An Employer's Guide to the Twitterverse: Rules, Strategies and Advice regarding Social Media Use by Prospective, Current and Past Employees

Christopher A. Page
Young Moore and Henderson, P.A.
Raleigh, North Carolina

October 12, 2018

The Hospitality and Retail Industries are part of the social media revolution, and not just in the way their members do their marketing. Their employees are the "twitterati," and even if they don't tweet, they are communicating with friends, colleagues, and the world via other social media platforms and sharing information that frequently concerns their experiences and observations about their work. Sound problematic? This is just the engraving on the outside of the Pandora's Box that is social media for the employer.

The legal landscape is rapidly evolving for employers because of social media. While social media presents many benefits and opportunities for every company, it also brings with it a substantial number of legal traps and problems for the employer. The purpose of this paper is to highlight the legal issues that employers have to face that arise directly out of a prospective or current employee's use of social media, and to offer a brief synopsis of the current state of the law on those issues. Each issue is the subject of multiple scholarly articles, but even with concerted study, an employer must remain vigilant in keeping abreast of current law because the case law is developing at a breakneck pace.[1]

In the new world dominated by social media, it is vital that an employer understand the relevant issues, stay well-informed on the state of the law, have an appropriate hiring policy in place regarding use of social media in screening job applicants, also have a clear, workable and enforceable social media policy in place for its employees, and lastly, understand how the rules and strategies for social media change when it comes to dealing with claims by past employees.[2]

The relationship between employer and employee is governed by contract and by state and federal laws. There are things an employer can and can't do during the job application process, and information that it can and cannot consider as it evaluates prospective job applicants. Likewise, the federal constitution and state and federal statutes dictate what an employer can and can't do in how it treats its employees and/or allows them to be treated.

Social media impacts this relationship greatly by *expanding* the arena in which information and conduct are exchanged. Social media provides much more information to the

---

[1] Just this past week, the Fourth Circuit became the first circuit court to rule that "liking" someone on Facebook was an exercise of the first amendment right to free speech, and thus, ruled that six sheriff's deputies who had "liked" their boss's election opponent should not have been fired. *See Bland v. Roberts* at http://www.ca4.uscourts.gov/Opinions/Published/121671.P.pdf.

[2] *See* Page, "Time to 'Friend' Facebook? Using Social Media to Win Your Case," Westlaw Journal of the Computer and the Internet, Vol. 31, Issue 8 (September 19, 2013).

employer during the job application process , and this is not necessarily a good thing. Likewise, harassment and discrimination now can occur not just within the four walls of an employer's worksite, but also via social media postings. Similarly, statements that employees used to exchange at the "water cooler" are now exchanged on a digital water cooler called the world wide web. All of those things that employees were allowed to gripe about at the water cooler and not lose their job over? They can still say them, even if the world is listening in.

Before we get to the relevant statutory and case law for employers in dealing with social media, let's take a look at the industry landscape.

The Train Has Officially Left the Station.

Retail companies did not miss the social media revolution. Rather, they embraced it wholeheartedly. A few statistics prove the point:[3]

YouTube:

- **700 YouTube video links are shared on Twitter every minute.**
- **500 years of YouTube videos are watched on Facebook every day.**
- **The equivalent of 100 hours of video is uploaded to YouTube each minute.**
- **99% of US online specialty retailers use YouTube, up from 93% in 2012.**

Facebook:

- **79% of social media log ins by online retailers are with Facebook, compared to 12% for Google+, and 4% for Twitter.**
- **Facebook will account for 13% of worldwide mobile ad revenue in 2013.**
- **Facebook users share 2.5B pieces of content on the site each day.**
- **70% of business-to-consumer marketers have acquired a customer through Facebook.**

LinkedIn:

- **43% of US marketers have found a customer through LinkedIn.**
- **61% of social media users primarily use LinkedIn for professional networking.**
- **60% of LinkedIn users have clicked on an ad on the site.**

[3] *See* http://socialmediatoday.com/node/1656466 (August 11, 2013) (citations omitted).

- **51% of online business-to-consumer marketers use LinkedIn, compared to 83% for business-to-business.**

Twitter:

- **Twitter users send 400M tweets each day.**
- **50% of technology companies have acquired a customer through Twitter.**
- **25% of consumers who complain about products on Facebook or Twitter expect a response within 1 hour.**
- **69% of online business-to-consumer marketers use Twitter, compared to 80% for business-to-business.**

Google+

- **70% of brands have presences on Google+, up 4% from Q4 2012.**
- **41% of online business-to-consumer marketers use Google+, compared to 39% for business-to-business.**
- **12% of social media log ins by online retailers are with Google+.**
- **Facebook's share of social logins dropped from 54% to 49% during 4Q12, while Google's share increased from 25% to 31%.**

Pinterest:[4]

- **90% of US online specialty retailers use Pinterest, up from 81% in 2012.**
- **83.8% of luxury brands have a presence on Pinterest.**
- **69% of brands have presences on Pinterest, up 10% from Q4 2012.**
- **25% of online US women use Pinterest, compared to 5% for men.**

Instagram:

[4] Pinterest is the fastest growing social media network. *See* http://www.business2community.com/social-media/12-awesome-social-media-facts-statistics-2013-0622265. Other interesting statistics from this study: (1) Google+ is catching up to Facebook in terms of users; (2) LinkedIn is most popular for older users and professionals; (3) Usage of social media networks by older users is increasing; and (4) the Asia Pacific region dominates social network usage.

- **41% of brands post 1 or more photos per week to their Instagram accounts, up from 34% in Q4 2012.**

- **59% of brands have presences on Instagram, up 9% from Q4 2012.**

- **17% of teens say Instagram is the most important social network, up from 12% in 2012.**

Social Media: The Means for Getting into Trouble for Employees and Employers Alike.

Clearly, companies worldwide see social media as the new medium to reach customers. But those companies have employees, whose own use of social media can cause their employers both business and legal problems, including:

- Claims by coworkers against the company for harassment, negligent retention or supervision, or infliction of emotional distress[5]
- Trade secret disclosures
- Comments damaging the company's reputation and business interests[6]
- Defamation
- Intellectual property infringement
- Disclosure of private customer and client information
- Fraud
- Unfair competition claims
- Securities laws claims
- Privacy related torts
- Violation of Non-Compete agreements;[7] and
- False endorsement and FTC Endorsement Guide issues[8]

[5] An employer is subject to vicarious liability to a victimized employee for an actionable hostile environment claim created by a supervisor with immediate authority over the employee. *Burlington Industries, Inc. v. Ellerth*, 524 U.S. 742, 765 (1998). Employers may also be liable if it knows or has reason to know of work-related harassment occurring on social media. *See, e.g., Faragher v. City of Boca Raton*, 524 U.S. 775, 779; Folkerson v. Circus Circus Enterprises, Inc., 107 F.3d 754, 756 (9th Cir. 1997); *Blakey v. Continental Airlines*, 2 F. Supp. 2d 598 (D.N.J. 1998); *Amira-Jabbar v. Travel Services, Inc.*, 726 F. Supp. 2d 77 (D. P. R. 2010)

[6] *E.g.*, Chrysler had a contract with a social media marketing firm, New Media Strategies, which managed its social media websites. In early March 2011, a tweet was posted on ChryslerAuto's Twitter account which stated "'I find it ironic that Detroit is known as the #motorcity and yet no one here knows how to f***ing drive.'" The tweet was posted by a now former employee at New Media Strategies and was quickly removed from Twitter. However the next day, Chrysler announced that it would "'not renew its contract with New Media Strategies . . . for the remainder of 2011.'" *See* http://www.informationweek.com/internet/social-network/chrysler-addresses-twitter-foul-up/229300704.

[7] *See, e.g., Amway Global v. Woodward*, No. 09-12946, 2010 WL 3927661 (E.D. Mich. Sept. 30, 2010) (refusing to overturn arbitrator's award for, among other things, defendant's violation of a nonsolicitation agreement for posts on a blog); *TEKsystems, Inc. v. Hammernick*, No. 10-cv-00819-PJS-SRN (D. Minn. 2010) (alleging violations of non-compete, non-solicitation, and non-disclosure agreements when defendant contacted current contract employees via LinkedIn).

[8] In October 2009, the FTC updated its Guides Concerning the Use of Endorsements and Testimonials to include social media activities. *See* 16 C.F.R. § 1255. As a result, employees commenting on company products and services must now disclose company affiliation. Failure to do so could result in liability for an employer.

Once employers become aware of conduct by employees in social media, employers must consider the legal ramifications stemming from firing employees, including the following potential claims by employees:

- Off-Duty conduct laws
- Retaliation under Title VII and state laws
- Whistleblowing under Sarbanes-Oxley
- Discrimination under Title VII and state laws
- Concerted action under the NLRA
- Invasion of Privacy, and
- Stored Communications Act.

We'll talk about some of those in more detail below.

Social Media and the Hiring Process

Employers are not just using social media to gain business. They are using it in their hiring processes. A recent study indicated that 45% of employers questioned used social media to screen job applicants; and that 35% of these employers decided not to offer a position to a job applicant based on information found on the applicant's social networking site. The study also indicated that Facebook was the most popular online site for screening job applicants, whereas 7% of employers investigated job applicants on Twitter.[9] The most common reasons for not hiring an applicant were provocative pictures, references to drinking and drug use, and negative comments about previous employers and coworkers.

A Microsoft Research study in 2010 indicated that 75% of companies have formal policies requiring hiring personnel to conduct some sort of online research of applicants.[10] 70% of employment recruiters admitted that they had rejected job applicants based on information they found online. 86% of recruiters have informed the candidate for the reason for the rejection.

The Wall Street Journal also reported on a study of 215 recruiters by the Corporate Executive Board that indicated that 44% of recruiters stated that "trashing" an employer on social media is a sufficient reason not to hire an applicant. The Wall Street Journal also reported on a study of "Likes" by Facebook users which indicated that the participants unintentionally revealed and shared very private and intimate personal information, for example, their religious and political views, divorce, drug use, and sexual orientation.[11]

There is no question that social media can provide a wealth of information not typically found during the standard application process, including information relating to demographic statuses protected by federal law: race, color, religion, sex, national origin, age, disability,

[9] Cavico, et al. "Social Media and the Workplace: Legal, Ethical and Practical Considerations for Management" Journal of Law, Policy and Globalization, Vol. 12, 2013 at 4.
[10] *See* http://www.slideshare.net/opinionwatch/online-reputation-for-job-seekers-report-crosstab.
[11] Id.

pregnancy status, and genetic information.[12] Specifically, Title VII of the Civil Rights Act (Title VII, 42 U.S.C. § 2000e *et seq.*), the Age Discrimination in Employment Act (ADEA, 29 U.S.C. § 621 *et seq.*), and the Americans With Disabilities Act (ADA, commencing at 42 U.S.C. §§ 12111), prohibit refusing to hire an applicant because of his or her race, religion, gender or national origin. More expansive state and local non-discrimination laws also cover other classifications, including height, weight, familial status, marital status, gender identity, and sexual orientation. Thus, employers who access social media may potentially waive any future argument that they were not aware of an applicant's protected status. In effect, by utilizing social media, employers risk losing an argument based upon "lack of notice" and thus are forced to prove a negative; that they did not consider the applicant's protected status.

While employers should be wary of learning "too much" about job applicants, it is possible that a claim may be made that an employer did not learn enough. The issue is whether employers have an affirmative obligation to search for and review publicly available information on social media sites. Given the amount of public information available on the web and the number of applicants who likely maintain some presence on social media sites, it is not surprising that there are claims alleging that employers negligently hired (or retained) an employee who is either known or should be known to harm individuals the employee comes into contact within the scope of his/her employment.[13]

Some employers have taken the step of requiring applicants to provide login and password information during the application process. However, some state legislatures have pushed back and have enacted, or are in the process of enacting, legislation prohibiting employers from asking for this information. In April 2012, Maryland enacted the nation's first "social media password protection law." In the past year, this effort has expanded to nine additional states: Arkansas, California, Colorado, Illinois, Michigan, New Jersey, New Mexico, Utah and Washington.[14]

Recommendations? Employers should implement clear procedures for social media use in screening job applicants. An employer in the possession of information about applicants' or employees' protected characteristics may face the challenge of establishing that employment decisions were made without regard for that information. A process that includes a division of duties between human resource professionals trained in the use of social media screening and managers making employment decisions is one good option. Such a division permits relevant information to reach decision-makers without unnecessary "inadvertently acquired" material obtained from social media sites.

---

[12] In 2011, the EEOC issued regulations specifically addressing the use of social media by employers in learning of health data (in the context of implementing the Genetic Information Nondiscrimination Act). S*ee* CFR § 1635.8(b)(1)(ii)(D) (providing an exception where one "inadvertently learns genetic information from a social media platform which he or she was given permission to access by the creator of the profile at issue").

[13] *Compare, e.g., Doe v. XYC Corp*., 887 A.2d 1156, 1168 (N.J. Sup. Ct. 2005) (employer breached its duty to exercise reasonable care when it knew about and failed to prevent an employee from using the employer's computer and network to view and transmit child pornography) *with Maypark v. Securitas Sec. Services USA, Inc*, 321 N.W.2d. 270, 272, 275-76 (Wis. App. 2009) (employer not liable for negligent supervision where employee uploaded altered pictures from home of other employees on adult websites).

[14] *See* http://privacyblog.littler.com/2013/05/articles/state-privacy-legislation/colorado-becomes-tenth-state-to-pass-social-media-password-protection-legislation/.

Employers Monitoring Employees' Social Media Use: The Need for an Electronic Communications Policy

An employee may believe that his electronic communications at work are private, but that is not the case when his communications take place during work time using company-owned devices (cell phones or computers). However, an employer's ability to monitor and access an employee's electronic communications might only be as broad as the scope of its electronic communications policy and the reach of its computer systems.

The Fourth Amendment to the U.S. Constitution creates privacy rights for public sector employees, but private sector employees (except those in California)[15] have no constitution right to privacy. However, even private sector employees can assert common law privacy rights. When it comes to emerging technologies, however, the U.S. Supreme Court has urged caution when determining privacy expectations in communications made on electronic equipment owned by an employer. *See City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619 (2010). In *Quon*, the Court refrained from deciding whether an employee had a reasonable expectation of privacy in text messages sent and received on employer-provided devices, and disposed of the case on narrower grounds. In doing so, the Court warned that the judiciary "risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." The Court further stressed in *Quon* 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."

A well-drafted electronic communications policy will, in most cases, eliminate any reasonable expectation of privacy in employee communications sent or stored on company systems or servers. *See, e.g., Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) ("[the employee] had no right of privacy in the computer that [the employer] had lent him for use in the workplace . . . [Where an employer has] announced [a policy stating] that it could inspect the laptops that it furnished for the use of its employees, . . . this destroyed any reasonable expectation of privacy that [the employee] might have had and so scotches his claim."); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) ("[R]egardless of whether [the employee] subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after [his employer] notified him that it would be overseeing his Internet use."); *Miller v. Blattner*, 676 F. Supp.2d 485, 497 (E.D. La. 2009) ("Where, as here, an employer has a rule prohibiting personal computer use and a published policy that emails on [its] computers were the property of [the company], an employee cannot reasonably expect privacy in [his or her] prohibited communications."); *Sims v. Lakeside School*, No. C06-1412(RSM), 2007 WL 2745367, *1 (W.D. Wash. Sept. 20, 2007) ("[W]here an employer indicates that it can inspect laptops that it furnished for use of its employees, the employee does not have a reasonable expectation of privacy over the employer-furnished laptop.").

The Supreme Court has recognized that different employers need different types of electronic communications policies. "Given the great variety of work environments, … the question whether an employee has a reasonable expectation of privacy must be addressed on a

[15] *See Hill v. National Collegiate Athletic Assn.*, 7 Cal. 4th 1, 18, 865 P.2d 633, 642-43, 26 Cal. Rptr. 2d 834, 844 (Cal. 1994).

case by case basis." *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987). "Because an employer's announced policies regarding the confidentiality and handling of email and other electronically stored information on company computers and servers are critically important to determining whether an employee has a reasonable expectation of privacy in such materials, the cases in this area tend to be highly fact-specific and the outcomes are largely determined by the particular policy language adopted by the employer." *In re Reserve Fund Securities and Derivative Litigation*, 275 F.R.D. 154, 160 (S.D.N.Y. 2011) (listing cases).

In addition to employee privacy rights, there are statutory restrictions on an employer's right to monitor employee activity: the Electronic Communications Privacy Act of 1986 ("ECPA"). The ECPA imposes criminal and civil penalties against any person who intentionally intercepts or accesses an electronic communication without proper authorization. Title I of the ECPA pertains to wire, oral and electronic communications while in transit, and it contains an exception permitting employers to intercept communications that are likely to further legitimate business interests. 18 U.S.C. §2510-2522. Title II comprises the Stored Communications Act ("SCA"), which covers stored electronic communications. 18 U.S.C. §§ 2701-2711. This includes any temporary, intermediate storage of wire or electronic communication incidental to the electronic transmission of that communication, as well as the storage of such communications for backup purposes. 18 U.S.C. §§ 2510(17), 2711(1).

The SCA was designed to prevent computer hackers from accessing stored electronic communications, but the statute also has created a federal cause of action for employees alleging that their employers improperly accessed or viewed their personal emails and restricted websites. (*See, e.g., Van Alstyne v. Electronic Scriptorium, Ltd*., 560 F.3d 199 (4th Cir. 2009) (Virginia jury issued a verdict in favor of plaintiff on her claim against her former employer and its president, alleging that for more than a year after she had left the company, the president repeatedly accessed her personal email account without authorization in violation of the SCA.)

The SCA contains certain exceptions which may, in some circumstances, permit employers to access its employee's social media posts and other electronic communications. Specifically, the statute's prohibitions do not apply to conduct authorized (1) by the provider of the electronic communication service or (2) by a user of that service with respect to a communication of or intended for that user. 18 U.S.C. §2701(c). The statute defines "user" as one who uses the service and is duly authorized to do so.

Courts have reached differing conclusions on whether an employer qualifies as a "system provider" under the SCA with respect to company-provided information technology resources. *Compare Steinbach v. Village of Forest Park*, No. 06 C 4215, 2009 WL 2605283, *5 (N.D. Ill. Aug. 25, 2009) ("[The employer] purchases Internet access from a third-party provider, and does not itself provide Internet service for purposes of the [SCA's service provider] exception"); *with Fraser v. Nationwide Mut. Ins. Co*., 352 F.3d 107, 114-15 (3d Cir. 2003) ("[W]e hold that, because [the employee's] e-mail was stored on [the employer's] system (which [the employer] administered), its search of that e-mail falls within §2701(c)'s exception to [the SCA]").

Even where employers are not deemed service providers, they may legitimately gain access to an employee's stored electronic communications through the authorization of the

employee or another authorized user. Even absent an employee's express consent, courts have held that implied consent exists where employers expressly notify their employees, through a policy or otherwise, that the particular type of communication at issue would be monitored. *See, e.g., Griffin v. City of Milwaukee*, 74 F.3d 824, 827 (7th Cir. 1996) (holding that implied consent existed where employee knew her telephone conversations at her workstation could be monitored by supervisors, employees were told that incoming emergency calls would be recorded, and recording equipment was located in employee's work area); and *Sporer v. UAL Corp.*, No. C 08-02835 (JSW), 2009 WL 2761329, *5 (N.D. Cal. Aug. 27, 2009) (employer did not violate SCA when it viewed pornographic video employee sent from his work account to his personal account; employer had policy of monitoring employees' computer use and warned employees of policy; thus, employee gave implied consent to his employer to monitor work email account).

Employer Terminations Relating to Social Media: A Few Examples

There are many current real-life examples of employees getting into trouble by their social media use,[16] including:

- An "excellent" job candidate was not hired by the prospective employer when the applicant's LinkedIn profile indicated that he was not a "team player" but rather a "lone wolf" who took credit for everything for himself.

- A Manatee County, Florida teacher stated in a Facebook exchange with seven other teachers that one of her students" may be the evolutionary link between orangutans and humans." The matter has been referred to the state Department of Education for review.

- Three airline employees were disciplined for posting a picture of a co-worker, an airline customer service agent, on one of the employee's Facebook pages, which showed the co-worker in a crouching position hunched over her desk with part of her buttocks showing and her thong underwear visible.

- A radiology employee was terminated for posting on her Facebook account statements that her boss put extra money in her and other employees' paychecks because he liked them, and also that her boss was a "snake" and creepy.

- A New York City teacher was disciplined for posting on her Facebook page the day after a public school student had drowned during a field trip to the beach that she was "thinking the beach sounds like a wonderful day for my 5th graders," "I hate their guts," they are the "devil's spawn," and that she would not throw a life jacket to a child "for a million."

- A former employee, a video and social media producer, was sued by her former employer because she displayed on her website as an example of her capabilities as a web designer content that included projects that she had worked on at her former employer.

[16] Cavico, et al. at 5-6 (citations omitted).

- A New Jersey teacher was suspended as a result of her posts on her Facebook page, which included her opinion that the school's gay history exhibit should be removed as well as comments urging her friends to pray as a result of the sinfulness of homosexuality.

- An employee of a Chicago car dealership was fired because he posted critical comments and photos of the employer on Facebook, including a statement that the sales commissions were likely to drop because the dealership's promotional event only served water and hot dogs.

- A high school teacher was fired after posting on her Facebook page that she thought the residents of the school district were "arrogant and snobby" and that she was not looking forward to another school year.

- A flight attendant was discharged for posting suggestive pictures of herself in her company uniform.

- Two employees of a pizza chain franchise were terminated after posting a joke video of themselves on YouTube that showed them preparing sandwiches at work while one put cheese up his nose and mucus on the food.

- A professor of anatomy was denied a job at the University of Kentucky after the hiring committee found articles he wrote suggesting that he might believe in "creationism."

- A part-time instructor at a Catholic college in Philadelphia was terminated when he disclosed on his Internet blog that he was in a committed long-term same-sex relationship for about 15 years.

- In Columbus, Mississippi, two firefighters and a police officer were suspended for "liking" the Facebook post of another firefighter who had written critically about the location of a woman whose two year old child was hit by a car.

- A Red Bull Racing crew member was terminated for posting what was perceived as an anti-gay Tweet on his Twitter page.

- Thirteen Virgin Atlantic cabin crew members were discharged after the company discovered that the employees were posting inappropriate comments about their employer and customers on Facebook, including comments that the planes were full of cockroaches and that the passengers were "chavs."

- A California woman was fired from her job at the Cold Stone Creamery for posting a racial slur about President Obama on Facebook and writing that "maybe he will get assassinated." She claims she is not racist and that she was merely stating her "opinion." The Secret Service is investigating.

- ❖ An employee of the water-taxi service in Ft. Lauderdale, Florida was fired for posting a video on You Tube about a developer's plan to remove a giant rain tree, which could be the largest in the state, along the New River. The Water Taxi leases its hub from the developer who wants to remove the tree for a marine and residential development project.

Employer Risks in Terminating Employees Because of Social Media Posts

Taking adverse action against an employee because of social media posts may trigger several federal and state employment statutes.

1. Off-Duty Conduct Laws

Employers should be generally aware that several states (California, New York, Colorado, and North Dakota) have passed statutes protecting employees in their "off duty conduct", recreational activities, and political practices.[17] Blogging or posting may perhaps be covered by these statutes.

2. The Digital "Water Cooler:" The Right to Bitch About Your Job.[18]

The National Labor Relations Act provides rights to employees to complain about the conditions of their employment. If an employee's internet posting represents an effort to organize a union or relates to a labor dispute between the employer and its employees, an employee could argue that any discipline relating to the postings constitutes an unfair labor practice. Specifically, the NLRA grants employees the right to "engage in other concerted activities for the purpose of mutual aid and protection."[19] The NLRA has been interpreted to protect non-union employees' concerted efforts to better the conditions of their employment.

For organizational speech to be protected it must be: 1) concerted; and 2) for mutual aid and protection. The National Labor Relations Board ("NLRB") and courts have arrived at varying definitions for "concerted" speech. Examples include: "organizational speech directed at only one other employee; speech that failed to actually produce any concerted group activity but appears to have had such activity as a primary goal, speech from employees who are merely spokespersons on matters of common concern, speech amounting to merely an implicit attempt to induce concerted action on the part of other employees, speech that is a logical outgrowth of previous group activity; and even completely independent expressive activity, not preceded by any group discussion and not characterized as a protest, as long as the activity implies a common goal to alter workplace conditions."[20]

In *Konop v. Hawaiian Airlines, Inc.*, the Ninth Circuit recognized an employee's comments on his secure website as concerted speech. Konop's website bore bulletins critical of

---

[17] *See*, Cavico, et al. at pp. 19-22.

[18] For a detailed discussion of this topic, *see generally*, Cavico, et al., at pp. 15-18; *see also* Davis, "Social Media Activity & the Workplace: Updating the Status of Social Media," 39 Ohio Northern University Law Review 359 (2012).

[19] *See* National Labor Relations Act, 29 U.S.C. §§ 157-158(a)(1)(2000).

[20] Andrew F. Hettinga, *Expanding NLRA Protection of employee organizational Blogs: Non-Discriminatory Access and the Forum-Based Disloyalty Exception*, 82 S. CHI. KENT L. REV. 997, 1001-02 (2007).

his employer, Hawaiian, its officers, and the incumbent union. The Ninth Circuit ruled that Hawaiian Airlines' discipline of a pilot who used his personal website to "vigorously criticize[]" the airline's management and labor concessions sought by the airline constituted protected union organizing activity. In so ruling, the Court rejected Hawaiian's arguments that the pilot lost this protection because his comments contained "malicious, defamatory and insulting material known to be false."[21]

The protection afforded by the NLRA is not absolute. Employees who engage in disloyal behavior or disparage the employer's customers or business activities are not protected by the NLRA. For instance, in *Endicott Interconnect Techs. v. NLRB*, where an employee posted his protests concerning recent layoffs and stated that his employer's recent layoff of 200 employees was causing the business to be "tanked," the D.C. Circuit reversed the NLRB's decision that the employee's resulting discharge constituted an unfair labor practice. The Court held that the employee's posting was so detrimentally disloyal that his discharge did not violate the NLRA. The Court reasoned that the employee's comments constituted "a sharp, public, disparaging attack upon the quality of the company's product and its business policies" at a "critical time" for the company, and were therefore unprotected by the NLRA.[22]

The NLRB also has reviewed cases involving employers who allegedly implemented unlawfully broad social media policies limiting how employees could communicate on-line in violation of Section 8(a)(1) of the NLRA. Employers violate Section 8(a)(1) when they maintain work rules which would reasonably tend to chill employees in the exercise of their right to engage in protected concerted activity.[23]

In January 2102, the NLRB's General Counsel released a report summarizing the agency's cases that involve employee participation in social media.[24] The report comes on the heels of a similar one released in August 2011[25] and makes it clear that the NLRB sees the world of social media as an extension of the workplace. It emphasizes that employers are not free to adopt social media policies that might discourage or interfere with certain types of online – even off-duty – activity, and that the NLRB intends to ensure that employees can engage in protected, concerted activities online without fear of adverse consequences from their employers.

The most recent NLRB legal advice comes from the agency's Office of General Counsel in the form of legal memorandum. On May 30, 2012, the Office of General Counsel to the National Labor Relations Board authored a legal memorandum dissecting seven (7) recent "social media" policies of employers which have been subject to labor complaints.[26] Six of the seven company policies were determined to contain provisions that were in part overbroad and unlawful under the NLRA. For example, in reviewing a motor vehicle manufacturer's social media policy, the NLRB's general counsel explained that the employer's policy instructing employees be sure their posts are completely accurate and not to reveal non-public information

[21] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 872-73 (9th Cir. 2002).
[22] *Endicott Interconnect Techs. v. NLRB*, 453 F.3d 532 (D.C. Cir. 2006)
[23] *Lafayette Park Hotel*, 326 NLRB 824, 825 (1998), *enf'd.* 203 F.3d 52 (D.C. Cir. 1999).
[24] *See* http://bit.ly/x0iKW8
[25] *See* http://bit.ly/opwRal
[26] *See* http://www.nlrb.gov/reports-guidance/operations-management-memos?memo_number=OM%5C+12.

on a public site was unlawful. This was based on the logic that the term "'completely accurate and not misleading" is overbroad because it could be "reasonably interpreted to apply to discussions about, or criticism of, the employer's labor policies and its treatment of employees that would be protected by the Act [NLRA] so long as they are not maliciously false . . . Moreover, the policy does not provide any guidance as to the meaning of this term by specific examples or limit the term in any way that would exclude Section 7 activity" (NLRB Memorandum OM 12-59, May 30, 2012, pp. 6-7).

Another policy that was interpreted as unlawful was a health care provider's social media policy. That policy was also scrutinized by the NLRB general counsel and interpreted to be unlawful under the NLRA when it required employees not to comment on any legal matters, including pending litigation and disputes. The NLRB's general counsel rationalized that since the policy's language was overbroad and could unlawfully prohibit employees from commenting on labor claims against the employer pending or contemplated by the workers, it was in violation of the NLRA (NLRB Memorandum OM 12-59, May 30, 2012 p. 10).

In the seventh case, Walmart's revised policy was approved as **lawful** under the NLRA. In this case the employee worked as a "greeter" for Walmart. The employee maintained a Facebook account at home that was open to the public and identified himself as a Walmart employee. He had 1800 Facebook friends, some of whom were co-workers. On July 12, 2011 he posted the following on his Facebook "wall":

> The government needs to step in and set a limit on how many kids people are allowed to have based on their income. If you can't afford to feed them you shouldn't be allowed to have them. . . . Our population needs to be controlled! In my neck of the woods when the whitetail deer get to be too numerous we thin them out! . . . Just go to your nearest big box store and start picking them off. . . . We cater too much to the handicapped nowadays! Hell, if you can't walk, why don't you stay the F@*k home!!!!

A customer read the post and complained to Walmart who terminated the employee three weeks later. The NLRB found that the aforementioned employee's communication was not "protected" as a Section 7 communication, and thus ruled against the charging party. However, more interestingly, during the processing of this particular complaint, Walmart revised its social media policy; and the NLRB gave its blessing on its legality under the NLRA (*Walmart Case* No. 11-CA-067171, May 30, 2012).[27]

Employers should not assume that the Wal-Mart policy will work for their company. Rather, they should tailor the core concepts to fit their own needs. A series of recommendations for company social media policies is provided below.

[27] A copy of the Wal-Mart policy is attached hereto as Exhibit A.

3. Retaliation under Title VII

Employers should consider the anti-retaliation provisions of federal and state employment laws before taking adverse action against an employee.[28] Title VII prohibits an employer from retaliating against an employee for "oppos[ing]" any unlawful discriminatory practice. Some employees may attempt to "oppose" a discriminatory practice on a social networking site or blog, which means that subsequent adverse action by the employer could lead to a claim. Other unique scenarios could also lead to a retaliation claim. For example, in *Williams v. Singing River Hospital System*, an employee sued following her resignation, alleging retaliation. The employee, an African-American, claimed she reported a former coworker who showed her a YouTube video entitled "Fry that Chicken." The Court dismissed the employee's claims, because the alleged adverse action occurred before she complained about the video.[29]

Compare this to *Navab-Safavi v. Broadcasting Board of Governors*, where an independent contractor sued after her contract was not renewed, alleging race and national origin discrimination and retaliation. The contractor, a U.S. citizen born in Iran, was terminated after she participated in a music video protesting the Iraq war which was posted to YouTube. The Court denied the defendants' motion to dismiss.[30]

4. Discrimination Under Title VII and State Laws

Employees terminated due to use of social media may argue discriminatory enforcement. Title VII establishes that it is unlawful for an employer to discriminate due to "race, color, religion, sex, or national origin." The Americans with Disabilities Act and the Age Discrimination in Employment Act offer similar protections to disabled employees and to employees over the age of forty. Some state laws also add sexual orientation, marital status, and status with regard to public assistance as protected classes.

Many people include demographic information on social networking sites or in the content of blogs, including sexual orientation, religion, age, medical conditions, marital status, race, and other protected categories. Some employee-bloggers may attempt to cloak themselves in the protection of an anti-discrimination statute by revealing these protected classes.[31]

The difficulty for employers in this type of lawsuit is the proverbial "un-ringing of the bell." The employer is forced to argue that while it knew of information related to a protected characteristic, this information did not sway its employment decision.

---

[28] Title VII of the Civil Rights Act, the Age Discrimination in Employment Act, as well as the Americans with Disabilities Act, have anti-retaliation provisions.

[29] *Williams v. Singing River Hospital System*, 2009 WL 484587 (S.D. Miss. February 26, 2009)

[30] *Navab-Safavi v. Broadcasting Board of Governors*, 650 F.Supp.2d 40 (D.C. 2009)

[31] A blogger who discussed his conversion to Islam alleged his subsequent termination was due to his religious beliefs in violation of Title VII. Scott Grubman, *Think Twice Before You Type: Blogging Your Way to Unemployment*, 42 Ga. L. Rev. 615, 617 (2008) (quoting William A. Clineburg Jr. & Peter N. Hall, *Addressing Blogging by Employees*, Nat'l L.J. June 6, 2005, at S6)

In *Shaver v. Davie County Public Schools, et al,*.[32] the plaintiff, proceeding pro se, claimed his employment as a public school bus driver was terminated because of religious discrimination stemming from his MySpace.com profile which identified plaintiff as a practicing Wiccan. This case was dismissed with prejudice in favor defendants as to the Title VII claims because plaintiff failed to exhaust his administrative remedies with the EEOC prior to filing suit; however his First Amendment claims were dismissed without prejudice, leaving open the possibility of further litigation.

Avoiding claims may be challenging for employers, who may not be aware of every posting made by employees. Thus, an employer should document any steps it takes to ascertain whether it is imposing comparable discipline on other similarly-situated employees who are not members of the protected class before taking action against an employee based on a posting.

An Enforceable Social Media Policy is a Necessity.

The literature on social media law reflects broad consensus on the need for every employer to have an appropriate and enforceable social media policy. Even employers that already have a policy in place should have legal counsel review it in light of recent NLRB decisions. Some advice:

- Know and understand NLRB decisions on appropriate and inappropriate social media policies;
- Make the policy very broad as to definition of "social media", and include all types of communications, including computers, cell phones and text messages, blogs, chat rooms;
- The policy should set for the circumstances by which employees can be disciplined or discharged for violating the policy;
- The policy should also establish clear and cogent procedures for monitoring and obtaining information contained on social media networking sites;
- The policy should state expressly, clearly, and exactly the employee's expectation of privacy regarding the employee's use of personal social media during working times and on employer-owned equipment;
- The policy should state that the employee has no reasonable expectation of privacy concerning social media posting and communications that are accessible to the general public, regardless if made during working or non-working times;
- The policy should not be overbroad so as to violate federal labor law or state lifestyle laws;
- The policy should prohibit the disclosure on social media of the employer's proprietary and confidential information, non-public information and trade secrets
- The policy should prohibit the unauthorized use of copyrighted materials;
- The policy should state that no employee has any authority to represent the employer on social media unless that authority has been expressly granted by the employer;

[32] *Shaver v. Davie County Public Schools, et al.*, 2008 WL 943035 (M.D.N.C. April 2008)

- The policy should inform employees that the employer will monitor use of social media during working hours while the employees use employer-owned equipment;
- The policy must have disciplinary components and must be consistently and equally applied like any other employer policy;
- The policy should include a statement that it in no way was designed or intended to be used as a means to interfere with the employee's rights under labor law to engage in concerted activities, such as the right to discuss working conditions; and
- The employer should train its employees regarding social media policy and try to make the employees understand the policy, the rationales therefor, and how the policy applies to them.

Final Thoughts: Some Recommendations for dealing with Social Media.

There is no escaping the new reality for every business in the world: "business as usual" for the foreseeable future will involve social media. While businesses have an amazing new set of tools with which to work to advertise their products and services, they are dealing with a Pandora's Box in terms of social media use by their employees. Social media presents new challenges to the employer. Fortunately, these are challenges that can be met head on and dealt with successfully.

In order to deal effectively with social media use by prospective and current employees, the employer should consider the following recommendations:

- Define company objectives
- Update personnel policies.
- Ensure policies are not overbroad.
- Adopt a policy specifically addressing social media.
- Incorporate social media into all employment contracts, including in provisions relating to confidentiality and non-competition.
- Dispel unwarranted expectations of privacy (establish an electronic communications policy)
- Monitor for security and content.
- Access employees' restricted social media posts only with proper authorization.
- Respect privacy concerns.
- Avoid the appearance of discrimination. Treat like situations alike.
- Be alert to obtained "protected" information online. Consider having someone other than the decision-makers screen social media postings and provide only non-protected content to those making the employment decision.
- Prevent the creation of an online hostile work environment. Regularly monitor activity on company-related sites and update anti-harassment policies. Online harassment should be treated no differently than harassment in other settings.
- Provide training and orientation for employees.
- Train the company's supervisors and professionals.

- Do not take action based upon "concerted" activity (comments on wage, benefits, hours and other terms and conditions).
- Be mindful of whistle-blower protections.
- Establish reporting procedures for violation of company policies.

Exhibit A: Wal-Mart's Social Media Policy

Social Media Policy

Updated: May 4, 2012

At [Employer], we understand that social media can be a fun and rewarding way to share your life and opinions with family, friends and co-workers around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media.

This policy applies to all associates who work for [Employer], or one of its subsidiary companies in the United States ([Employer]).

Managers and supervisors should use the supplemental Social Media Management Guidelines for additional guidance in administering the policy.

GUIDELINES

In the rapidly expanding world of electronic communication, *social media* can mean many things. *Social media* includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with [Employer], as well as any other form of electronic communication.

The same principles and guidelines found in [Employer] policies and three basic beliefs apply to your activities online. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow associates or otherwise adversely affects members, customers, suppliers, people who work on behalf of [Employer] or [Employer's] legitimate business interests may result in disciplinary action up to and including termination.

Know and follow the rules - Carefully read these guidelines, the [Employer] Statement of Ethics Policy, the [Employer] Information Policy and the Discrimination & Harassment Prevention Policy, and ensure your postings are consistent with these policies. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

Be respectful - Always be fair and courteous to fellow associates, customers, members, suppliers or people who work on behalf of [Employer]. Also, keep in mind that you are more likely to resolved work-related complaints by speaking directly with your co-workers or by

utilizing our Open Door Policy than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage customers, members, associates or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy.

Be honest and accurate - Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Never post any information
or rumors that you know to be false about [Employer], fellow associates, members, customers, suppliers, people working on behalf of [Employer] or competitors.

Post only appropriate and respectful content
* Maintain the confidentiality of [Employer] trade secrets and private or confidential information. Trades secrets may include information regarding the development of systems, processes, products, know-how and technology. Do not post internal reports, policies, procedures or other internal business-related confidential communications.

* Respect financial disclosure laws. It is illegal to communicate or give a "tip" on inside information to others so that they may buy or sell stocks or securities. Such online conduct may also violate the Insider Trading Policy.

* Do not create a link from your blog, website or other social networking site to a [Employer] website without identifying yourself as a [Employer] associate.

* Express only your personal opinions. Never represent yourself as a spokesperson for [Employer]. If [Employer] is a subject of the content you are creating, be clear and open about the fact that you are an associate and make it clear that your views do not represent those of [Employer], fellow associates, members, customers, suppliers or people working on behalf of [Employer]. If you do publish a blog or post online related to the work you do or subjects associated with [Employer], make it clear that you are not speaking on behalf of [Employer]. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of [Employer]."

Using social media at work - Refrain from using social media while on work time or on equipment we provide, unless it is work-related as authorized by your manager or consistent with the Company Equipment Policy. Do not use [Employer] email addresses to register on social networks, blogs or other online tools utilized for personal use.

Retaliation is prohibited - [Employer] prohibits taking negative action against any associate for reporting a possible deviation from this policy or for cooperating in an investigation. Any associate who retaliates against another associate for reporting a possible deviation from this

policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination.

Media contacts - Associates should not speak to the media on [Employer's] behalf without contacting the Corporate Affairs Department. All media inquiries should be directed to them.

For more information - If you have questions or need further guidance, please contact your HR representative.