Internet, "traditional concepts of defamation law may indeed be dead." Jonathan D. Frieden, *The CDA Has Killed Traditional Concepts of Defamation Law*, E-Commerce Law (August 23, 2006), http://www.ecommercelaw.typepad.com/ecommerce_law/2006/08/the_cda_has_kil.html.

44. 433 F. Supp. 2d 523 (E.D. Pa. 2006).

45. *Id.* at 524-26.

46. *Id.* at 525.

47. *Id.* at 527.

48. *Id.* at 531.

49. 47 U.S.C. §§ 230(c)(1), (e)(3) (2010).

50. *Dimeo,* 433 F. Supp. 2d at 531-32.

51. DiMeo v. Max, 248 Fed. Appx. 280, 281 (3rd Cir. 2007).

52. *Id.* at 281-82.

53. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); *see also* 29 U.S.C. § 157 ("[e]mployees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection"); *In re St. Josephs Hosp.,* 337 NLRB 94, 94 (2001) (holding hospital "violated Section 8(a)(1) of the [NLRA] by discriminatorily prohibiting [a nurse] from displaying a union-related computer screensaver message on a computer at her workstation and Section 8(a)(3) and (1) by issuing a warning to [her] for displaying such a message"); *Timekeeping Systems, Inc.,* 323 NLRB 244, 247, 250 (1997) (holding employee's "e-mailings clearly constituted 'concerted" activity'" and employer "violated Section 8(a)(1) of the [NLRA]" "[b]y discharging" the employee).

54. 302 F.3d 868 (9th Cir. 2002).

55. *Id.* at 872-73.

56. *Id.*

57. *Id.* at 873.

58. *Id.*

59. *Id.* at 866.

60. 18 U.S.C. § 2511(1)(a) (2010).

61. *Konop,* 302 F.3d at 876-79.

that Hawaiian viewed his secure website without authorization, disclosed the contents of that website, and took other related actions in violation of the federal Wiretap Act (18 U.S.C. § 2511(1)(a)), the Stored Communications Act (18 U.S.C. § 2701(a)(1)), and the Railway Labor Act (45 U.S.C. §§ 151-188), which governs labor relations in the railway and airline industries and is interpreted in a manner similar to that of the National Labor Relations Act. Konop also alleged several state tort claims.[57] The district court granted summary judgment against Konop on all claims, except his retaliation claim under the Railway Labor Act, on which judgment was entered against him following a bench trial. Konop appealed to the U.S. Court of Appeals for the Ninth Circuit on all claims, except on those brought under state tort law.[58]

The Ninth Circuit first examined Konop's claim that Hawaiian had violated the federal Wiretap Act,[59] which makes it an offense to "intentionally intercept [ ] … any wire, oral, or electronic communication."[60] The court concluded that, although Konop's website fit the definition of "electronic communication," the Wiretap Act prohibits only "interceptions" of electronic communications, and the term "intercept" is narrowly construed.[61] Since Konop had previously transmitted electronic documents to a server, where the documents were already stored, no "interception" took place. Therefore, because Davis' conduct did not constitute an "interception" of an electronic communication in violation of the Wiretap Act, the Ninth Circuit affirmed the district court's grant of summary judgment against Konop on his Wiretap Act claim.[62]

The court next considered Konop's claim that Hawaiian violated the Stored Communications Act (SCA),[63] which makes it an offense to "intentionally access[ ] without authorization a facility through which an electronic communication service is provided … and thereby obtain[ ] … access to a wire or electronic communication while it is in electronic storage in such system."[64] The SCA excludes from liability "conduct authorized ... by a user of that service with respect to a communication of or intended for that user.[65] The district court granted summary judgment to Hawaiian on the SCA claim, finding that this exception applied because Wong and Gardner consented to Davis' use of Konop's website. However, the Ninth Circuit concluded that the plain language of § 2701(c)(2) indicates that only a "user" of the service can authorize a third party's access to the communication; the statute defines "user" as one who uses the service and is duly authorized to do so; there was no evidence in the record that Wong ever used Konop's website; and the district court did not make any findings on whether Wong and Gardner actually used Konop's website. Therefore, the Court reversed the district court's grant of summary judgment to Hawaiian on Konop's SCA claim.[66]

Next, the court examined whether the district court had properly granted summary judgment on Konop's three claims under the Railway Labor Act (RLA). Given that Konop's website publication vigorously criticized Hawaiian management and its proposal for wage concessions in the existing collective bargaining agreement, it was clear that Konop's website publication would have ordinarily constituted protected union organizing activity under the RLA. However, Hawaiian argued that Konop forfeited any protection he would otherwise enjoy because his website's articles contained malicious, defamatory and insulting material known to be false.[67] Nevertheless, the court concluded that Konop's statement that Bruce Nobles (Hawaiian's President) did his "dirty work … like the Nazis during World War II" and his statement that a "Soviet Negotiating Style" was essential to Nobles' "Plan" were simply "rhetorical hyperbole" protected by federal labor laws; his statements commenting on Nobles' competence and people skills were opinions also protected by federal labor laws; and his statement that Nobles was "suspected of fraud" was protected by federal law labor because there was no evidence that he published it with knowledge of its falsity or with reckless disregard for the truth.[68]

Konop alleged that Hawaiian violated the RLA by: (1) interfering with his organizing efforts by accessing his website under false pretenses; (2) wrongfully supporting one labor group in favor of another by informing the opposing labor faction of the website's contents; (3) engaging in coercion and intimidation by threatening to file a defamation suit against Konop based on statements on the website. With regard to Konop's first claim, the court noted that, absent a legitimate justification, employers are generally prohibited from engaging in surveillance of union organizing activities. Because Davis had accessed Konop's website and monitored private union organizing activities, there were triable issues of fact regarding whether Hawaiian interfered with Konop's union organizing activity in violation of the RLA by accessing Konop's website.[69]

With regard to Konop's claim that Nobles wrongfully supported an opposing labor union, the court explained that there was evidence indicating that Nobles disclosed the contents of the website to the opposing union, and Nobles effectively conceded that he interceded to help ensure that an opposing union faction (which favored ratification of the concessionary contract) would prevail over Konop's faction (which opposed the agreement). In Konop's third RLA claim, he alleged that Nobles engaged in unlawful coercion and intimidation by threatening to file a defamation suit against Konop based on statements on Konop's website. Such conduct may, under appropriate circumstances, violate the RLA. The court concluded that, given that there was evidence that Nobles threatened to sue Konop for defamation, there was a triable issue of fact on this issue. Accordingly, the Ninth Circuit reversed the district court's granting of summary judgment on Konop's RLA claims.[70]

Thus, Konop makes clear that an employee's secure web page, which criticizes management, may constitute protected organizational activity under the Railway Labor Act or the National Labor Relations Act.[71] In fact, the Hartford regional office of the National Labor Relations Board (NLRB) recently lodged a complaint against American Medical Response of Connecticut, Inc., alleging that the ambulance service illegally terminated an employee, Dawnmarie Souza, for posting negative comments about her supervisor on her personal Facebook page and wrongfully denying her union representation during an investigatory interview.[72]

62. *Id.* at 878-79.
63. *Id.* at 879.
64. 18 U.S.C. § 2701(a)(1) (2010).
65. 18 U.S.C. § 2701(c)(2) (2010).
66. *Konop,* 302 F.3d at 880.
67. *Id.* at 881-82.
68. *Id.* at 882-83.
69. *Id.* at 884.
70. *Id.* at 885-86.
71. *Id.* at 882.
72. *See* National Labor Relations Board Press Release, *Complaint alleges Connecticut company illegally fired employee over Facebook comments* (Nov. 2, 2010),

D. Employer Policies Regarding Social Media Use

Because blogs and other social media devices can be dangerous if left unregulated and unmonitored, commentators suggest that it is necessary for employers to devise effective social media use policies.[73] To reduce the likelihood of liability for invasion of privacy or for claims under the Stored Communications Act (SCA), the policy should state that computer access may be monitored, searched, or blocked.[74] In addition, the policy should prohibit the disclosure of confidential information regarding the company, its customers, and its employees, as well as the use of company logos and trademarks without written consent.

When developing social media use policies, employers should keep in mind that federal and state laws may prohibit them from taking adverse employment actions against employees for social media use in certain circumstances.[75] For example, some states, such as New York and California, have laws that prohibit employers from considering off-duty conduct when making an adverse employment decision.[76] However, most states, including Massachusetts, have no such laws.[77]

Additionally, many states have laws prohibiting employers from discriminating against employees based on their political activities or their use of tobacco products outside the course of employment.[78] In Connecticut, employers who engage in any type of "electronic monitoring" must give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur.[79] Further, public employers should keep in mind that they must not infringe on their employees' constitutional rights, including freedom of speech rights, when monitoring employees.[80]

IV. Post-Employment Risks—Employee Lawsuits

Employers are increasingly terminating employees due to their unacceptable social media use, and it inevitable that lawsuits based on these terminations will become more common in the future.[81] The most viable claims for employee discharged in such circumstances are wrongful discharge claims, First Amendment claims, invasion of privacy claims, and claims under the Stored Communications Act.

A. Wrongful Discharge Claims

The vast majority of states, including Massachusetts, follow the "basic common law rule governing employment," the "employment-at-will doctrine," under which employers are free to "discharge or retain employees at will for good cause or for no cause, or even for bad cause without thereby being guilty of an unlawful act."[82] However, virtually every state, including Massachusetts, has created "judicial exceptions to the employment-at-will doctrine during the past three decades," including the public policy exception, under which a terminated employee can bring an action for wrongful discharge.[83]

available at http://www.nlrb.gov/shared_files/Press%20Releases/2010/R-2794.pdf; Jenna Greene, NLRB Sues Company for Firing Worker Over Facebook Post, The National Law Journal (Nov. 8, 2010), *available at* http://www.law.com/jsp/article.jsp?id=1202474521710&rss=newswire.

73. *Workplace Blogging: The Good, The Bad and the Ugly*, *supra* note 38.

74. *See* Haynes v. Office of the AG, 298 F. Supp. 2d 1154, 1162 (D. Kan. 2003) (explaining policy providing that "[t]here shall be no expectation of privacy using this system" "has considerable significance"). However, as noted below, an employer may be liable under the SCA), 18 U.S.C. §§ 2701-11, for accessing information on an employee's personal electronic communications account without authorization.

75. *See* Christine E. Howard, *Emerging Technology and Employee Privacy: Symposium: Invasion of Privacy Liability in the Electronic Workplace: A Lawyer's Perspective*, 25 Hofstra Lab. & Emp. L.J. 511 (2008) ("A prudent blogging policy should be reviewed for compliance with state law and compatibility with company goals and objectives.").

76. Cal. Lab. Code § 96(k) (prohibiting employers from demoting, suspending, or discharging employees "for lawful conduct occurring during nonworking hours away from the employer's premises"); N.Y. Labor Law § 201-d (prohibiting employers, generally, from discriminating against employees for engaging in political activities, the legal use of consumable products, legal recreational activities, or membership in a union).

77. *See* French v. UPS, 2 F. Supp. 2d 128, 131 (D. Mass. 1998) (holding "the company's questioning [of the employee] about facts" regarding his off-duty "violent rage" due to intoxication "amounted, at most, to a *de minimis* intrusion into [the employee's] privacy, not actionable under" the Massachusetts invasion of privacy statute); *see also* Molly DiBianca, *Terminating Employees for Off-Duty Conduct*, The Delaware Employment Law Blog (October 20, 2008) (explaining that "in most states," "[e]mployers can terminate employees for what the employees do in their personal, non-working time").

78. *See* Cal. Lab. Code §§ 1101-1102 (prohibiting employers from adopting rules, regulations, or policies concerning the political activities or affiliations of their employees and from coercing or influencing employees' political activities by means of threat of discharge or loss of employment); *cf.* Conn. Gen. Stat. § 31-40s (prohibiting employers from discriminating against employees who smoke or use tobacco outside the course of employment); Conn. Gen. Stat. § 31-51q (prohibiting employers from discriminating against an employee for exercising his or her First Amendment rights, provided that the employee's activity does not substantially or materially interfere with the employee's bona fide job performance or the working relationship between the employee and the employer); Conn. Gen. Stat. §§ 2-3a and 31-51l (prohibiting employers of 25 or more employees from discriminating against employees based on certain political activities); N.H. R.S.A. 275:37-a (providing that employers may not prohibit employees from using tobacco products outside the course of employment).

79. Conn. Gen. Stat. § 31-48d. However, an employer may conduct monitoring without giving prior written notice if: (1) the employer has reasonable grounds to believe that employees are engaged in conduct that violates the law (or the legal rights of the employer/employees) or creates a hostile work environment; (2) and electronic monitoring may produce evidence of this misconduct. *Id.* A poster, conspicuously displayed, satisfies the notice requirement. *Id.*

80. *See infra* text associated with notes 93-123 (regarding public employees' First Amendment claims).

81. DiBianca, *supra* note 4; Armour, *supra* note 47 ("Delta Air Lines, Google and other major companies are firing and disciplining employees for what they say about work on their blogs."); Darrow & Lichtenstein, *supra* note 31 ("In recent years, several employee terminations for information contained in the employee's blog have received national attention.").

82. Rafael Gely & Leonard Bierman, *Social Isolation and American Workers: Employee Blogging and Legal Reform*, 20 Harv. J. Law & Tec. 288, 315 (2007); *see also* Upton v. JWP Businessland, 425 Mass. 756, 757 (1997) ("The general rule is that an at-will employee may be terminated at any time for any reason or for no reason at all."). "To date, only Montana has statutorily altered the at-will doctrine. The Montana Wrongful Discharge from Employment Act gives all employees in the state protection from discharge without 'just cause.'" Gely & Bierman, *supra.* The doctrine is "rooted in laissez faire socioeconomic values of nineteenth century capitalism," but whether it is "appropriate in a modern economy is the subject of ongoing debate in academic and legislative circles." Scott C. Moriearty et al., 45 Massachusetts Practice: Employment Law § 2.1 & n.3 (2d ed. 2003) (citing numerous sources). For a history of the development of the employment-at-will rule, see Jay M. Feinman, *The Development of the Employment At Will Rule*, 20 Amer. J. of Legal Hist. 118 (1976).

83. Gely & Bierman, *supra* note 82, at 315 (2007); *see also* Upton v. JWP Businessland, 425 Mass. 756, 757 (1997) ("Liability may be imposed on an employer, however, if an at-will employee is terminated for a reason that violates

The public policy exception "makes redress available to employees who are terminated for asserting a legal right (e.g., filing a workers' compensation claim), for doing what the law requires (e.g., serving on a jury), or for refusing to disobey the law (e.g., refusing to commit perjury)."[84] Additionally, "a personnel manual can be shown to form the basis of an express or an implied contract."[85] Employees who are discharged for using social media may assert these legal theories in an attempt to recover from their employers.[86] *Goldstein v. PFPC Worldwide, Inc.*[87] serves as an example of this scenario.

In *Goldstein*, the plaintiff, Daniel Goldstein, was an at-will employee of PFPC, Inc. He started as a customer service representative with the company, but at the time of his discharge, he was paid approximately $190,000 as Vice President of Client Services and Sales. In August 1999, he entered into a "Stay Bonus Agreement" with PFPC that provided that he would be paid a "Stay Bonus" in the amount of $30,000 if he was continuously employed by PFPC until December 1, 2001, or if he was terminated without cause prior to that date. "For cause" termination was defined in the Stay Bonus Agreement to include violations of PFPC's policies, such as its Code of Ethics. The agreement specifically stated that it did not change the at-will nature of Mr. Goldstein's employment with PFPC.[88]

PFPC operated under a written Code of Ethics containing an Electronic Media Policy that prohibited the sending of "articles, jokes, stories, chain letters or other items of personal interest," prohibited employees from using PFPC's e-mail "for any purpose unrelated to an employee's job duties," prohibited using e-mail to communicate "offensive, harassing, pornographic or other inappropriate material" and forewarned employees that violations of the Code of Ethics and Electronic Media Policy could result in termination of employment. In August 2001, PFPC investigated e-mail usage at the site where Goldstein worked and determined that he sent at least 18 e-mails that violated the Electronic Media Policy on the company's system. One of those emails, which was sent to prospective client, included the words "prohibited" and an attached photo of a woman with her breasts exposed. Goldstein was terminated on October 16, 2001 for violating the company's Electronic Media Policy.[89]

Goldstein filed an action in the Massachusetts Superior Court, bringing claims for wrongful termination, breach of contract, defamation, breach of the duty of good faith and fair dealing, interference with advantageous business relations, fraudulent misrepresentation, promissory estoppel, and quantum meruit. PFPC filed a motion for summary judgment on all counts. The court granted PFPC's motion on the last 7 counts and simply adopted the reasoning from PFPC's arguments in its summary judgment memorandum and reply brief. However, the court engaged in a more extensive analysis of Goldstein's wrongful termination claim.[90]

Goldstein argued that he was wrongfully terminated in violation of the implied covenant of good faith and fair dealing and in violation of a clearly established public policy because PFPC terminated him to deprive him of the $30,000 retention bonus that he was eligible to receive under his Stay Bonus Agreement. The court held that the covenant of good faith and fair dealing was not violated because, given that the agreement specifically provided that Goldstein would not be eligible for the $30,000 retention bonus unless he continued employment with PFPC until December 1, 2001, there had been no deprivation of compensation for past services. The court further noted that the internal administration and functioning of an organization cannot form the basis for a public policy exception to the at-will employment rule and that Goldstein failed to point to any public policy that was violated.[91]

This decision demonstrates the difficulty employees face when bringing a wrongful termination claim following a termination for inappropriate social media use. Nevertheless, employers should take care to avoid acting in a discriminatory way when discharging employees for their social networking activities.[92]

B. First Amendment Claims

Under the state action doctrine, public employers must not interfere with employees' constitutional rights by, for example, terminating them for exercising their First Amendment right to speak out regarding matters of public concern.[93] However, to prevail on a 42 U.S.C. § 1983 for a termination in violation of the First Amendment, an employee must demonstrate a causal connection between the protected activity and the employer's adverse action.[94] Moreover, the employee must show that his interest in commenting upon those matters outweighed the government employer's interests in the

a clearly established public policy.").

84. Upton v. JWP Businessland, 425 Mass. 756, 757 (1997). The Massachusetts Supreme Judicial Court has also held that an employer's termination of its employee due to the employee's enforcement of safety laws, refusal to give false testimony against a coworker in a criminal trial, reporting of a suspected criminal wrongdoing occurring within the company, or cooperation with a law enforcement agency's investigation of an employer "directly contradict well-defined public policies of the Commonwealth." *See id.* However, the court has held that an employee's "participation in shareholder derivative suit," "failure to comply with [the] employer's internal policy of mandatory drug testing," or reporting "problems to high-ranking officials within [a] hospital organization" do not "do not warrant recovery by an at-will employee." *Id.* at 758.

85. Jackson v. Action for Boston Community Dev., Inc., 403 Mass. 8, 14 (1988); *see also* O'Brien v. New England Tel. & Tel. Co., 422 Mass. 686, 691-92 (1996); Gaudio v. Griffin Health Servs. Corp., 249 Conn. 523, 532 (1999) ("statements in an employer's personnel manual may . . . under appropriate circumstances . . . give rise to an express or implied contract between employer and employee"). However, "employers can protect themselves against employee contract claims based on statements made in personnel manuals by following either (or both) of two simple procedures: (1) eschewing language that could reasonably be construed as a basis for a contractual promise; and/or (2) including appropriate disclaimers of the intention to contract." *Gaudio,* 249 Conn. at 535 (internal quotation marks omitted).

86. *See* Darrow & Lichtenstein, *supra* note 31 (describing various theories of liability).

87. 17 Mass. L. Rep. 333, 2004 WL 389107 (Mass. Super. Ct. February 19, 2004).

88. *Goldstein,* 2004 WL 389107, at *1.

89. *Id.* at *3.

90. *Id.* at *3-4.

91. *Id.*

92. *See* Williams v. Wells Fargo Fin. Acceptance, 564 F. Supp. 2d 441, 443 (E.D. Pa. 2008) (holding employer may be liable under employment discrimination law for "discriminat[ing] against [an employee] on the basis of his race when it terminated his employment because he sent emails that contained sexually suggestive and otherwise inappropriate jokes or picture attachments in violation of its Information Security and Sexual Harassment policies").

93. *See* Darrow & Lichtenstein, *supra* note 31 ("the First Amendment only protects individual freedom of speech from government action, not from the acts of private employers").

94. *See* Spanierman v. Hughes, 576 F. Supp. 2d 292, 310, 313 (D. Conn. 2008). The Civil Rights Act of 1871, 42 U.S.C. § 1983, provides plaintiffs with a civil remedy against state or local government officials who deprive them of rights guaranteed by the U.S. Constitution or federal statutes.

efficient performance of its public services.[95]

Two cases involving the termination of a public employee due to inappropriate social media usage, *Spanierman v. Hughes*[96] and *Curran v. Cousins,*[97] demonstrate these principles. In *Spanierman,* the plaintiff, Jeffrey Spanierman, was hired by the State of Connecticut's Department of Education (DOE) in January 2003 to be an English teacher at Emmett O'Brien High School in Ansonia, Connecticut. In 2005, Spanierman opened a MySpace account, creating several different profiles, which he used to communicate with students about homework, to learn more about the students so he could relate to them better, and to conduct casual, non-school related discussions. One of his accounts was called "Mr. Spiderman."[98]

In the fall of 2005, Elizabeth Michaud, a guidance counselor at Emmett O'Brien High School, received several student complaints about the "Mr. Spiderman" page. She reviewed it and was disturbed when she saw that there were pictures of naked men with inappropriate comments beneath them and casual conversations with students about non-school-related topics, such as their weekend activities and personal problems. She then informed Spanierman that some of the pictures on his "Mr. Spiderman" profile page were inappropriate, and Spanierman deactivated the profile page.[99] He later created a nearly MySpace profile page called "Apollo68," of which Michaud also became aware. Michaud reported the situation to Lisa Hylwa, the principal of Emmett O'Brien, who placed Spanierman on administrative leave with pay so that an investigation could be conducted. Spanierman deactivated the "Apollo68" profile during this time.[100]

A subsequent investigation of Spanierman's MySpace profiles revealed that he was "friends" with several Emmett O'Brien students and that he had posted comments on their MySpace profile pages. In January 2006, Ferraiolo met with Spanierman, his union representative, and Hylwa to discuss his MySpace activities. In March 2006, Hylwa sent him a letter explaining that he had exercised poor judgment as a teacher, and Anne Druzolowski, Assistant Superintendent of the Connecticut Technical High School system, sent him a letter informing him that the DOE would not renew his contract for the 2006-2007 school year.[101] Spanierman requested a hearing. At the hearing, Abigail L. Hughes, Superintendent of the Connecticut Technical High School system, agreed with Druzolowski's decision not to renew Spanierman's contract. Spanierman received his pay and benefits until the end of the summer of 2006, when his contract with the DOE for the 2005-2006 school year expired.[102]

Spanierman subsequently brought a 42 U.S.C. § 1983 action against Hughes, Druzolowski, and Hylwa in their individual and official capacities alleging that, by failing to renew his contract, they violated his First Amendment rights to freedom of speech and freedom of association as well as his Fourteenth Amendment rights to procedural due process, substantive due process, and equal protection.[103] The Defendants filed a motion for summary judgment on all claims.

The court found that Spanierman's procedural due process claim failed because, although states may not deprive any person of the Fourteenth Amendment's protection of liberty and property, Spanierman did not have a protected property interest in his employment at Emmett O'Brien: since he did not have tenure, the DOE was free to terminate him, even without just cause. Similarly, Spanierman's substantive due process claim failed because he had no constitutionally-protected property interest in the renewal of his employment contract with the DOE. Therefore, the court granted summary judgment on both claims.[104]

The court analyzed Spanierman's equal protection claim as two separate claims: one based on the *Olech* "Class-of-One" standard and the other based on the *LeClair* "Selective Prosecution" standard.[105] The Court granted summary judgment on both equal protection claims because neither theory applies in the public employment context.[106]

The court then examined Spanierman's claim that the Defendants retaliated against him because he exercised his freedom of speech and freedom of association rights.[107] The court noted that a public employee's statements made pursuant to his or her official duties are not protected by the First Amendment, but that Spanierman was not acting pursuant to his responsibilities as a teacher. The court then analyzed the elements of Spanierman's First Amendment retaliation claims.[108] The court found that, while the vast majority of the contents of Spanierman's MySpace profile did not touch on matters of public concern, it did contain a poem Spanierman had written in opposition to the Iraq war, which was a political statement that constituted protected speech. Because there was no question that Spanierman suffered an adverse employment action, the issue became whether there was a causal connection between his poem and the decision to not renew his employment contract.[109]

The court found that Spanierman failed to establish the necessary causal connection because there was no evidence of retaliatory animus or that his poem played any part in the decision to not renew his employment contract. Moreover, the evidence indicated that the disruptiveness of Spanierman's speech outweighed its value. For example, Spanierman made a facetious threat about detention to a student on MySpace and had a discussion with a student about "getting any" (presumably sex) with another student. Students also complained that his MySpace comments made them

95. Curran v. Cousins, 509 F.3d 36, 47, 50 (1st Cir. 2007).

96. 576 F. Supp. 2d 292 (D. Conn. 2008).

97. 509 F.3d 36, 47 (1st Cir. 2007).

98. *Spanierman*, 576 F. Supp. 2d at 297-98.

99. *Id.* at 298.

100. *Id.* at 298-99.

101. *Id.* at 299.

102. *Id.*

103. *Id.* "[Section] 1983 'is not itself a source of substantive rights,' but merely provides 'a method for vindicating federal rights elsewhere conferred.'" *Id.* "To prevail on a § 1983 claim, a plaintiff must establish that a person acting under color of state law deprived him of a federal right." *Id.*

104. *Id.* at 300-04.

105. *Id.* at 304-08; *see also* Village of Willowbrook v. Olech, 528 U.S. 562, 564 (2000); LeClair v. Saunders, 627 F.2d 606, 609-10 (2d Cir.1980). A successful class-of-one equal protection claim can be brought "where the plaintiff alleges that [ ]he has been intentionally treated differently from others similarly situated and that there is no rational basis for the difference in treatment." *Spanierman,* 576 F. Supp. 2d at 305. A selective prosecution claim requires a showing: (1) that the plaintiff was treated differently from other similarly situated individuals; and (2) that such differential treatment was based on impermissible considerations such as race, religion, intent to inhibit or punish the exercise of constitutional rights, or malicious or bad faith intent to injure a person. *Id.* at 306.

106. *Id.* at 306-07.

107. *Id.* at 308.

108. *Id.*

109. *Id.* at 310-11.

feel uncomfortable.[110]

With regard to Spanierman's freedom of association claim, the court noted that, given that MySpace is a medium through which people meet and have contact with other people, it is doubtful that it would be considered an "organization" itself for the purposes of a First Amendment claim analysis, a threshold requirement for such a claim. However, even if it were, there was no evidence that MySpace, as an organization, purported to speak out on matters of public concern or that there was a causal connection between the expressive association and the adverse employment action in this case. Accordingly, the court granted summary judgment on both of Spanierman's First Amendment claims.[111]

As is likely to be the case in most terminations for social media usage, almost none of Spanierman's speech touched upon matters of public concern. However, even where a public employee's speech touches upon matters of public concern, his First Amendment claim will not prevail if the employer can demonstrate an adequate justification for terminating him, as is evident from *Curran v. Cousins*.[112] In *Curran,* the plaintiff, Joseph Curran worked as a corrections officer with the Essex County, Massachusetts Sheriff's Department. In 1996, Frank G. Cousins, Jr. was appointed Sheriff of Essex County by the governor of Massachusetts. The following year, the Essex County Correctional Officers Association (the "union") was formed. In 2004, Cousins ran for re-election as Sheriff, and the union took a strong public position against him. Curran served as the campaign manager for Bill Murley, Cousins's opponent. Cousins was re-elected in November 2004.[113]

Approximately one year later, on September 8, 2005, Curran called in sick to work. The following month, Department Captain Michael Halley approached Curran at work and discussed the Department's policy of conducting home visits when corrections officers called in sick. When Curran told Halley that the sick-call policy wasted taxpayers' money, Halley responded that he was "just following orders," and in response, Curran told Halley that German officers had raised the same defense during the Nuremberg war crimes trials following World War II.[114]

Later that month, Department Captain Arthur Statezni had a conversation regarding the sick-call policy with Curran. Curran became upset and made threatening statements, including "you captains and deputies are gonna get shot." After holding a disciplinary hearing, the Department found Curran's comments to be "threatening and menacing" and that the two incidents "would tend to adversely affect the operations of the Department by prompting employees to second-guess direct orders." As a result, Curran was suspended for one month and ordered to submit to a psychological evaluation to assess his fitness for duty as a corrections officer.[115] Within a week, Curran posted an angry message on the union website, which contained a discussion board with thousands of messages posted since its creation. Curran's postings compared Cousins to Hitler, the correctional officers as the Jews, the Department's deputies and generals as the Nazis, and another group (including himself) as ones who may attack the Nazis. Curran was terminated later that month.[116]

Curran filed a 42 U.S.C. § 1983 action in federal court against the Department as well as Cousins and Special Sheriff Thomas C. Goff, in their individual and official capacities, asserting violations of his First Amendment rights. The complaint also pled a state-law claim under the Massachusetts Declaration of Rights and defamation based on a letter from Cousins to the Billerica police chief informing him of Curran's threats. After the defendants answered, Curran moved for partial judgment on the pleadings under Rule 12(c). The defendants filed a cross-motion for judgment on the pleadings thereafter. The federal district court granted the defendants' motion for judgment on the pleadings on the § 1983 First Amendment claim and declined to exercise jurisdiction over the remaining state-law claims, leaving Curran to pursue his state-law claims in state court. Curran appealed the district court's decision dismissing his First Amendment claim to the U.S. Court of Appeals for the First Circuit.[117]

The First Circuit began by noting that Curran's initial verbal threats, for which he was suspended, were not entitled to First Amendment protection because they were made not as a citizen, but were made to his superiors in the course of his duties within the Department and during a discussion of official Department policy. However, the court found that part of Curran's online postings were both made as a citizen and touched upon matters of public concern. For instance, Curran's posting asked others how they could "sit back and watch the unfairness of the discipline and harassement [sic] being doled out to political/union rivals of the sheriff and not stand up and say that it's not right and try to stop it."[118] Nevertheless, Curran's First Amendment claim failed because the Department had an adequate justification for terminating him, given that his statements "directly went to impairing discipline by superiors, disrupting harmony and creating friction in working relationships, undermining confidence in the administration, invoking oppositional personal loyalties, and interfering with the regular operation of the enterprise."[119]

The vast majority of courts have concluded that a private employee may not base a wrongful termination claim on a violation of freedom of speech because there is no state action involved in such cases.[120] However, given the persistent erosion of the employment-at-will doctrine, private employees who have been terminated for their social networking activities may begin to bring wrongful discharge claims alleging violations of their First Amendment rights.[121] For instance, in *Wiegand v. Motiva Enterprises, LLC*,[122] the plaintiff, a store manager at a Texaco gas station, which was operated by defendants Motiva Enterprises and Starstaff, Inc., brought a wrongful termination claim against the defendants claiming that he was terminated in violation of a clear mandate of public policy: the exercise of his Constitutional right to free speech.[123]

110. *Id.* at 312-13.
111. *Id.* at 313-14.
112. 509 F.3d 36, 47 (1st Cir. 2007).
113. *Id.* at 39-40.
114. *Id.* at 40.
115. *Id.*
116. *Id.* at 40-43.
117. *Id.* at 43.
118. *Id.* at 45-46.
119. *Id.* at 49-50.
120. Petrovski v. Fed. Express Corp., 210 F. Supp. 2d 943, 948 (N.D. Ohio 2002) (citing numerous decisions).
121. Darrow & Lichtenstein, *supra* note 31.
122. 295 F. Supp. 2d 465 (D.N.J. 2003).
123. *Id.* at 466-67.

When two newspapers ran articles stating that Wiegand was operating a "mail order neo-Nazi skinhead music company" and that he was a "personal friend and supporter" of Katja Lane (the purported wife of Aryan Nation leader David Lane), Wiegand brought the articles to the attention of his supervisor at the gas station. The defendants' investigated and discovered that Wiegand was operating a website that sold racist and offensive underground music and records, swastika flags, and t-shirts with sayings like "Skinheads." Wiegand was then terminated because his operation of the website violated the company's "core value" of "respect for all people."[124]

Wiegand subsequently filed a lawsuit in the U.S. District Court for the District of New Jersey claiming that the defendants: (1) wrongfully terminated him because they discharged him "in violation of a clear mandate of public policy," namely his exercise of his Constitutional right to free speech;(2) breached a provision in his employee handbook when they fired him; and (3) were liable for damages under a theory of promissory estoppel because he relied on a statement from his supervisor regarding future employment.[125] The defendants filed for summary judgment. The court granted summary judgment on the second claim because the employee handbook clearly provided that it did not create a contractual relationship between the parties and denied summary judgment on the third claim because there were questions of fact regarding whether Wiegand reasonably relied on a promise for continued employment.[126]

With regard to Wiegand's wrongful termination claim, the Court explained that, under New Jersey law, an at-will employee may sustain a claim for wrongful termination if he shows that his discharge was "contrary to a clear mandate of public policy" and that sources of public policy include the United States and New Jersey Constitutions; federal and state laws and administrative rules, regulations and decisions; the common law and specific judicial decisions; and in certain cases, professional codes of ethics.[127] Interestingly, the court noted that the issue regarding whether a wrongful termination claim against a private employer may be based on a First Amendment constitutional claim had not yet been addressed by the New Jersey courts.[128]

However, rather than considering that issue, the court then engaged in an extensive First Amendment analysis. The court determined that, even if an employee could assert a First Amendment wrongful termination claim against a private employer under New Jersey law, Wiegand's claim would fail. The court concluded that, because Wiegand's speech was commercial hate speech regulated by an employer, it was not clearly protected by the First Amendment. Therefore, the court granted summary judgment on Wiegand's wrongful termination claim.[129] This decision is significant because it indicates that courts may be more willing to entertain the argument that a wrongful termination claim in the private employment context may be based upon a violation of First Amendment rights.

C. Invasion of Privacy Claims

In addition to wrongful discharge and First Amendment claims, employees terminated for their social media use may bring claims for invasion of privacy against their employers. The Restatement (Second) of Torts recognizes four categories of invasion of privacy: (1) unreasonable intrusion upon the seclusion of another; (2) appropriation of the other's name or likeness; (3) unreasonable publicity given to the other's private life; and (4) publicity that unreasonably places the other in a false light before the public.[130] Of these four torts, intrusion upon seclusion probably is the most apt for an employee whose employer intrudes upon his social media use.[131] However, employees may also assert invasion of privacy claims based on the third theory: "unreasonable publicity given to the other's private life"[132] (also known as "public disclosure of private facts"[133]).

Under the Massachusetts Privacy Act, which codifies the common law right to privacy, "[a] person shall have a right against unreasonable, substantial or serious interference with his privacy."[134] The Massachusetts courts have recognized two of the four types of invasion of privacy under this statute: public disclosure of private facts,[135] and unreasonable intrusion upon the seclusion of another.[136] Under both theories, "the employer's legitimate interest in determining the employees' effectiveness in their jobs should be balanced against the seriousness of the intrusion on the employees' privacy."[137]

124. *Id.* at 466.

125. *Id.* at 466-67.

126. *Id.* at 466-67.

127. *Id.* at 473.

128. *Id.*

129. *Id.* at 477-78.

130. Brown-Criscuolo v. Wolfe, 601 F. Supp. 2d 441, 455 (D. Conn. 2009); *see also* Restatement (Second) of Torts 652A (1977). The right to privacy is derived from the U.S. Constitution, states constitutions, statutory sources, and the common law. Scott C. Moriearty et al., 45 Massachusetts Practice: Employment Law § 7.1 (2d ed. 2003); *Opinion of the Justices to the Senate*, 375 Mass. 795, 807 (1978) ("Like the United States Constitution, the Massachusetts Constitution does not expressly refer to a right to privacy. If the right exists it must be implied in specific provisions of the Constitution."). The modern tort of invasion of privacy was largely based on theories proposed by William L. Prosser in his 1960 *California Law Review* article entitled "Privacy" as well as Samuel Warren and Louis Brandeis in their 1890 *Harvard Law Review* article entitled "The Right To Privacy." *See generally* William T. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960); Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193 (1890).

131. Darrow & Lichtenstein, *supra* note 31; *see also* Amanda Richman, *Note, Restoring The Balance: Employer Liability and Employee Privacy*, 86 Iowa L. Rev. 1337, 1352 (2001) ("Of the four theories of tort liability for invasion of privacy, 'intrusion upon seclusion' is the claim often brought by employees . . . whose e-mail is monitored without their consent.").

132. *See* Oropallo v. Brenner, 25 Mass. L. Rep. 147, 2009 Mass. Super. LEXIS 13, at *9-10 (Jan. 14, 2009) (Lemire, J.).

133. Howell v. Enter. Publ'g Co., *LLC,* 72 Mass. App. Ct. 739, 749 (2008).

134. Mass. Gen. Laws ch. 214, § 1B (2010). This statute applies to both private and public employment. *See* O'Connor v. Police Comm'r of Boston, 408 Mass. 324, 330 (1990).

135. Bratt v. International Business Machines Corp., 392 Mass. 508, 510 (1984) ("the disclosure of private facts about an employee through an intracorporate communication is sufficient publication to impair an employee's right of privacy").

136. Folmsbee v. Tech Tool Grinding & Supply, 417 Mass. 388, 392 (1994) ("We have recognized that requiring an employee to submit to urinalysis involves a significant invasion of privacy."). The Massachusetts Supreme Judicial Court has relied upon the Restatement rule when evaluating an intrusion claim. *See* Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 409 Mass. 514, 519 (1991).

137. *Folmsbee,* 417 Mass. at 392; Bratt v. International Business Machines Corp., 392 Mass. 508, 520 (1984); *see also* Ayash v. Dana-Farber Cancer Inst., 443 Mass. 367, 383 (2005). This balancing test is "reminiscent of, if not identical to, the conventional federal approach on the constitutional question" of whether there has been a Fourth Amendment violation. Jackson v. Liquid Carbonic Corp., 863 F.2d 111, 116 (1st Cir. 1988); O'Connor v. Police Com'r of Boston, 408 Mass. 324, 330 (1990).

In addition, appropriation of an individual's name or likeness for commercial purposes is actionable under a specific statute in Massachusetts.[138] The "false light" theory of the invasion of privacy has been neither adopted nor rejected in Massachusetts.[139]

Courts have suggested that there is no reasonable expectation of privacy in information transmitted via work e-mail where an employer's e-mail policy warns employees that their messages may be monitored.[140] Moreover, even where the employee has a reasonable expectation of privacy with regard to his social media usage, an employer's "legitimate business interest in protecting its employees from harassment in the workplace" may trump the employee's privacy interests.[141] Furthermore, an employee terminated for his use of social media might also find it difficult to demonstrate that the invasion of privacy was "highly offensive," which is a requirement in many states.[142]

Given the "obstacles that could impede or prevent a successful challenge to the doocing," it is "unlikely" that a "doocee" will prevail in a wrongful discharge or invasion of privacy lawsuit against an employer.[143] However, despite this, employers should be aware that courts have held that "[w]hether a particular person has relinquished an expectation of privacy … is a factual question,"[144] and under certain circumstances, liability may be found.[145] In addition, a violation of state invasion of privacy law could "contravene public policy" and give rise to a wrongful discharge claim.[146]

Although it appears that there are no Massachusetts cases involving invasion of privacy claims based on employees' social media use, Massachusetts courts have applied common law principles when resolving such claims based on employee email use and would likely apply those principles in social media cases as well. *Garrity v. John Hancock Mut. Life Ins. Co.*[147] and *Restuccia v. Burk Tech., Inc.*[148] are two Massachusetts decisions involving the application of these principles in which plaintiffs brought invasion of privacy claims following their terminations for inappropriate email use.

In *Garrity,* the plaintiffs, Nancy Garrity and Joanne Clark were employees of John Hancock Mutual Life Insurance Company ("John Hancock") for twelve and two years, respectively, until they were terminated in July of 1999. When one of their coworkers complained about receiving a sexually explicit email from them, Hancock promptly commenced an investigation of their email folders and those with whom they regularly emailed and determined that they had violated its email policy, which provided that: defamatory, abusive, obscene, profane, sexually oriented, threatening or racially offensive messages were prohibited; the inappropriate use of email was a violation of company policy that could subject an employee to disciplinary action, up to and including termination; all information stored, transmitted, received, or contained in the company's e-mail systems was company property; and the company management reserved the right to access all email files.[149]

Following their terminations, Garrity and Clark filed action in the Massachusetts Superior Court, bringing claims for invasion of privacy, unlawful interception of wire communications, wrongful discharge in violation of public policy, wrongful discharge to deprive plaintiffs of benefits, and defamation. Hancock filed a motion for summary judgment on all counts.[150] The court first examined

138. *See* Mass. Gen. Laws ch. 214 § 3A; Albright v. Morton, 321 F. Supp. 2d 130, 139 (D. Mass. 2004).

139. *See* Barnes v. Town of Webster, 20 Mass. L. Rep. 151, 2005 Mass. Super. LEXIS 480, at *3-4 (Oct. 11, 2005) (Agnes, J.).

140. *See* Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *1, *4 (D. Mass. 2002) (Zobel, J.) (holding employees who "regularly received" "sexually explicit e-mails," "which they then sent to coworkers," had no "reasonable expectation of privacy in their work e-mail" because they knew that the employer "had the ability to look at e-mail on the company's intranet system" and that the emails "would eventually be sent to third parties"); Chimarev v. TD Waterhouse Investor Servs., 280 F. Supp. 2d 208, 216 (S.D.N.Y. 2003) ("New York's limited right of privacy does not prohibit an employer from accessing employee email and other documents produced on the company's system").

141. Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *6 (D. Mass. 2002) (Zobel, J.). "Both Title VII of the Civil Rights Act of 1964 and M.G.L. c. 151B require employers to take affirmative steps to maintain a workplace free of harassment and to investigate and take prompt and effective remedial action when potentially harassing conduct is discovered." *Id.* (holding defendant was "required by law to commence an investigation" when it "received a complaint about the plaintiffs' sexually explicit e-mails").

142. *See* Brown-Criscuolo v. Wolfe, 601 F. Supp. 2d 441, 455 (D. Conn. 2009); Goodrich v. Waterbury Republican-American, Inc., 188 Conn. 107, 134 (1982); *see also* Hilderman v. Enea TekSci, Inc., 551 F. Supp. 2d 1183, 1192 (S.D. Cal. 2008) (holding employer's search of employee's company-issued laptop containing private e-mails was not invasion of privacy because not "highly offensive," as required by applicable law); *Smyth v. Pillsbury Co.,* 914 F. Supp. 97, 101 (E.D. Pa. 1996) ("we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy"); Restatement (Second), Torts §§ 652B & 652D (1977).

143. Darrow & Lichtenstein, *supra* note 31; Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) ("we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee . . . notwithstanding any assurances that such communications would not be intercepted by management" because "[o]nce plaintiff communicated the alleged unprofessional comments to a second person . . . over [the company's] e-mail system . . ., any reasonable expectation of privacy was lost").

144. Oropallo v. Brenner, 25 Mass. L. Rep. 147, 2009 Mass. Super. LEXIS 13, at *14 (Jan. 14, 2009) (Lemire, J.).

145. *See* Brown-Criscuolo v. Wolfe, 601 F. Supp. 2d 441, 455 (D. Conn. 2009) (denying defendant's motion for summary judgment on plaintiff's invasion of privacy claim where policy provide "limited expectation of privacy" and defendant accessed plaintiff's email account "without permission and looked at a correspondence that was not addressed to him"); Oropallo v. Brenner, 25 Mass. L. Rep. 147, 2009 Mass. Super. LEXIS 13 (Jan. 14, 2009) (holding, where employer "circulated confidential materials stemming from an internal investigation into [the employee's] job performance, employer could be liable under invasion of privacy statute for disclosing "facts related to her sexual affair" with a coworker); Restuccia v. Burk Tech., Inc., 5 Mass. L. Rep. 712, 1996 Mass. Super. LEXIS 367, at *2, *9-10 (1996) (Lopez, J.) (holding employer's "reading of the [employees'] E-Mail messages" where there "was no policy against using the E-Mail system for personal messages" and where the employees "were not specifically told that supervisors had access to their systems" might give rise to invasion of privacy claim and wrongful termination claim based on public policy violation).

146. Cort v. Bristol-Myers Co., 385 Mass. 300, 307 (1982) (explaining that if the employer "had no right to ask the questions that the plaintiffs declined to answer," it "could be liable for discharging the plaintiffs for their failure to answer those questions").

147. No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 (D. Mass. 2002) (Zobel, J.).

148. 5 Mass. L. Rep. 712, 1996 Mass. Super. LEXIS 367 (1996) (Lopez, J.)

149. *Garrity,* 2002 U.S. Dist. LEXIS 8343, at *2. Hancock periodically reminded its employees that it was their responsibility to know and understand the e-mail policy, and also warned them of several incidents in which employees were disciplined for violations. *Id.*

150. *Id.* at *3.

the plaintiffs' invasion of privacy claims. The court concluded that the Plaintiffs had no reasonable expectation of privacy in their work email because they admitted that they knew Hancock had the ability to look at email on its intranet system and that they had to be careful about sending emails. The court further held that, even if they had a reasonable expectation of privacy in their work email, Hancock's legitimate business interest in protecting its employees from harassment in the workplace (which was required under Title VII of the Civil Rights Act of 1964 and Mass. Gen. Laws ch. 151B) trumped the plaintiffs' privacy interests. Therefore, the plaintiffs' invasion of privacy claims failed.[151]

The court held that the plaintiffs' claims under the Massachusetts Wiretap Statute (Mass. Gen. Laws ch. 272 § 99 (2010), which prohibits certain interceptions of wire and oral communications, failed because the reading of e-mails after they have been transmitted to the recipient does not constitute "interception" within the meaning of the statute. With regard to the plaintiffs' claim that Hancock violated the public policy of the invasion of privacy statute and the wiretap statute by terminating their employment, the court held that their ability to assert their rights under these statutes precluded the invocation of the public policy doctrine.[152] The plaintiffs also claimed that Hancock terminated their employment solely to minimize the anticipated cost of reducing its work force, in violation of section 510 of ERISA, 29 U.S.C. § 1140. However, this claim failed because they presented no evidence showing that Hancock engineered their terminations to deprive them of ERISA benefits.[153]

The plaintiffs' final count alleged that Hancock's supervisors defamed them by telling other employees that they were terminated for sending and receiving sexually lewd, harassing, defamatory, and sexually explicit e-mails. However, the court concluded that, even if these statements met the required elements of a defamation claim, as an employer, Hancock was entitled to a conditional privilege that insulated it from liability for these statements. As a result, the plaintiffs had to show that Hancock abused this privilege by recklessly publishing defamatory facts, and they could not do so. Further, Hancock had a legitimate business purpose for making these statements: to warn them of the consequences of violating the email policy and to prevent such violations in the future. Therefore, the court granted summary judgment on all counts of the plaintiffs' complaint.[154] This decision indicates that a court will be unlikely to find a reasonable expectation of privacy (and an invasion of privacy claim will be unlikely to prevail) where an employer's policy states that all information stored and transmitted on its email system is company property and that the company has the right to access all emails.

The U.S. District Court for the District of Pennsylvania reached a similar conclusion in *Smyth v. Pillsbury Co.*[155] In *Smyth*, the plaintiff, Michael A. Smyth, worked as an at-will employee in the position of regional operations manager for the Pillsbury Company. Pillsbury maintained an electronic mail communication system in order to promote internal corporate communications between its employees. It also repeatedly assured its employees, including Smyth, that all e-mail communications would remain confidential and privileged, and that they could not be intercepted and used by defendant against its employees as grounds for termination or reprimand.[156] Despite this, in January 1995, Pillsbury terminated his employment for transmitting what it deemed to be inappropriate and unprofessional comments over its e-mail system. Smyth subsequently brought a diversity action in the U.S. District Court for the District of Pennsylvania claiming that he was terminated in violation of the public policy protecting an employee's "right to privacy as embodied in Pennsylvania common law." Pillsbury filed a motion to dismiss Smyth's complaint.[157]

In considering the motion to dismiss, the district court began by noting that, under Pennsylvania law, an employer may discharge an at-will employee with or without cause and that the public policy exception is an especially narrow one. The court then explained that the discharge would violate public policy based on the intrusion upon seclusion species of the invasion of privacy tort if it was related to a "substantial and highly offensive invasion of the employee's privacy." The court concluded that Smyth had no reasonable expectation of privacy in email communications that he voluntarily made to his supervisor over the company email system, even though he was assured that such communications would not be intercepted by management.[158]

The court also concluded that, even if Smyth had a reasonable expectation of privacy, a reasonable person would not have considered Pillsbury's interception of his communications to be a substantial and highly offensive invasion of his privacy because he was not required to disclose any personal information about himself and there was no invasion of his person or personal effects. Furthermore, Pillsbury's interest in preventing inappropriate and unprofessional comments or even illegal activity over its email system outweighed any privacy interest Smyth may have had in those comments. Therefore, the court granted Pillsbury's motion to dismiss Smyth's wrongful termination claim.[159]

A contrary result was reached in *Restuccia v. Burk Tech., Inc.*[160] In *Restuccia,* the plaintiffs, Laurie Restuccia and Neil LoRe, were employees of Burk Technology, Inc., a manufacturer of electronic equipment that was owned by Peter Burk. The company's computer system, which included an email system, required a password to log in. There was no policy against using the email system for personal messages, but there was a policy against excessive chatting. Although supervisors had the ability to access employees' computer files by using supervisory passwords, the plaintiffs were not specifically informed of this.[161]

In January 1994, Burk held a staff meeting in which he outlined a fixed break-time policy requiring all employees to take their breaks at the same time. LoRe protested the policy at the meeting. Burk was displeased with LoRe but did not intend to terminate him at that time. Later that day, a production manager informed Burk that LoRe was spending a lot of time using the email system. That evening, Burk used his supervisory password to gain access to back up files and read his employees' email files, including Restuccia's and LoRe's, for approximately eight hours.[162]

151. *Id.* at *3-6.
152. *Id.* at *7-9.
153. *Id.* at *10-11.
154. *Id.* at *11-13.
155. 914 F. Supp. 97 (E.D. Pa. 1996).
156. *Id.* at 98.
157. *Id.* at 98, 100.
158. *Id.* at 100-01.
159. *Id.* at 101.
160. 5 Mass. L. Rep. 712, 1996 WL 1329386 (Aug. 13, 1996).
161. *Restuccia,* 1996 WL 1329386, at *1.
162. *Id.*

The emails between Restuccia and LoRe included nicknames for Burk and references to his extra-marital affair with another employee, as well as other personal correspondences. Burk terminated Restuccia and LoRe shortly thereafter, allegedly for the excessive quantity of the email, rather than the content of the messages. The plaintiffs subsequently filed an action in the Massachusetts Superior Court, bringing claims against the company and Burke for wrongful termination, invasion of privacy, unlawful interception of wire communications, intentional and negligent infliction of emotional distress, loss of consortium, and interference with contractual relations. The defendants moved for summary judgment on all counts in the complaint.[163]

The court first examined the plaintiffs' claim that the defendants unlawfully intercepted wire communications in violation of the Massachusetts Wiretap Act. The court held that the company's back-up system (which automatically stored all computer files, including plaintiffs' emails) did not constitute an unlawful wire interception in violation of the statute because the company's interest in storing computer information in back-up files was clearly the type of permissible interception contemplated by the "ordinary course of business" exemption to the statute,[164] which exempts the possession or use of an "office intercommunication system which is used in the ordinary course of their business."[165]

The court held that the plaintiffs' intentional infliction of emotional distress claims failed because they had not established that Burk's conduct was extreme and outrageous, that his conduct was intended to cause emotional distress, or that he should have known that emotional distress was the likely result of his conduct. However, the plaintiffs negligent infliction of emotional distress claims were allowed to proceed to trial because Restuccia demonstrated that she experienced sleeplessness, stomachaches, headaches and suffered a miscarriage as a result of her termination; and LoRe demonstrated that he suffered from sleeplessness, gastrointestinal difficulties, and fatigue as result of his termination.[166]

The plaintiffs' tortious interference with contractual relations claims failed because he did not allege that they had an existing or prospective contract with a third party. The court denied summary judgment on the plaintiffs' invasion of privacy claims, concluding that there were genuine issues of material fact on the issue of whether they had a reasonable expectation of privacy in their emails and whether Burk's reading of the emails constituted an unreasonable, substantial or serious interference with their privacy. The court also denied summary judgment on the plaintiffs' wrongful termination claims because it found that there were genuine issues of material fact on the invasion of privacy claims.[167]

Although the court did not explicitly state that the lack of a policy prohibiting the use of the company email system for personal messages was critical to its analysis in this case, this appears to be the distinguishing feature of this case and the reason why the invasion of privacy and wrongful termination claims were allowed to go forward to trial. Thus, this case makes clear that an employer's electronic communications or social media policy should make clear that company computers may not be used for personal affairs.

The U.S. Supreme Court recently issued a significant decision involving privacy issues for public employers and employees. In *City of Ontario, California v. Quon*,[168] the Court held that a city's search of an employee's text messages was reasonable under the Fourth Amendment.[169] The Court explained that the search of the text messages was conducted for a "legitimate work-related rationale," given that it was necessary to determine whether the character limit on the city's contract with a wireless service provider was sufficient to meet the city's needs, and reviewing the text message transcripts was reasonable because "it was an efficient and expedient way to determine whether [the employee's] overages were the result of work-related messaging or personal use." Therefore, the Court held that the search did not violate the employee's Fourth Amendment rights and that his § 1983 action failed.[170]

Significantly, the court concluded that the search would be "regarded as reasonable and normal in the private-employer context."[171] Further, the court also noted that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."[172] Thus, although this case involved a public employer, it may provide guidance to private employers as well.

D. Stored Communications Act Claims

An employer may be liable under Title II of the Electronic Communications Privacy Act (ECPA)—the Stored Communications Act (SCA)—for accessing information on an employee's personal electronic communication account without authorization.[173] Such was the case in *Pietrylo v. Hillstone Restaurant Group*.[174] Brian Pietrylo and Doreen Marino worked as servers for Hillstone Restaurant Group at its Houston's restaurant in Hackensack, New Jersey. Pietrylo created a private, invitation-only group on MySpace.com called the "Spec-Tator," the stated purpose of which was to "vent about any BS we deal with out [sic] work without any outside eyes spying in on us."[175]

The posts on the Spec-Tator included sexual remarks about management and customers of Houston's, jokes about some of the specifications that Houston's had established for customer service and quality, references to violence and illegal drug use, and a copy of a new wine test that was to be given to the employees. Pietrylo invited other past and present employees of Houston's to join the group, including Marino. Houston's management gained access to the site through another employee, and Pietrylo and Marino were later terminated due to the content on Spec-Tator.[176]

163. *Id.*
164. *Id.* at *2.
165. Mass. Gen. Laws ch. 272, § 99(D)(1)(b)(2010).
166. *Restuccia,* 1996 WL 1329386, at *2-3.
167. *Id.* at 3.
168. 130 S. Ct. 2619 (2010).
169. *Quon,* 130 S. Ct. at 2632-33.
170. *Id.* at 2633.
171. *Id.* at 2630.
172. *Id.* at 2633.
173. Charles H. Wilson, *Trouble Investigating 'Textual Harassment,'* Law.com (November 3, 2009), http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202435127911; *see also* 18 U.S.C. § 2701 et seq.; Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 587 F. Supp. 2d 548, , 551, 562 (S.D.N.Y. 2008) (holding employer violated SCA by accessing employee's personal email account); Rozell v. Ross-Holst, 2007 U.S. Dist. LEXIS 46450, at *19-21 (S.D.N.Y. June 21, 2007) (holding employer may be liable under the SCA for "having hacked into the plaintiff's AOL account").
174. Civil Case No. 06-5754, 2008 WL 6085437 (D.N.J. July 25, 2008).
175. *Id.* at *1.
176. *Id.* at *1-2.

In November 2006, Pietrylo and Marino filed a six-count complaint in the U.S. District Court for the District of New Jersey alleging: (1) violations of the federal Wiretap Act (18 U.S.C. §§ 2510-22); (2) the parallel New Jersey Wiretapping and Electronic Surveillance Control Act (N.J.S.A. 2A:156A-3 and 4(d)); (3) the federal Stored Communications Act (18 U.S.C. §§ 2701-11); (4) the parallel provision of the New Jersey Act (N.J.S.A. 2A:156A-27); (5) wrongful termination in violation of a clear mandate of public policy; (6) and common law tort of invasion of privacy. They later amended their complaint to split the fifth count into two counts: the first alleging a violation of a public policy favoring freedom of speech and the second alleging a violation of a public policy against invasion of privacy. They also voluntarily dismissed their claims under the state and federal wiretapping statutes after discovering that Hillstone did not intercept any electronic communications pursuant to these statutes. Hillstone filed a motion for summary judgment on the remaining counts.[177]

The court first addressed the plaintiffs' claims under the federal SCA and the identical provision of the New Jersey Act (N.J.S.A. 2A:156A-27), which make it an offense to intentionally access stored communications without authorization or in excess of authorization.[178] The court held that, since St. Jean testified that she felt as though she would "get in trouble" or possibly be fired if she refused to comply with her manager's request for the password, management's access of the Spec-Tator was likely not "authorized" under the statute. Thus, the court denied summary judgment on these counts.[179]

The court next considered the plaintiffs' claim that Hillstone wrongfully discharged them in violation of a clear mandate of public policy, freedom of speech, by terminating them for commenting on and criticizing their employer. The court noted that freedom of speech protections generally do not extend to the private employment context and, further, that New Jersey state courts have not addressed whether a wrongful termination claim may be based on an alleged interference with freedom of speech as protected by the New Jersey Constitution. However, the court granted summary judgment on this count, reasoning that even if Houston's had been a public employer, the plaintiffs failed to meet the test for a public employee's retaliation claim based on protected activity because there was no evidence indicating that the speech at issue was a matter of public concern.[180]

With regard to the plaintiffs' claim that Hillstone wrongfully discharged them in violation of a clear mandate of public policy against invasion of privacy, the court explained that a right to privacy may be a source of "a clear mandate of public policy," but these privacy interests will be balanced against the employer's interests in managing its business. Because the Spec-Tator was an invitation-only internet discussion space, the plaintiffs had an expectation that only invited users would be able to read the discussion. Moreover, it was not clear whether St. Jean voluntarily provided authorization to access the website. Thus, the court denied summary judgment on this count. Similarly, the court denied summary judgment on the plaintiffs' common law tort invasion of privacy claim alleging that Hillstone impermissibly intruded on their seclusion because it was not clear that St. Jean gave consent to Hillstone's management to view the Spec-Tator and the plaintiffs' expectations of privacy was a question of fact for the jury to decide.[181]

The court issued its decision granting Hillstone partial summary judgment in July 2008. The following year, in July 2009, a jury trial commenced to determine whether Hillstone: (1) violated the federal or state Stored Communications Acts; (2) violated the plaintiffs' common law right to privacy; and (3) wrongfully terminated the plaintiffs in violation of the public policy favoring their right to privacy. The jury found in favor of Hillstone on the latter two claims, but returned a verdict in favor of the plaintiffs on the SCA claims, finding that Hillstone, through its managers, had knowingly, intentionally, or purposefully accessed the Spec-Tator without authorization on five occasions. The jury awarded $2,500 and $903 in compensatory damages to Pietrylo and Marino, respectively, and by stipulation of the parties, an award of punitive damages equal to four times the amount of compensatory damages.[182] This decision establishes that "[e]mployers should not log into an employee's social-networking site under false pretenses or by coercing another employee to grant them access they would not otherwise be able to obtain."[183]

A more significant jury verdict was awarded in *Van Alstyne v. Electronic Scriptorium, Ltd.,*[184] where the president of a company accessed an employee's personal email account in violation of the SCA.[185] Following a trial, plaintiff was awarded $150,000 in statutory damages and $75,000 in punitive damages against the president; $25,000 in statutory damages and $25,000 in punitive damages against the company; and $135,723.56 in attorneys' fees and costs. On appeal, the court vacated the award of statutory damages, concluding that plaintiffs pursuing claims under the SCA must prove actual damages in order to be eligible for an award of statutory damages, but upholding the award of punitive damages and the attorneys' fees.[186] The U.S. District Court for the Southern District of New York has also concluded that an employer's unauthorized access of an employee's email account violates the SCA.[187]

In a recent decision, the U.S. District Court for the Central District of California held that private Facebook and MySpace

177. *Id*.

178. *Id.* at *3. The SCA is part of the Electronic Communications Privacy Act (18 U.S.C. § 2510), which was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute) intended to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. *See* 18 U.S.C. § 2511.

179. *Id.* at *4.

180. *Id.* at *5-6.

181. *Id.* at *6-7.

182. Pietrylo v. Hillstone Restaurant Group, Civil Case No. 06-5754, 2009 WL 3128420 (D.N.J. Sept. 25, 2009).

183. Molly DiBianca, *Jury Verdict Against Employer Who Accessed Employee's MySpace Page*, The Delaware Employment Law Blog (September 4, 2009), http://www.delawareemploymentlawblog.com/2009/09/jury_verdict_against_employer.html.

184. 560 F.3d 199 (4th Cir. 2009).

185. *Id.* at 201.

186. *Id.* at 201-02.

187. *See* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 562 (2008).

messages constitute protected information under the SCA, and cannot be subpoenaed for use in civil litigation.[188] When determining whether information on social networking websites and other electronic communications are discoverable in litigation, courts will balance the user's reasonable expectation of privacy against the relevance of the information.[189] For an overview of the various methods by which electronically stored information (ESI), including emails, website postings, and text messages, may be authenticated, as well as other evidentiary issues relating to ESI, see *Lorraine v. Markel American Ins. Co.*[190]

V. Conclusion

The explosion of social media use here in the U.S. and throughout the world presents both challenges and opportunities for employers. The law relating to these issues is still developing, but courts are likely to rely upon principles established well before the advent of social media. Employers must be cognizant of the risks inherent in the use of social media among their employees and the potential liability issues throughout the employment relationship, from pre-employment, to employment, to post-employment. An awareness of these risks will become increasingly important as social media use continues to grow.

188. Crispin v. Christian Audigier, Inc., --- F.Supp.2d ----, 2010 WL 2293238, at *16 (C.D.Cal. May 26, 2010); Doug Cornelius, *Are Facebook and MySpace Messages Subject to Discovery?,* Compliance Building (June 16, 2010), http://www.compliancebuilding.com/2010/06/16/are-facebook-and-myspace-messages-subject-to-discovery/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+compliancebuilding+%28Compliance+Building%29&utm_content=Google+Reader.

189. Ronald J. Levine and Susan L. Swatski-Lebson, *Are Social Networking Sites Discoverable?*, Law Technology News (Nov. 13, 2008), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202425974937; Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 308 (2010) (holding that employee "could reasonably expect that e-mail communications with her lawyer through her personal account would remain private, and that sending and receiving them via a company laptop did not eliminate the attorney-client privilege that protected them"); National Economic Research Associates, Inc. v. Evans, 21 Mass. L. Rptr. 337, 2006 WL 2440008, at *5 (Aug. 3, 2006) (Gants, J.) (denying employer's motion to compel production of employee's emails sent from his personal, password-protected email account to his attorney).

190. 241 F.R.D. 534. 554-62 (D. Md. 2007).