SOCIAL MEDIA POLICIES AND THE PUBLIC EMPLOYER: LESSONS FROM THE PRIVATE SECTOR

COURTNEY BARKSDALE PEREZ
Carter, Stafford, Arnett, Hamada & Mockler
8150 N. Central Expressway, Suite 1950
Dallas, Texas 75206

State Bar of Texas
25TH ANNUAL
SUING & DEFENDING GOVERNMENTAL ENTITIES COURSE
July 18-19, 2013
Austin

CHAPTER 21

CARTER ▪ STAFFORD
ARNETT HAMADA MOCKLER



Courtney Perez

Of Counsel

214.550.5052
cperez@carterstafford.com

Courtney Barksdale Perez is Of Counsel to Carter Stafford Arnett Hamada & Mockler. Ms. Perez represents individuals, corporations, and government entities in all phases of commercial and employment-related litigation including administrative proceedings, state court and federal court. Ms. Perez has represented plaintiffs and defendants in disputes involving fraud, negligence, breach of contract, breach of covenants not to compete, tortious interference with contracts, misappropriation of trade secrets, trademark infringement, breach of fiduciary duty and employment-related civil rights claims.

Ms. Perez also advises clients concerning compliance with employment-related statutes such including Title VII, the Americans with Disabilities Act, Age Discrimination in Employment Act, Family Medical Leave Act, Federal Labor Standards Act, the Pregnancy Discrimination Act, 42 U.S.C. § 1983, the Texas Whistleblower Act, the Texas Payday Act, the Texas Labor Code and employment agreements. She also conducts internal investigations, reviews and prepares policies and procedures, and provides training for employers. Ms. Perez also has experience advising government contractors with their obligations under federal contract compliance laws, developing compliance programs, drafting Affirmative Action plans and representing government contractors in administrative proceedings.

In addition, Ms. Perez is a trained mediator and uses her dispute resolution training and experience to assist litigants in resolving employment, business, commercial, consumer, personal injury and civil rights disputes.

Prior to joining Carter Stafford, Ms. Perez maintained a solo practice. Ms. Perez was an associate at K&L Gates, LLP from 2008-2011, and served as Law Clerk to the Honorable James A. Beaty, Jr., U.S. District Court for the Middle District of North Carolina from 2007-2008.

Education:

- The University of Texas School of Law, 2007, Austin, Texas
  Juris Doctor
  Order of Barristers
- Wake Forest University, 2004, Winston-Salem, North Carolina
  Bachelor of Arts, Political Science & Communication
  With Honors

Mediation Credentials:

- Dispute Resolution Services of North Texas, Inc. Basic Mediation Training (40 Hours)
- Annual Texas Bar CLE Alternative Dispute Resolution Course
- Association of Attorney-Mediators, Member

Honors and Distinctions:

- Selected for inclusion in Thomson Reuters' *Super Lawyers® Rising Stars* (Texas), 2013
- Recipient of the Dallas Bar Association Outstanding Committee Chair Award, 2012

Professional Associations and Community Involvement:

- State Bar of Texas
  - CLE Committee Member
  - Leadership SBOT - Participant, 2011-2012
- Dallas Bar Association
  - Business Litigation Section Council Member
  - Judiciary Committee Member
  - Membership and Admissions Committee Member
  - Minority Participation Committee, Co-Chair, 2012
  - Minority Participation Committee, Co-Vice Chair, 2011
- Dallas Association of Young Lawyers
  - Leadership Class, 2011-2012
  - Solo & Small Firm Committee, Co-Chair
- Patrick A. Higginbotham Inn of Court - Associate Member, 2010-2011
- J.L. Turner Legal Association, Member
- Delta Sigma Theta Sorority, Inc., Member
- Dallas Children's Theater, Member, Board of Trustees
- Dallas Summer Musicals Associate Producers, Member
- Dallas Black Dance Theatre, Contributor

Published Works and Speaking Engagements:

- "What Employers Can Expect When Their Employees Are Expecting" Texas Bar CLE Webcast, July 2013
- "Trending: Recent Developments in FLSA Litigation," Texas Bar CLE Webcast, May 2013
- "Fair Labor Standards Act: Introduction and Summary of Employer Obligations," Texas Bar CLE, Essentials of Business Law Course, March 2013
- "What Employers Can Expect When Their Employees Are Expecting," Dallas Association of Young Lawyers *Dicta*, September 2012
- "Social Media and the Public Employer: Policies, Pitfalls and Proof," 2012 Dallas City Attorney's Office CLE 13th Annual CLE Program, June 2012
- "DAYL Solo & Small Firm Series: Making the Best of Your Of Counsel Relationship," Dallas Association of Young Lawyers, June 2012
- "*All That Glitters Isn't Gold*: Analyzing the Costs and Benefits of Litigation Finance," 26 REV. LITIG. STUD. 707 (2007)
- "Mexico and Forum Non Conveniens: Current U.S. Law," U.S.-Mexico Bar Association Newsletter, March 2009

Bar Admissions:

- Texas, 2007
- U.S. Court of Appeals for the Fifth Circuit, 2010
- U.S. District Court for the Eastern District of Texas, 2011
- U.S. District Court for the Northern District of Texas, 2008
- U.S. District Court for the Southern District of Texas, 2008
- U.S. District Court for the Western District of Texas, 2008

Practice Areas:

- Labor & Employment
- Commercial Litigation
- School Law

TABLE OF CONTENTS

I. INTRODUCTION 1

II. EMPLOYER USE OF SOCIAL MEDIA 1
A Organizational Tool for Information and Marketing 1
B Research Tool for Employment-Related Decisions 2

III. EMPLOYER LIABIITY ARISING FROM USE OF SOCIAL MEDIA 3
A. Discrimination 3
B. Harassment 4
C. Retaliation 4
D. First Amendment 6
E. Stored Communications Act 6
F. Open Meetings Act 7
G. Public Information Act 8
H. National Labor Relations Act 9

IV. BEST PRACTICES FOR SOCIAL MEDIA POLICIES 10
A. Best Practices for Screening Applicants 11
1. Create a Wall 11
2. Define the Process 11
3. Establish the Relevance 11
4. Document the Purpose and the Search 11
5. Be Consistent 11
6. Notify the Applicant 11
B. Best Practices for Existing Employees 12
1. Protect Trade Secrets 12
2. Protect Confidential Information 12
3. Prohibit False, Abusive or Defamatory Comments 12
4. Prohibit Discrimination, Harassment and Retaliation 12
5. Designate an Authorized Spokesperson 12
6. Discourage Personal Use of Social Media During Working Time 12
7. Discourage Use of Work Email for Personal Use 12
8. Provide Notice of Consequences for Violations of the Social Media Policy 12
9. Be Specific 12
10. Eradicate Any Expectation of Privacy 12
11. Be Consistent 12
12. Train Employees on Use of Social Media 13
13. Monitor the Organization's Website and Social Media Pages 13
14 Retain Information from the Organization's Website and Social Media Pages 13
15. Include a Disclaimer 13

SOCIAL MEDIA POLICIES AND PUBLIC EMPLOYERS: LESSONS FROM THE PRIVATE SECTOR

I. INTRODUCTION

What is social media? Merriam Webster defines the term "social medial" as "forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages and other content."[1] The term "social media," first used in 2004, includes web-based magazines, internet forums, websites, blogs, podcasts, photographs and videos.[2] There are hundreds of social media websites, but the top five most popular social media websites include:

1. Facebook
2. Twitter
3. LinkedIn
4. Pinterest
5. MySpace[3]

The reality is that social media usage has increased dramatically since SixDegrees.com, the first recognized social network site, launched in 1997.[4] According to Neilson's most recent social media report, social media now accounts approximately 20% of all time spent online in the United States via personal computers, and 30% of total time spent online via mobile services.[5] Social networking is reportedly the number one activity on the web. On average, Americans spent 37 minutes per day with services such as Facebook, Twitter or LinkedIn in the past year.[6]

Use of social media by employees and employers alike does not cease between the hours of 9:00 a.m. and 5:00 p.m. Indeed, there is even a social media forum dedicated solely to complaining about the workplace, www.jobitorial.com (formerly www.jobvent.com). By all accounts, personal use of social media at work is frequent and widespread, and with the increased presence of Smartphone apps, social media access is just a click away, even if employers restrict access from company computers. The reality, however, is that most employers are no longer restricting access to social media websites and recent surveys report a decline in the number of employers blocking employee access to social media.[7] And, while it's safe to assume that social media at least to some degree is a vehicle for decreased productivity, employees report using social media while at work to connect with co-workers, to drive new ideas and innovative thinking, to track goals or to gain recognition, to share work-related content and to connect with customers.[8]

II. EMPLOYER USE OF SOCIAL MEDIA

A Organizational Tool for Information and Marketing

Both private and public employers are utilizing new technologies to achieve their marketing and communication goals. In particular, public employers are increasingly using social media to improve government services and to engage their citizens.

Social media in the employment context is used in the following three ways: (1) agency use: (2) professional use; and (3) personal use.[9] Agency use describes the authorized use of social media for the express purpose of communicating the organization's interest, programs and/or policy interest. Some reasons public employers choose to utilize social media include:

- To promote Services
- To relay information
- To expand outreach capability
- To improve interaction with the public
- To advertise jobs
- To announce and market events

---

[1] *Social Media Definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/social%20media (last visited July 10, 2013)

[2] *See Id.*

[3] *See Top 15 Most Popular Social Networking Sites July 2013*, eBizMBA, *http://*www.ebizmba.com/articles/social-networking-websites (last visited July 9, 2013) (analyzing monthly average of each website's *Alexa* Global Traffic Rank and U.S. Traffic Rank from *Compete* and *Quantcast* data).

[4] Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History and Scholarship*, 13 JOURNAL OF COMPUTER-MEDIATED COMMUNICATION, 11 (2007)

[5] *State of the Media: The Social Media Report 2012*, NEILSON (Dec. 4, 2012), http://www.nielsen.com/us/en/reports/2012/state-of-the-media-the-social-media-report-2012.html.

[6] *Social Netowrking Is the No. 1 Online Activity in the U.S.*, STATISTA, http://www.statista.com/topics/1164/social-networks/chart/1238/digital-media-use-in-the-us/ (last visited July 9, 2013).

[7] *Social Media and Workplace Collaboration*, SILKROAD http://pages.silkroad.com/rs/silkroad/images/Social-Media-Workplace-Collaboration-SilkRoad-TalentTalk-Report.pdf (last visited July 9, 2013).

[8] *See id.* (reporting that of over 1,100 employees surveyed, 44% reported using social media sites while at work to connect with customers).

[9] *Designing a Social Media Policy for Government: Eight Essential Elements*, Center for Technology in Government (May 2010), http://www.ctg.albany.edu/publications/guides/social_media_policy/social_media_policy.pdf.

- To promote interagency and intergovernmental communication

Professional use describes the employer and employee's use of social media for furthering job-related responsibilities or professional duties through an external site.

Personal use involves an employee's use of social media for personal interest, and typically do not have anything to do with their job duties for the organization.[10]

B Research Tool for Employment-Related Decisions

Just as the presence and influence of social media websites has increased in recent years, so too has employers' reliance on them for information when making hiring and firing decisions. According to Careerbuilder.com, in 2012 37% of employers across industries and company sizes were using social networking websites to screen potential employees.[11] Mainly, employers are searching Facebook, followed by LinkedIn and finally, Twitter.[12] Business and Legal Report conducted a comprehensive survey of employers' use of social media and found that of the employers that use social networks to screen job applicants 35% have at least once decided not to offer a job to an applicant based on the content posted. Over 50% of those employers attributed their decision not to hire based on:

- Provocative photos
- References to drinking and drug abuse
- Bad mouthing of previous employers' and colleagues[13]

The reasons employers might use social-networking are obvious—it allows employers to reach beyond the interview process for a more revealing look at an applicant's background and personality. Indeed, to employers, social media websites are conduits used:

- To see if the candidate presents himself/herself professionally
- To see if the candidate is a good fit for the company culture
- To learn more about the candidate's qualifications
- To see if the candidate is well-rounded
- To look for reasons not to hire the candidate[14]

Around the country, these statistics have played out in cases where hiring and/or firing decisions were made based on the aforementioned categories of information discovered through social media searches. For example, an employee sued her employer after being terminated upon her employer's finding of Facebook pictures of her dancing and playing Frisbee while she was on leave under the Family and Medical Leave Act for a "serious medical condition" that allegedly left her "completely incapacitated."[15] A co-worker brought the photographs of the plaintiff to the attention of management, and when she offered no explanation for the photographs, she was fired.[16]

However, employers aren't just using social media websites to search for reasons not to hire applicants or to discipline existing employees. Employers also reported learning information from social media profiles that caused them to extend offers of employment. Of those employers who found reasons to hire individuals based on their social media profiles:

- 58% reported a good feel for the candidate's personality
- 55% reported that the information conveyed a positive image
- 51% discovered that the candidate appeared to be well-rounded with a wide range of interests
- 44% found evidence of creativity
- 49% found great communication skills
- 34% discovered references from others about the candidate.[17]

Employers' proactive use of social media to screen applicants and to monitor employee conduct in this regard could on the one hand, help to mitigate risks of negligence in hiring, retention, and supervision. On the other hand, employers' reliance on social media for information concerning job applicants is not without risk. The potential benefits for an employer who gains a glimpse into a potential hire's life through Facebook, MySpace or Twitter, must be weighed against those risks. Indeed, information acquired from social media

---

[10] *Id.*

[11] *Press Release*, CAREERBUILDER(Apr. 18, 2012), http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr691&sd=4%2F18%2F2012&ed=4%2F18%2F2099 (reporting that of the employers' surveyed, 65% use Facebook (65 percent) 63% reported using LinkedIn and 16% reported using Twitter to research candidates).

[12] *See Id.*

[13] *Should You Check Facebook Before Hiring*, THE WASHINGTON POST (Jan. 22, 2011), http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012203193.html.

[14] *Press Release*, *supra* note 9.

[15] *Jaszczyszyn v. Advantage Health Physician Network*, 504 F. App'x 440 (6th Cir. 2012) (affirming summary judgment in favor of employer).

[16] *See id.*

[17] *See Press Release*, *supra* note 9.

websites could potentially subject employers to liability simply by virtue of becoming aware of information concerning an applicant that they might not otherwise have known were it not for social media.

III. EMPLOYER LIABIITY ARISING FROM USE OF SOCIAL MEDIA

A. Discrimination

Social media profiles contain a wealth of information about a person's "protected status" under the law. "Protected status" means those attributes of an individual that give rise to certain statutory protections from discrimination in employment based on those attributes and includes an individual's sex, race, color, religion, national origin, and pregnancy status.[18] Age, disability status, veteran status, and genetic information are also protected.[19] Employment discrimination statutes provide protections from discrimination against individuals based on their protected status. A public or private employer who makes a hiring decision without knowingthe individual's protected status does not risk liability for discrimination on the basis of an applicant's protected status. Employers who make hiring decisions after reviewing an applicant's social media profiles can no longer claim ignorance of the applicant's protected status and open the door to discrimination claims.

Employer use of social media in hiring practices could give rise to disparate treatment claims under Title VII or the Texas Labor Code. Disparate treatment claims could arise if an employer looks at social media profiles of some applicants, but not others, and uses that information to evaluate suitability of the candidate. Conducting a search of social media only for female applicants and deciding not to extend interviews to those who are pregnant, are of child-bearing age or who already have children could give rise to disparate treatment claims. Likewise, evaluating information gathered from social media sites differently based on protected status could give rise to disparate treatment claims. For example, if two equally qualified candidates have posted pictures on their profiles and one posts that he is from Dallas, Texas, and the other Mexico City, Mexico, and the employer decides that the applicant from Dallas might be a "better fit" with the company culture, then that could give rise to a disparate treatment claim.

Not only could using social media to screen applicants give rise to a claim of disparate treatment under Title VII and the Texas Labor Code, but it could also give rise to a claim of disparate impact. Disparate impact claims assert that a hiring practice that was not necessarily intended to be discriminatory, nonetheless, has an adverse impact on a group of applicants whose protected status is recognized under the law. Social media websites, particularly LinkedIn, have lower percentages of Latino and African American users than are in the general population.[20] Facebook has more users that are under 40 than over 40.[21] Only considering applicants who have a social media profile on LinkedIn or Facebook, though seemingly harmless, could give rise to liability.

Employers who are federal contractors have an even greater burden. The Office of Federal Contract Compliance Programs (OFCCP) requires that federal contractors keep detailed records on the backgrounds of job applicants, including the sources contractors use to find job candidates. Although there appears to be no clear guidance from the OFCCP on the use of social media, because contractors must track internet usage in connection with job posting and expressions of job interest, this could potentially include tracking and documenting use of social media.

Employers who take disciplinary action against existing employees based on information obtained from social media can also subject themselves to litigation. For example, in *Marshall v. Mayor of Savannah*, a female employee filed suit alleging that she was disciplined and eventually terminated based on race and gender in violation of Title VII and for violations of her Constitutional rights under 42 U.S.C. § 1983.[22] Marshall, a firefighter trainee maintained a MySpace account that included photographs of Marshall "fresh out of the shower" posing bare-shouldered, and of her backside.[23] The fire department learned of the photographs from an anonymous caller

---

[18] *See* 42 U.S.C. § 2000e-2 (2012) (Title VII of the Civil Rights Act of 1964) ("Title VII") (prohibiting discrimination on the basis of race, color, sex, national origin and religion); *see also* 42 U.S.C. § 2000e-k (The Pregnancy Discrimination Act) (defining "because of sex" to include "pregnancy, childbirth, or related medical conditions"); Tex. Labor Code § 21.051 (2012) (prohibiting discrimination on the basis of race, color, sex, national origin, religion, age and disability).

[19] *See id*; *see also* Americans with Disabilities Act, 42 U.S.C. § 12112 (2012) (prohibiting discrimination on the basis of an actual or perceived disability); Rehabilitation Act of 1873 § 503, 29 U.S.C. § 701 (prohibiting discrimination in employment against federal employees); Vietnam Area Veterans' Readjustment Assistance Act, 38 U.S.C. § 4212 (2012) (prohibiting discrimination against veterans by federal contractors and subcontractors).

[20] *See Use Social Media Smartly When Hiring*, SOCIETY FOR HUMAN RESOURCE MANAGEMENT (Mar. 19, 2013), http://www.shrm.org/hrdisciplines/technology/articles/pages/be-smart-when-using-social-media-for-hiring.aspx.

[21] *Report: Social network demographics in 2012*, PINGDOM (Aug. 21, 2012) http://royal.pingdom.com/2012/08/21/report-social-network-demographics-in-2012/.

[22] *See Marshall v. Mayor of Savannah*, 366 F. App'x 91 (11th Cir. 2010).

[23] *Id.* at 93.

issued Marshall an oral reprimand.[24] When Marshall requested to see the photos that formed the basis for the reprimand and demanded to know who else knew about the photographs, she was terminated for her "combative tone" and "disrespect toward administration and Chief officers."[25] Marshall claimed that no similarly situated male, white or black employees were subjected to discipline for similar offenses.[26] The Eleventh Circuit affirmed the district court's award of summary judgment in favor of the employer, finding that Marshall failed to establish that other employees outside her protected class were treated differently when she could not provide any evidence that the fire department was aware of any other employee's MySpace photographs.[27]

B. Harassment

Employee conduct, on and off employer premises, could potentially give rise to liability fro public and private employers. Employee conduct via the Internet is no exception. For example, a supervisor's posting of a sexually suggestive comment on an employee's social media page about his or her appearance could form the basis of a sexual harassment claim under Title VII or the Texas Labor Code, whether or not the comment was posted during work hours or on work premises. Employer monitoring of employee use of social media could also give rise to a claim of sexual harassment if through the employer's monitoring it knew or should have known of sexual harassment by an employee against another.[28]

In *Yancy v. U.S. Airways, Inc.*, a male employee posted a photograph on Facebook of the plaintiff leaned over her desk while sleeping.[29] In the photograph, the female employee's thong underwear and part of her buttocks were exposed.[30] Eight months after the photograph was posted, the plaintiff discovered it and reported it to human resources, who investigated and subsequently disciplined the three employees responsible for the photograph and posting.[31] The plaintiff nevertheless pursued suit against U.S. Airways on the basis of the Facebook posting alleging sexual harassment and retaliation after she was selected for furlough.[32] Although the court ultimately granted U.S. Airways' motion for summary judgment, the company incurred the expense of retaining outside counsel to defend against the suit before the district court and on appeal to the Fifth Circuit Court of Appeals.[33]

Additionally, individual employees may be criminally liable for harassing co-workers via online or text communications. Texas Penal Code 33.07 makes it unlawful to send "an electronic mail, instant message, text messages, or similar communication" referencing any identifying information of another person. Further, if the employer knows or has reason to know that an employee is engaging in unlawful conduct under section 33.07, the employer could potentially be vicariously liable for the employee's action.[34]

C. Retaliation

Employee complaints about employers may also be protected by anti-retaliation provisions in Title VII, the Americans with Disabilities Act (ADA), Age Discrimination in Employment Act (ADEA), the Genetic Information Nondiscrimination Act (GINA), and the Texas Labor Code.[35] These statutes prohibit public and private employers from taking adverse employment action against employees for engaging in "protected activity."[36] An employee has engaged in "protected activity" if he or she has either: (1) opposed any practice made an unlawful employment practice; or (2) made a charge, testified, assisted or participated in any manner in an investigation, proceeding or hearing under the statutes.[37] Thus, employee complaints of alleged discrimination against them or others, threats to file a charge of discrimination, picketing in opposition of discrimination or refusing to obey directives believed to be discriminatory could

---

[24] *Id.* at 94.
[25] *Id.* at 95-96.
[26] *Id.* at 96.
[27] *Id.* at 98-100.
[28] *See Burlington Indus. v. Ellerth*, 542 U.S. 742 (1998) (holding that an employer is negligent with respect to sexual harassment if it knew or should have known about the conduct, but failed to stop it).
[29] *Yancy v. U.S. Airways, Inc.*, 469 F. App'x 339, 341 (5th Cir. 2012).
[30] *Id.* at 341.
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Burlington Indus.*, 542 U.S. at 742.
[35] *See* Title VII, 42 U.S.C. § 2000e-3(a) (2012); ADA, 42 U.S.C. § 12203(a)-(b) (2012); ADEA, 29 U.S.C. § 623(d) (2012); GINA, 42 U.S.C. § 2000ff *et. seq*. (2012).
[36] *See* Title VII, 42 U.S.C. § 2000e-3(a) (2012); ADEA, 29 U.S.C. § 623(d) (2012) (nearly identical to Title VII's anti-retaliation provision); 42 U.S.C. § 12203(a)-(b) (2012) (providing that no person shall discriminate against an individual because such individual has opposed an y act or practice made unlawful by the ADA or because such individual made a charge, testified, assisted, or participated in an y manner in any investigation, proceeding or hearing under the ADA); *see also* Fennell v. First Step Designs, Ltd., 83 F.3d 526, 535 n.9 (1st Cir. 1996) (Observing that "[t]he analytical framework for ADEA discrimination and retaliation cases was patterned after the framework for Title VII cases.").
[37] Title VII, 42 U.S.C. § 2000e-3(a) (2012).; *see also Haynes v. Pennzoil Co.*, 207 F.3d 296 (5th Cir. 2000).

potentially give rise to liability for retaliation.

The U.S. Supreme Court takes an expansive view of "opposition" for purposes of retaliation claims arising under federal anti-discrimination statutes. In *Crawford v. Metropolitan Gov't of Nashville and Davidson Cnty, Tennessee*, the court concluded that an employee's mere answering of questions during an investigation of a sexual harassment complaint constituted "opposition" under Title VII, and therefore could form the basis of a retaliation claim.[38] Similarly, the U.S. Supreme Court held in *Thompson v. North America Stainless, LP*, that the plaintiff was an "aggrieved person" under Title VII, despite that he had not personally engaged in protected activity.[39] In *Thompson*, the court held that Title VII's anti-retaliation provision prohibits employers from taking adverse employment action against the plaintiff for his fiancé's protected activity.[40]

Employers who take action against employees based upon an employee's protected activity on social media websites may be vulnerable to retaliation lawsuits. In *Deneau v. Orkin, LLC*, an employee filed suit against her employer for violation of Title VII alleging that she was terminated in retaliation for posting on her Facebook page: "anyone know a good EEOC lawyer? I need one."[41] The employer moved for summary judgment on her claim. Interestingly, the employer did not contest, but presumed, that the employee had engaged in "protected activity" under Title VII when she posted the Facebook comment seeking an employment attorney.[42] Instead, the employer argued that she failed to establish a causal link between her Facebook post and the employee's termination.[43] The court disagreed and found that the one-week proximity between the Facebook post and her termination, combined with the employer's awareness of the Facebook post prior to her termination was sufficient to state a *prima facie* case of retaliation.[44] Nevertheless, the court ultimately granted the employer's motion for summary judgment when the employee was unable to proffer evidence that the employer's stated legitimate, non-retaliatory reasons for her termination were pretext for unlawful retaliation.[45]

In a similar lawsuit, however, the outcome was not so favorable to the employer. In *Stewart v. CUS Nashville, LLC*, an employee filed suit against her former employer alleging that she had been constructively discharged after her employer retaliated against her for joining an existing discrimination lawsuit against the company.[46] The court found evidence that the employee's former supervisor posted on his Facebook page: "Dear God, please don't let me kill the girl that is suing me . . . that is all . . ."[47] The court found that the supervisor's Facebook post, combined with evidence that he stated, "[w]hy does everyone sue? I'm tired of all these bi***es taking out their issues on our company. They're f***ing idiots,"[48] created a fact issue sufficient to survive summary judgment on the retaliation claim.[49]

Other federal statutes with anti-retaliation provisions may provide additional protections for employees from adverse employment action based upon information learned from social media. The National Labor Relations Act (NLRA), the Fair Labor Standards Act (FLSA), the Occupational Safety Health Act of 1970 (OSHA), and the Employment Retirement Income Security Act of 1974 (ERISA) all contain retaliation prohibitions.[50]

For example, the FLSA prohibits an employer from discharging or discriminating in any other manner against an employee because he or she has "filed any complaint" or instituted any proceeding under the Act.[51] The U.S. Supreme Court has interpreted the FLSA's requirement that a complaint be "filed" liberally to include protection from retaliation for oral complaints.[52] Public employers must be especially conscious of employee complaints in social media venues. Employee complaints alleging that governmental entities have engaged in unlawful activity may give rise to protection under the Texas Whistleblower Act or federal whistleblower statutes such as Sarbanes-Oxley.[53] Although the Texas Whistleblower Act limits protection from retaliation to reports made to an "appropriate law enforcement authority," the Act does not specify the medium though, which an employee must make his report to trigger protection under the Act.[54] Thus, it is possible

[38] *Crawford v. Metro. Gov't*, 555 U.S. 271, 276 (2009).
[39] *Thompson v. N. Am. Stainless, LP*, 131 S. Ct. 863, 870 (2011)
[40] *Id.*
[41] No. 11-00455-B, 2013 WL 2178045, at *15 (S.D. Ala. May 20, 2013).
[42] *Id.* at *16.
[43] *Id.*
[44] *Id.* at *14.
[45] *Id.* at 18.
[46] *See Stewart v. CUS Nashville, LLC*, No. 3:11-CV-0342, 2013 WL 456482, at *1 (M.D. Ten. Feb. 6, 2013).
[47] *Id.* at *4, 11.
[48] *Id.*
[49] *Id.* at *11.
[50] *See* NLRA, 29 U.S.C. § 158(a)(4) (2012); FLSA, 29 U.S.C. § 215(a)(3) (2012); OSHA, 29 U.S.C. § 660(c)(1) (2012); ERISA, 29 U.S.C. § 1140 (2012).
[51] 29 U.S.C. § 215(a)(3).
[52] *Kasten v. Saint-Gobain Performance Plastics Copr.*, 131 S.Ct. 1325, 563 U.S. 1325, 179 L Ed. 2d 379 (2011).
[53] *See, e.g.*, Tex. Gov't Code §§ 552.001, 554.035; *see also* Sarbanes-Oxley, 18 U.S.C.§ 1514A (2012).
[54] Tex. Gov't Code § 554.002; *see also* State v. Lueck, 290 S.W.3d 876 (Tex. 2009).

that an employee's posting of a comment to a website or Facebook page maintained by "appropriate law enforcement authority" could be sufficient to trigger the Act's protection. If an employer took action against the employee based on the employee's posting, it could give rise to a claim under the Texas Whistleblower Act.[55]

D. First Amendment

Public employers have the heightened obligation to ensure that their social media policies do not infringe on an employee's First Amendment rights. Public employers may only discipline their employees for inappropriate social media activity if the activity does not fall under First Amendment free speech protections. But, what can be considered "speech" in social media? Can a Facebook post or Tweet constitute protected speech under the First Amendment? Can "liking" or "friending" a Facebook page engender free speech protection?

Speech is protected if it is made as a citizen regarding a matter of public concern.[56] That is not to say, however, that public employers have no right to restrict speech. The employee's rights and thus the employer's limitations on them turn on whether speech is a matter of public concern. Whether speech is a matter of public concern is determined by the form, content and context of expression. If it is political, social or a concern to the community then it is public.[57] If the speech concerns a purely personal interest, however, the First Amendment does not afford protection.

Even if the speech is made by a citizen on a matter of public concern via social media, is there a legitimate government interest in regulating the "speech?" In other words, can a government entity's interests in maintaining employee privacy, organizational security, and a productive and efficient workplace justify restrictions on social media "speech?" The government may permissibly restrict the speech if the government's interest in an efficient workplace outweighs the employee's First Amendment interests.[58] Factors the court considers include whether the speech is disruptive of the workplace, if it affects other employees' performance and loyalty and whether it affects public confidence in the office. *Id*.

Third, even if the employee's First Amendment interests outweigh those of the government, the employee still must show that his speech was the substantial or motivating factor for his termination. He must prove that "but for" his speech he would not have been terminated or disciplined.[59]

In *Spanierman v. Hughes*, the court found a school superintendent did not violate the First Amendment rights of a non-tenured high school teacher by refusing to renew the teacher's contract when, the teacher friended students on MySpace to communicate about homework.[60] He also, however, posted pictures of naked men and engaged in peer-to-peer level exchanges.[61] Students complained about the teacher's page and messages, and the teacher was warned to cease communication with students on MySpace.[62] The court found the teacher's behavior to be disruptive of school activity and the school's interest in preventing this activity outweighed the teacher's speech protection.[63]

In *Richerson v. Beckon*, the Ninth Circuit held that a school district did not violate the First Amendment rights of an administrator by demoting her to a teaching position as a result of her postings on a personal blog.[64] The administrator's public blog contained negative comments about fellow school employees, the union, and the school district, which the court found severely impaired her ability to effectively supervise and work with others.[65] The court held that the school district's legitimate interest in the well being of the workplace outweighed the administrator's interest in engaging in her blog speech.[66]

In another case, a student teacher in Pennsylvania was denied her teaching certificate because she posted a picture on MySpace wearing a pirate cap, holding a plastic cup with the caption "drunken pirate."[67] Since the content of her MySpace page was not a matter of public concern, the court found that the posting was not protected by the First Amendment.[68]

E. Stored Communications Act

Employers monitoring employee access to social media could also be subject to liability under the

---

[55] *See, e.g., Gresham v. City of Atlanta*, Civil Action No. 1:10-CV-1301-RWA-ECS, 2011 WL 46011022, at *13-14 (N.D. Ga. Aug. 29, 2011)(applying Georgia Whistleblower Act and holding that plaintiff's Facebook post did not give rise to liability under the Act because it was not made to "a supervisor or other governmental agency" as required by the Act) *report and recommendation adopted in part, rejected in part*, No. 1:10-CV-1301-RWA-ECS , 2011 WL 460101 (N.D. Ga. Sept. 30, 2011).

[56] *Garcetti v. Ceballos*, 547 U.S. 410, 419 (2006).

[57] *Connick v. Myers*, 461 U.S. 138, 146 (1983).

[58] *Pickering v. Board of Education*, 391 U.S. 563, 568 (1968).

[59] *Mt. Healthy City School Dist. Board of Education v. Doyle*, 429 U.S. 274, 287 (1977).

[60] 576 F. Supp. 2d 292, 313 (D. Conn. 2008).

[61] *Id*. at 298-99.

[62] *Id*. at 312.

[63] *Id.*

[64] 337 F. App'x. 637, 639 (9th Cir. 2009).

[65] *Id.*

[66] *Id*. at 639.

[67] *Snyder v. Millersville University*, No. 07-1660, 2008 WL 5093140 (E.D. Pa. Dec. 3, 2008).

[68] *Id.*

Stored Communications Act ("SCA"). The SCA prohibits knowing or intentional unauthorized access to a facility which an electronic communication service is provided.[69] The SCA does not expressly prohibit an employer from accessing employee's stored electronic communications where the communications are stored on employer's systems. But, under the SCA, an employer may only access an employee's stored communications if: (1) the entity is the provider of the service; or (2) the entity is the user of the service and the communication is from or intended for that user.[70] Likewise, the SCA does not prohibit an employer from intercepting communications with the employee's consent. However, where the employer is monitoring an employee's electronic communications stored by a third-party, the SCA restricts the information that can be obtained.

For example, in *Lazette v. Kulmatycki*, a former employee brought action against his former employer and supervisor, alleging violations of the SCA and intentional infliction of emotional distress, where the employer accessed her email from a company-issued Blackberry.[71] Lazette claimed that Verizon provided her with a company-issued Blackberry which she used to access a personal email account. When Lazette turned the Blackberry in to her supervisor believing that the personal email account had been deleted from the phone, she later learned that her supervisor had been accessing her personal emails for nearly eighteen months.[72] The employer and supervisor sought dismissal of the case arguing that Lazette failed to state a claim under the SCA. In denying Verizon and the supervisor's motion to dismiss, the court rejected the defendants' argument that they had authority to access Lazette's email account because she used company-owned property, finding that Lazette neither consented to nor knew her supervisor was accessing her emails.[73] The court further rejected the defendants' argument that the SCA did not apply because the Blackberry was not a "facility" as defined by the statute.[74] The SCA does not define "facility."[75] Nevertheless, the court found that the "electronic communications service" accessed by the employer resided in the Gmail server, not on the Blackberry, and as such, the employer accessed a "facility." Finally, the court held that Lazette sufficiently asserted and that defendants' had admitted that the supervisor was acting within the scope of his employment and in furtherance of Verizon's interests when he accessed Lazette's emails and thus, Verizon was vicariously liable for the supervisor's actions.[76] Under these facts, public and private employers could find themselves liable for violations of the SCA where they have monitored an employee's Facebook posts, Facebook messages, or Tweets if they do so without the employee's clear consent.

In another case, *Pietrrylo v. Hillstone Restaurant Group*, an employer was held liable under the SCA where two supervisors coerced an employee into providing her MySpace account password so that they could view messages on in a chat group where employees vented their frustrations about working at the company.[77] The jury found for the plaintiff and awarded punitive damages against the employer.[78]

Additionally, individual employees may be liable under the SCA, or the Wire Tap Act for accessing an employee's communications.[79] In, *U.S. v. Syzmuszkiewicz,* an IRS agent created a rule in his supervisor's Microsoft Outlook email account that automatically forwarded all the emails received by the supervisor to his inbox.[80] Syzmuszkeiwicz was prosecuted for violation of the Wire Tap Act.[81] Interestingly, Syzmuszkeiwicz contended that he should have been charged under the SCA, rather than the Wire Tap Act, arguing that the rule directed the email system to forward the supervisor's emails only "after the message arrived" rather than a "contemporaneous interception" as required under the Wire Tap Act.[82] The Seventh Circuit noted, "it is risky to defend against one crime by admitting to another,"[83] rejected the defendant's argument, and affirmed his conviction under the Wire Tap Act.[84]

F. Open Meetings Act

The Open Meetings Act requires meetings of governmental bodies in Texas to be open to the public, except for expressly authorized closed sessions, and to post public notice of the date, hour, place and subject matter of the meeting.[85] "Governmental body" under the Open Meetings Act is broadly defined and includes boards, commissions, departments and agencies directed by one elected or appointed members; county commissioners courts; municipal governing bodies;

[69] 18 U.S.C. § 2701(a)(1).
[70] 18 U.S.C.§ 2701(c)(2).
[71] No. 3:12CV2416, 2013 WL 2455937, at *1 (N.D. Ohio June 5, 2013).
[72] *Id.* at *1.
[73] *Id.* at *4.
[74] *Id.* at *5.
[75] *Id.* (citing 18 U.S.C. § 2701(a)(1) (2012)).
[76] *Id.* at *8-9.
[77] No. 06-5754, 2009 WL 3128420, at *1-6 (D. N.J. Sept. 25, 2009).
[78] *Id.* at 4-6.
[79] *See* 18 U.S.C. § 2510 (2012) (also known as the Electronic Communications Privacy Act).
[80] 622 F.3d 701 (7th Cir. 2010).
[81] *Id.* at 704.
[82] *Id.*
[83] *Id.* at 704-05.
[84] *Id.*
[85] TEX. GOV'T CODE § 552.001.

deliberative bodies with rulemaking or quasi-judicial power classified as department, agency or political subdivision of a county; school district boards of trustees; county board of school trustees; county boards of education, governing boards of special districts; local workforce development boards; and certain nonprofit corporations.[86] Likewise, "meeting" is broadly defined as "a deliberation between a quorum of a governmental body . . . during which public business or public policy over which the governmental body has supervision or control is discussed . . ."[87] The provisions of the Act are mandatory and are construed liberally in favor of open government.[88]

With the exception of the Texas Secretary of State who is required to post notice of state governmental body meetings on the Internet, there is no requirement under the Open Meetings Act to maintain a website where notices of meetings can be published online.[89] In fact, Section 551.050 previously provided that municipal governing bodies were required to post notice of each meeting on a bulletin board. [90] However, the section was amended in 2011 to authorize a municipal government body to post its meeting notices on an "electronic bulletin board."[91] The term "electronic bulletin board" means "an electronic communication system that includes a perpetually illuminated screen on which the governmental body can post messages or notices viewable without manipulation by the public."[92] Additionally, Texas law now requires that if a city has a website and a population of over 48,000, it must post the full agenda of any city council meeting on its website.[93] For cities with a population of less than 48,000, cities must only post notice of the time, place and date of the council meeting.[94]

In light of increased use of social media by public employers and their officials and employees, the Senate Committee on State Affairs prepared an Interim Report to the Eighty-second Legislature concerning the impact social media might have on transparency of government entities.[95] The Interim Report acknowledged challenges that new technologies present in complying with the Open Meetings Act and noted:

> The walking quorum concept combined with newer technologies such as microblogs (e.g. Twitter), social media website (e.g., Facebook), text messaging and instant messaging, raise new issues for consideration by the Attorney General, the courts and the Legislature . . . under the current interpretations of the Act, a quorum would exist if a majority of the governmental body discusses public business on a Facebook wall. The Facebook wall could be closed to the public, or open; however absent a prior notice of the "meeting" the [members of the governmental body] could be in violation of the [Act]. . .[96]

The Legislature declined to pass legislation that attempted to tackle this hypothetical scenario posed by the State Affairs Committee. But, it is likely the courts will have the opportunity to do so as use of social media by governmental bodies and officials increases. In fact, just last year in 2012 the Fifth Circuit Court of Appeals had occasion to decide a case with somewhat similar facts that involved two city council officials who were indicted over an email exchange.[97] In *Asgeirsson v. Abbott*, the government argued the email exchange constituted a closed meeting, and was therefore in violation of the Act.[98] The local officials challenged the Act as an unconstitutional restriction on their First Amendment rights.[99] The central issues before the Fifth Circuit were whether the officials' conduct could be considered a "meeting" under the Open Meetings Act, and whether the requirement for a quorum to be present before discussing public business or policy was a content-based restriction on their right to free speech, overbroad or constitutionally vague.[100] The Fifth Circuit disagreed with the officials' position and upheld the constitutionality of the provision. The officials appealed to the U.S. Supreme Court which denied certiorari.[101] Given this case, it not difficult to imagine a scenario contemplated by the Senate State Affairs Committee.

G. Public Information Act

Texas governmental bodies are also subject to the Public Information Act.[102] Additionally, while the

[86] TEX. GOV'T CODE § 551.001(3).
[87] TEX. GOV'T CODE § 551.001.
[88] *See City of Laredo v. Escamilla*, 219 S.W.3d 14, 19 (Tex. App.—San Antonio 2006, pet. denied).
[89] *See* Tex. Gov't Code § 551.048(b)
[90] Tex. Gov't Code § 551.050
[91] *See* Act of May 25, 2011, 82d Leg., R.S., ch. 1007 § 2, 2011 Tex. Sess. Law Serv. 2549 (to be codified as an amendment to Tex. Gov't Code § 551.050)
[92] *Id.*
[93] TEX. GOV'T CODE § 551.056(c).
[94] TEX. GOV'T CODE § 551.056(b).
[95] Senate Committee on State Affairs, Interim Report to the 82d Legislature at 59 (Dec. 2010).
[96] *Id.*
[97] *See Asgeirsson v. Abbott*, 696 F.3d 454 (5th Cir. 2012) *cert. denied*, 133 S.Ct. 1634 (2013).
[98] *Id.* at 458-60.
[99] *Id.*
[100] *Id.* at 459, 464, 466.
[101] *See* 133 S.Ct. 1634 (2013).
[102] *See* TEX. GOV'T CODE § 552.003(1)(A).

Public Information Act does not apply to private persons or businesses simply because they provide goods or services under a contract with a governmental body, entities that are supported in whole or in part by public funds, or that spend public funds are considered "governmental bodies" for purposes of the Public Information Act.[103]

The Public Information Act gives the public the right to request access to government information. Under the Public Information Act, governmental bodies must provide information when requested by the public in accordance with the requirements of the Act.[104] "Public information" as defined by the Act includes all information that is "collected, assembled, or maintained under a law or ordinance or in connection with the transaction of business."[105] If the information is "collected, assembled, or maintained" by the governmental body, it is public information and therefore subject to disclosure unless it can be considered confidential information or an exception applies.

There are no exemptions for information that is kept either exclusively or collectively in electronic form. Under the Act, forms in which public information may exist include books, papers, letters, documents, printouts, photographs, film, tape, microfiche, microfilm, photostat, sound recording, maps, drawings, voice, data or video kept in computer memory.[106] Further, if the information is kept in electronic form, the governmental body must provide a copy in electronic form if requested, and provided that the entity has the technological ability to do so.[107] In this regard, information kept by the governmental body on social media websites is most likely public information subject to disclosure under the Public Information Act if the social media content is maintained by the governmental body. Additionally, governmental bodies have an affirmative duty to retain records and information, regardless of the medium.[108] Thus, information on a governmental body's website or social media page should also be retained in accordance with applicable records retention schedules.

In a case involving the City of Dallas, *City of Dallas v. Dallas Morning News*, the City refused to turn over emails sent to and from the mayor's personal email address requested by the Dallas Morning News under the Public Information Act.[109] In that case, the City of Dallas argued that the emails were not subject to the disclosure because they were not "collected, assembled or maintained" by the City.[110] Whether a document is public information and subject to disclosure depends on several factors. Those factors include:

(1) who prepared the document;
(2) the nature of the contents;
(3) the purpose of the document;
(4) who possessed the document;
(4) who had access to the document;
(5) whether the governmental body required the preparation of the document;
(6) whether the document was necessary for official business[111]

The district court disagreed with the City of Dallas and held that the mayor's personal emails became public when she engaged in communication related to her authority as mayor, regardless of whether those communications were sent via her personal email address.[112] The City of Dallas appealed and the case was remanded back to the trial court to determine the amount of access the City had to the mayor's personal emails.[113] On remand, the City of Dallas filed a plea to the jurisdiction arguing that the trial court lacked subject matter jurisdiction over the case, which was affirmed in part and reversed in part.[114] It is not a stretch of the imagination then to say understand how a Facebook post or Tweet by a city employee or official could be considered public information under the Public Information Act if the post or tweet can be considered related to official city business.

H. National Labor Relations Act

Importantly for purposes of this article, it is imperative to keep in mind that the NLRA does not apply to the United States government or any state or political subdivision.[115] Therefore, public employers are not subject to liability for violations of the NLRA or the National Labor Relations Board's (NLRB) jurisdiction. Nevertheless, the NLRA and the actions

[103] Tex. Gov't Code § 552.003(1)(S)(xii); *see also* Open Records Decision No. 1 (1973) (concluding that bank that holds funds of governmental body is not subject to Act).
[104] TEX. GOV'T CODE § 552.003(1)(A).
[105] TEX. GOV'T CODE § 552.002.
[106] TEX. GOV'T CODE § 552.002(c).
[107] TEX. GOV'T CODE § 552.228.
[108] TEX. GOV'T CODE § 552.203; *see also* Tex. Loc. Gov't Code §§ 203.025(a), 203.026(a). (requiring local governments to designate a records management officer and establish a records management program).

[109] *See City of Dallas v. The Dallas Morning News, LP*, 281 S.W.3d 708 (Tex. App.—Dallas April 9, 2009, no pet.).
[110] *Id.* at 710.
[111] *Id*.
[112] *Id.* at 718.
[113] *See City of Dallas v. The Dallas Morning News*, 331 S.W.2d 141 (Tex. App.—Dallas 2010).
[114] *See Id.*
[115] 29 U.S.C. § 152(2) (2012) (excluding government employers from the definition of employer).

taken by the NLRB bear mentioning here because increased scrutiny and activity concerning issues related to private employer's social media policies inform best practices for all employers who maintain such policies.

That said, the NLRA restricts private employers' actions concerning employee rights to engage in collective action. Section 7 of the NLRA provides:

> Employees shall have the right to self-organization, to form, join, or assist labor orgnaizations, 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 . . .[116]

Activity is "concerted" when an employee acts "with or on the authority of other employees and not solely by and on behalf of the employee himself; also includes activity where individual employees seek to initiate or to induce or to prepare for group action."[117]

Section 7 rights as discussed above are enforced through Section 8 of the NLRA. According to the NLRB, an employer violates Section 8(a)(1) of the NLRA when a work rule "would reasonably tend to chill employees in the exercise of their Section 7 rights."[118] The rule is examined through a two-step test to determine whether it is unlawful.[119] First, it must not explicitly restrict Section 7 activities." If the rule does not specifically restrict these protected activities, it will only violate Section 8(a)(1) when the employee can show: (1) "that employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights."[120]

For example, in *Hispanics United of Buffalo*, an employee posted a status update on her Facebook page stating that the employer messed up and that she was no longer going to be a good employee because she was transferred to a different department within a collections agency.[121] Other coworkers agreed with her sentiment. When the employer discovered the post, it immediately terminated the employee because her comments were in violation of the employer's policy prohibiting employees from "making disparaging comments about the company through any media, including online blogs, other electronic media or through the media."[122] The NLRB found the employer's policy unreasonably restricted Section 7 activity because it prevented employees from discussing unfair treatment or pay.[123]

On the other hand, the employer is not liable if he can establish that the employee's conduct interfered with the employee's own work or that of other employees or actually interfered with the employer's operations and the employer can show that the interference was the reason for the discipline.[124] This issue arose when an employee of a home improvement store updated her status after she was reprimanded.[125] The NLRB found that her discharge was lawful because her status did not create a discussion about terms and conditions of employment with her coworkers. Rather, only one coworker "liked" her status, no coworkers responded to the post, and the employee used an expletive and the name of her employer's store on her status.[126]

The NLRB has recently engaged in vigorous scrutiny of employer social media policies and has unequivocally stated that social media policies that infringe on employee's rights to engage in concerted activity will result in liability. Rules that prohibit employee solicitation on company property during non-work time, or that discourage employees from discussing terms and conditions of employment or their employer in a disparaging or negative way will not pass muster under NLRB scrutiny.[127] The NLRB also routinely finds employers liable for NLRA violations whose social media policies contain ambiguous language that prohibits generally conduct that is "disrespectful" or "inappropriate."[128]

IV. BEST PRACTICES FOR SOCIAL MEDIA POLICIES

It is evident that private and public employers alike are facing claims based on allegations arising from employee use of social media. Examining the areas of potential liability, however, should inform

---

[116] 29 U.S.C. § 157 (2012).

[117] *Meyers Industries (Meyers I)*, 268 NLRB 493, 497 (1984), revd. sub nom. *Prill v. NLRB*, 755 F.2d 941 (D.C. Cir. 1985), cert. denied 474 U.S. 948 (1985), on remand *Meyers Industries (Meyers II)*, 281 NLRB 882 (1986), affd. sub nom. *Prill v. NLRB*, 835 F.2d 1481 (D.C. Cir. 1987), cert. denied 487 U.S. 1205 (1988).

[118] *Lafayette Park Hotel*, 326 NLRB 824, 825 (1998), enfd. 203 F.3d 52 (D.C. Cir. 1999).

[119] *Lutheran Heritage Village-Livonia*, 343 NLRB 646, 647 (2004).

[120] *Id*.

[121] 359 NLRB No. 37 (Dec. 14, 2012).

[122] *Id.*

[123] *Id.*

[124] *The Continental Group, Inc.*, 357 NLRB No. 39, slip op. at 4 (2011).

[125] *Id.*

[126] *Id.*

[127] *Id.*

[128] *See, e.g.*, Walmart, No. 11-CA-067171, NLRB Advice Memorandum (May 30, 2012); *Cox Communications*, No.17-CA-087612, NLRB Advice Memorandum (Oct. 19, 2012); OM 12-59, NLRB Operations Management Memorandum (May 30, 2012).

employers' social media policies in such a way that the risks associated with employer and employee use of social media can be mitigated. Prudent public and private employers will develop and maintain social media policies with these areas of potential liability in mind. In doing so, best practices have emerged that have largely been learned from the private sector and greatly informed by decisions and opinions from the NLRB.

Social media policies are aimed at minimizing the risk of litigation that could arise from employee professional and personal use of social media. Accordingly, components of prudent social media policies will address:

(1) Employee access to social media
(2 Management of the organization's social media account
(3) Defining acceptable use
(4) Regulating employee conduct
(5) Managing content
(6) Legal considerations:

- Applicable state, federal and local laws
- Intellectual property
- Union/organized employees
- Data/document retention

(7) Managing customer/citizen-generated conduct
(8) Maintaining appropriate security of data and technological infrastructure[129]

Keeping in mind the most common areas of potential employer liability previously discussed and the components of a comprehensive social media policy listed above, here are some best practices all employers should apply in drafting social media policies.

A. Best Practices for Screening Applicants

1. Create a Wall

Create a wall between the human resources professional reviewing application and determining qualifications/eligibility for hire and the decision-makers who ultimately make the hiring decision. Do not use surreptitious measures to obtain social media information.

2. Define the Process

Define the process for researching social media. Provide clear instructions to human resource professionals regarding the following: (1) Which social media websites will be researched? (2) When during the application process will social media websites be researched? (3) How will the research be documented?

3. Establish the Relevance

Be able to explain how information obtained from social media is relevant to the job requirements or is otherwise an indicator of job performance. This may mean that information on LinkedIn may be relevant (i.e. resume, references, connections, past work experience, recommendations), while information on Facebook may not. Questions to consider when determining if and what information learned from social media may be relevant to the job qualifications include:

- Job Description
- Decision-maker specifications/desires
- Geography
- Company policies that set expectations for employee culture and behavior

Finally, document the universe of information considered relevant to the job.

4. Document the Purpose and the Search

Document what is searched and the purpose of the search. This can be done at the outset of the job search by reviewing the job description and determining which social media sites could be informative as to which qualifications and documenting which websites will be reviewed. Alternatively, this can be done by keeping a log per applicant of what was searched and which qualification it pertains to.

5. Be Consistent

Be consistent in the search and apply the search uniformly for the position to be filled. If that it has been determined based on the job qualifications or expectations that information on LinkedIn and Twitter could be relevant to the job qualifications for the position, be consistent in searching LinkedIn and Twitter for each applicant. Do not expand or narrow your search depending on the applicant to "rule out" or eliminate otherwise qualified applicants.

6. Notify the Applicant

Inform the applicant of the pre-employment screening process and that any available information in the public domain may be considered, including information available on the Internet and social media websites in making the employment decision. If using a third party to gather background information, including information available on the Internet, get the applicant's written consent.

[129] *See Designing a Social Media Policy for Government: Eight Essential Elements*, Center for Technology in Government (May 2010), http://www.ctg.albany.edu/publications/guides/social_media_policy/social_media_policy.pdf.

B. Best Practices for Existing Employees

1. Protect Trade Secrets

Employers may permissibly prohibit disclosure of trade secrets, confidential, proprietary, financial or internal information not otherwise generally available to the public. This may include, but is not limited to the organizations' systems, reports, processes, products sold, forthcoming product releases, know-how, training, technology, policies, procedures, pricing, customer lists or contacts, company strategies, or internal communications concerning the organization. Employers should also prohibit use of organization's trademarked, copyrighted materials or other intellectual property.

2. Protect Confidential Information

Prohibit disclosure of private or identifying information concerning the organization, its employees, vendors, suppliers, customers, business partners or competitors including information that is prohibited from disclosure by law. This includes protected medical information, social security numbers, marital status, etc.

3. Prohibit False, Abusive or Defamatory Comments

Prohibit employees from posting material that is intentionally false, abusive, intimidating, threatening, offensive, insulting, humiliating, pornographic, profane, malicious, or that would incite violence or could constitute bullying regarding the organization, its employees, vendors, suppliers, customers, business partners or competitors.

4. Prohibit Discrimination, Harassment and Retaliation

Prohibit employees from engaging in any conduct that may be construed as harassment based on race, ethnicity, national origin, religion, sex, sexual orientation, age, disability, or any other legally protected characteristic. Prohibit employees from retaliating against individuals on the basis of social media posts or messages.

5. Designate an Authorized Spokesperson

Designate an authorized spokesperson to make statements on behalf of the organization on the organization's website or social media pages. Prohibit employees who have not been specifically authorized from making representations that they are spokespersons for or otherwise authorized to speak on behalf of the organization or stating that their views represent that of the organization unless they have received express authorization from such an authorized person.

6. Discourage Personal Use of Social Media During Working Time

Discourage use of social media while on working time or on equipment provided by the organization during working time, unless it is work-related. Encourage use of social media consistent with the organization's Social Media Policy and Company Equipment Policy.

7. Discourage Use of Work Email for Personal Use

Employers should also discourage personal use of organization email addresses to register on social networks, blogs or other social media websites utilized for personal use.

8. Provide Notice of Consequences for Violations of the Social Media Policy

Inform employees that in the event the organization's social media policy is violated, whether the conduct occurs after-hours or on the employee's own equipment, it can subject the employee to disciplinary action up to and including immediate termination, and could subject the employee to criminal liability under Tex. Penal Code § 33.07.

9. Be Specific

Do not leave the social media policy open to interpretation. Avoid words that discourage ambiguous conduct like "inappropriate," "distasteful," "unfavorable," "critical," or "obscene." Instead, use words that encourage conduct the organization would consider appropriate like "respectful," "courteous," "fair," "honest," and "accurate."

10. Eradicate Any Expectation of Privacy

Advise employees that they should not have an expectation of privacy when using social media on organization equipment and that any and all information, including deleted information, is subject to disclosure. State that the organization reserves the right to access any organization computers, electronic communication devices and network, including email and Internet use. But, if the organization accesses employee communications, have a documented business reason for doing so (i.e. monitoring company charges/expenses). Do not search social media for reasons to take employment action without some complaint or reasonable suspicion that a policy or law is being violated, such as a human resources complaint or an instance where review of charges/expenses merits a closer look.

11. Be Consistent

Be fair and consistent in applying the social media policy. If disciplinary action is taken based on a social media post make sure the punishment fits the crime.

Consider and rule possible retaliation that could have influenced the employment decision.

12. Train Employees on Use of Social Media

Be sure to train all employees concerning the organization's social media policy. Document attendance at training and consider getting a signature from the employee acknowledging receipt of and training on the social media policy.

13. Monitor the Organization's Website and Social Media Pages

Designate an employee to be responsible for updating and monitoring the organization's website and social media pages. Employers should not be caught unaware of information, posts or comments on their websites or social media pages that the organization maintains.

14 Retain Information from the Organization's Website and Social Media Pages

Retain information posted to the organization's website and social media pages in accordance with the organization's document retention policy, litigation holds, and applicable laws. This can be done via daily screen shots stored on a hard drive, or through a third-party vendor who specializes in storing archived Internet data.

15. Include a Disclaimer

Include a disclaimer that the social media policy is not intended to restrict an employee's right to discuss the terms and conditions of his or her employment, including hours, wages, and working conditions. State affirmatively that employees will not be disciplined or retaliated against for engaging in conduct that is lawful and consistent with the organization's social media policy.