Workplace Problems and Solutions: Dealing with Social Media in the Workplace

American Bar Association
11th Annual Labor and Employment Law Annual Meeting
Thursday, November 9, 2017

Melinda C. Burrows, NetScout Systems, Inc.
Westford, MA

Julia Campins, Campins Beham-Baker, PC
Lafayette, CA

Jolsna John Thomas, Union and Employee Advocate
Austin, TX

Joane Si Ian Wong, National Labor Relations Board (Presenter only)
New York, NY

TABLE OF CONTENT

I. Recent NLRB Guidance and Decisions Dealing with Social Media in the Workplace

A. NLRB Guidance from the General Counsel
B. NLRB Board Decisions – a summary of cases
   (1) Plaza Auto Center, Inc., 360 NLRB 972 (2014).
   (2) Three D, LLC d/b/a Triple Play Sports Bar and Grille, 361 NLRB No. 31 (2014).
   (3) Richmond District Neighborhood Center, 361 NLRB No. 74 (2014).
   (4) Atelier Condominium and Cooper Square Realty, 361 NLRB No. 11 (2014).
   (5) Purple Communications, Inc., 361 NLRB No. 126 (2014).
   (6) UPMC, 362 NLRB No. 191 (2015).

II. A Survey of State Laws and Their Protection of Employee Rights In the Context of Social Media

A. First Amendment Protection for Public Employees
B. Off Duty Conduct
C. Privacy Laws
D. Spoliation
E. Defamation
F. Non-Solicitation and Non-Compete

III. Practical Tips for Managing Employee Social Media Use

A. Coordinate Management Oversight
B. Develop Policy
C. Communicate and Train on Policy
D. Monitor and Respond to Employee Social Media Use Responsibly
E. Sample Social Media Policy

I. Recent NLRB General Counsel Guidance and Decisions on Dealing with Social Media in the Workplace

A. NLRB Guidance from the General Counsel

The Obama appointed National Labor Relations Board emerged as an enforcement agency in the workplace when it focused on "overly broad" workplace policies, finding many personnel policies unlawful under the National Labor Relations Act (NLRA).[1] Policies governing social media, confidentiality, professionalism, anti-harassment, trademark, photography/recording, and media contact fall under the Board's review.[2]

On March 18, 2015, General Counsel Richard F. Griffin, Jr. issued Memorandum GC 15-04 to give guidance on "this evolving area of labor law, with the hope that it will help employers to review their handbooks and other rules, and conform them, if necessary, to ensure that they are lawful."

The Trump Board may reverse the Board's position and repeal GC Memo 15-04, but practitioners will have to continue to guide their clients as *Lutheran Heritage Village-Livonia,* 343 NLRB 646 (2004) established the test that the mere maintenance of a work rule may violate NLRA Section 8(a)(1) if the rule has a chilling effect on employees' Section 7 activity. The rule does not need to obviously ban union activity, but the Board could decide it unlawful if "1) employees would reasonably construe the rule's language to prohibit Section 7 activity; 2) the rule was promulgated in response to union or other Section 7 activity; or 3) the rule was actually applied to restrict the exercise of Section 7 rights."

Section 7 provides employees the right to discuss wages, hours, and other terms and conditions of employment with fellow employees, as well as nonemployees. Therefore, an employer's personnel policy that specifically prohibits employee discussions of identified Section 7 topics or that an employee would reasonably understand to prohibit such discussions violates the NLRA. In 1999, the Board found that employees would reasonably construe "overly broad" rules to restrict Section 7 protected communications. See *Flamingo-Hilton Laughlin*, 330 NLRB 287, 288 n.3, 291-92. Prohibitions regarding the disclosure of "confidential information" are acceptable so long as they do not include Section 7 topics because employers have a substantial and legitimate interest in maintaining the privacy of business information. See *Lafayette Park Hotel*, 326 NLRB 824, 826 (1998), enforced, 203 F.3d 52 (D.C. Cir. 1999); *Super K-Mart*, 330 NLRB 263, 263 (1999).

B. NLRB Board Decisions – a summary of cases

In 2014 and 2015, the Board issued a number of social media decisions. This paper will review some of the decisions to provide the current context for review of these policies to assist practitioners in addressing social media in the workplace. GC Memo 15-04 provides examples

[1] 29 U.S.C.A. § 151, *et seq*.

[2] GC Memo 15-04 (March 18, 2015).

of lawful and unlawful rules. Panelists recommend that all readers review the memo for the best example of guidance.

(1) Plaza Auto Center, Inc. 360 NLRB 972 (2014)

While Plaza Auto Center is not a social media case, it does involve personnel rules. The Board addressed circumstances in which workers' concerted activity loses protection because of insubordination, profanity, or belligerence. The Board, on remand from the Ninth Circuit, analyzed the question by re-balancing the four-factor test set forth in *Atlantic Steel*, adopting the Administrative Law Judge (ALJ)'s facts without accepting her inferences or legal conclusions. This strategy may be useful to practitioners who can argue for different conclusions about the significance of facts without overcoming the deference owed to an ALJ's fact-finding.

i. Basic Facts

This case involved a car salesman who worked at Plaza Auto Center. During his short tenure, the employee raised concerns about working conditions on numerous occasions. His concerns centered on restroom facilities, breaks, commissions, and wages. The employer did not allow breaks during tent sales and did not provide minimum wage as a draw against commission. The employee talked with other workers about these issues, and on at least one occasion, a co-worker joined him in voicing concern. This dispute came to a head on a day that the employee pressed the office manager about minimum wage. The office manager responded that Plaza Auto did not pay minimum wage, just commissions, and if he did not like it, he should work elsewhere. The employee told the office manager that he talked with Arizona's wage and hour agency, and asked the office manager to look into the issue.

Later that afternoon, a sales manager called the employee into a meeting in a small office with the owner and another sales manager. The owner confronted the employee for raising so many negative issues. The employee responded that he had questions about commissions and minimum wage. The owner said that the employee had to live with the existing policies, and told him at least twice that if he did not like it, he should work elsewhere. At that point, the employee lost his temper and in a raised voice called the owner a "fucking mother fucking," a "fucking crook," and an "asshole." During this outburst, the employee stood up, pushed his chair aside, and told the owner that if the owner fired him, the owner would regret it. The owner then fired the employee.

ii. Board's Analysis

The Board Rejected the ALJ's Inferences and Legal Conclusions. The ALJ credited all of the above evidence, and based on those findings of fact, concluded that the employee's statement that the owner would regret his decision was menacing. The ALJ based this conclusion on the facts that the employee pushed his chair back as he made the statement and that the employee did not qualify that he was merely threatening legal consequences rather than physical violence. The Board credited the ALJ's findings of fact, but rejected the conclusion that the employee had been menacing. The Board reasoned that the employee had no history of violence, had earlier raised the specter of action with the state wage agency, and management took no action indicating that anyone felt physically threatened. The Board also declined to attach significance to the employee

pushing his chair back, but rather concluded that the act was a natural result of standing up to leave a small, crowded office.

The employee's outburst was protected under the Act. The Board then applied the four-factor *Atlantic Steel* test de novo. The Board found that while the nature of the outburst weighed against protecting the employee, it was not severe enough to cost him the protection of the Act when balanced against the other factors. The Board found that the employee's obscene and denigrating remarks must be given considerable weight because he targeted the owner personally and face-to-face. However, the Board reasoned, the fact that the nature of the outburst weighed against protection did not require a finding that he lost protection. "[N]ot every impropriety committed during otherwise protected activity places the employee beyond the protective shield of the Act." *Plaza Auto Center,* at 7, (citing and quoting *NLRB v. Thor Power Tool Co.,* 351 Fd. 584, 587 (7th Cir. 1965)). The protection of the Act would "be meaningless were the Board not to take into account the realities of industrial life and the fact that disputes over wages, hours, and working conditions are among the disputes most likely to engender ill feelings and strong responses." Id. (citing and quoting *Consumer Power Co.*, 282 NLRB 130, 132 (1965)).

The Board then found that the other three factors weighed more heavily in favor of protection than the profanity weighed against it. The subject matter of the meeting during which the outburst occurred was the employee's concerns about working conditions. Thus, protecting the outburst served the goal of protecting § 7 rights. The place of discussion likewise favored protection. This was not the employee confronting management in front of his coworkers in a way that was likely to undermine authority, but rather took place in a private, closed office meeting. Finally, the Board found that the employer's provocation also strongly supported protection. The employee was provoked into responding to management in a meeting that he did not want to be in. By telling him twice that if he did not like it, he could quit, the Board reasoned, the owner was effectively threatening to fire the employee if he did not quit organizing around working conditions. Moreover, this threat of constructive discharge provoked the employee's spontaneous, emotional response. Based on its consideration of the factors, the Board concluded that extending the Act's protection advanced the goals of the Act without unduly burdening the employer's interest in maintaining order. The Board's remedy included reinstatement and make-whole remedy on lost wages.

(2) Three D, LLC d/b/a Triple Play, 361 NLRB No. 31 (2014).

Triple Play Sports Bar involved social media "liking" and a Facebook discussion by two employees related to claims that employees unexpectedly owed additional State income taxes because of the Respondent's withholding mistakes. The Facebook communications clearly evidenced Section 7 protected concerted activities and were "for the purpose of . . . mutual aid or protection."

i. Basic Facts

A waitress at the bar and restaurant and another employee discovered that they owed more in State income taxes than expected, and they discussed this at work with other employees. Some employees complained to restaurant management. Respondent then planned a staff

meeting with its payroll provider to discuss the employees' concerns. Before the meeting, a former employee posted the following on her Facebook page: "Maybe someone should do the owners of Triple Play a favor and buy it from them. They can't even do the tax paperwork correctly!!! Now I OWE money...Wtf!!!!" A customer posted a comment and a coworker commented as well. The former employee called out the owner for failing to complete the paperwork properly and stated that they were calling the Labor Board. A cook liked that comment. The waitress commented with "I owe too. Such an asshole." The waitress's privacy settings only permitted her friends to see her comments. The restaurant terminated the waitress's employment for lack of loyalty because of her Facebook comment. Restaurant management interrogated the cook about his "like" of the comment and then terminated him.

ii. Board's Analysis

The Board adopted the ALJ's rulings on unlawful discharge and threat of litigation but also found the policy unlawful. The Board agreed with the ALJ that both the discharge of the waitress and cook violated the Act and constituted unlawful activity. The Board adopted the ALJ's finding that the restaurant violated the Act by threatening employees with discharge, interrogating employees about their Facebook activity, and informing the employees that it based its decision to discharge on their Facebook activity. The Board found the Atlantic Steel framework inapplicable. The employees engaged in protected Section 7 concerted activity by taking part in a social media discussion among offsite, off-duty employees and two non-employees. Managers and supervisors did not participate in the discussion, and the employees did not directly confront management. The Board found that the waitress's use of "a single expletive to describe a manager, in the course of a protected discussion on a social media website, does not sufficiently implicate the Respondent's legitimate interest in maintaining discipline and order in the workplace to warrant an analysis under Atlantic Steel." The Board determined that the employees' comments were not so disloyal to lose protection under the Jefferson Standard, and the employees' comments did not mention Respondent's products or services, much less disparage them. Therefore, the communication remained protected. The Board also adopted the ALJ's finding that the restaurant unlawfully threatened legal action against employees for engaging in Section 7 protected activity.

The Board reversed the ALJ and found that the restaurant violated Section 8(a)(1) by maintaining its "Internet/Blogging" policy because it concluded that employees would reasonably construe the policy to prohibit the protected Facebook communications that led to discharge. Here is the policy that the Board determined unlawful:

> The Company supports the free exchange of information and supports camaraderie among its employees. However, when internet blogging, chat room discussions, e-mail, text messages, or other forms of communication extend to employees revealing confidential and proprietary information about the Company, or engaging in inappropriate discussions about the company, management, and/or co-workers, the employee may be violating the law and is subject to disciplinary action, up to and including termination of employment. Please keep in mind that if you communicate regarding any aspect of the Company, you must include a disclaimer that the views you share are yours, and not necessarily the views of the

Company. In the event state or federal law precludes this policy, then it is of no force or effect.

The Board applied the *Lutheran Heritage Village* test and found the policy unlawful as overly broad. "An employer rule is unlawfully overbroad when employees would reasonably interpret it to encompass protected activities."[3] The Board found the term "inappropriate" overly board and that employees would reasonably understand it to encompass Section 7 protected activities.

(3) *Richmond District Neighborhood Center*, 361 NLRB No. 74 (2014).

This case involves the loss of protected status for concerted Facebook conversation between two employees where the employees described in detail their acts of insubordination.

i. Basic Facts

Two employees of an afterschool program engaged in a Facebook discussion where they complained about management and their plans for the program. Respondent rescinded the employees rehire offers and explained, "These statements give us great concern about you not following the directions of your managers in accordance with RDNC program goals. . . . We have great concerns that your intentions and apparent refusal to work with management could endanger our youth participants." *Id*. at 2.

ii. Board's Analysis

The employees' Facebook exchange lost protection because it contained numerous statements advocating insubordination in specific detail. *Broyhill & Associates, Inc.*, 298 NLRB 707, 709–710 (1990) (no protection for employee who "expressed quite clearly over and over again . . . that he was not going to work the night schedule"). The Board found that Respondent acted reasonably when it rescinded the rehire offers and it did not need to wait for the employees to follow through on the misconduct they advocated. *Broyhill*, 298 NLRB at 707–710 (where employee said he "could not and would not work 12 nights," "would just take time off," and "get sick a lot," "[r]espondent was not obliged to wait for [him] to carry out his threat").

---

[3] See, e.g., *First Transit, Inc.*, 360 NLRB No. 72, slip op. at 2–3 (2014) (finding rule prohibiting "[d]iscourteous or inappropriate attitude or behavior to passengers, other employees, or members of the public" unlawfully overbroad); *Hill & Dales General* Hospital, 360 NLRB No. 70, slip op. at 1–2 (2014) (finding unlawfully overbroad rules requiring employees to "represent [the employer] in the community in a positive and professional manner" and prohibiting "negative comments" and "negativity"); *Lafayette Park Hotel*, 326 NLRB 824, 828 (1998) (finding unlawfully overbroad rule prohibiting "false, vicious, profane or malicious statements toward or concerning [the employer] or any of its employees"). The Board's approach in this area has received judicial approval. See, e.g., *Cintas Corp. v. NLRB*, 482 F.3d 463, 469–470 (D.C. Cir. 2007) (approving the Board's finding that rule requiring employees to maintain "confidentiality of any information concerning the company, its business plans, its partners, new business efforts, customers, accounting and financial matters" was unlawfully overbroad), enfg. 344 NLRB 943 (2005); *Brockton Hospital v. NLRB*, 294 F.3d 100, 106 (D.C. Cir. 2002) (approving the Board's finding that rule prohibiting discussions of "[i]nformation concerning patients, associates, or hospital operations . . . except strictly in connection with hospital business" was unlawfully overbroad), *enfg*. 333 NLRB 1367 (2001).

(4) *Atelier Condominium and Cooper Square Realty, as Joint Employer*, 361 NLRB No. 11 (2014).

This case arises from an organizing campaign among the Respondent's employees. The Board found Respondent's lawsuit regarding the allegation that a former employee published statements on the Internet baseless and the naming of the employee amounted to retaliation for his protected activity and the filing of the litigation violated the Act.

i. Basic Facts

Respondents operated a highrise building in mid-town Manhattan consisting of luxury residential condominiums. In early 2009, the building service employees began organizing in support of the Union. Board of Directors President interrogated an employee and said that he knew the employee wanted a union and that the Respondent did not. On July 1, a group of condominium owners filed a lawsuit in state court against Respondent accusing the defendants of corruption, bribery, payoffs, and extortion related to an alleged conspiracy to manipulate the sale and leasing of condominium units in the building. The resident manager shot himself that day. Internet postings addressed to the Atelier residents appeared on two websites discussing resident manager's suicide and the corrupt activities of the Board of Directors President alleged in the owners' lawsuit. On July 8th, Respondent sent an email to building residents responding to the Internet posting. He credits former employees and named condominium owners for the posting and asserts that they were involved in illegal activities in the building. Respondent then filed a lawsuit against the named residents and three recently discharged employees. The lawsuit broadly alleged that all the defendants were responsible for publishing multiple false statements on the Internet accusing the plaintiffs of various criminal activities, including complicity in the death of the resident manager. The allegations, however, did not attribute any particular role in posting the statements to any particular defendants. Nor did the allegations state that defendants subscribed to the postings. Indeed, it was apparent from the complaint allegations that the postings were anonymous. The lawsuit demanded $190 million in compensatory and punitive damages.

ii. Board's Analysis

The Board found that the interrogation "statement" to the employee was the type of statement that "begs a reply," and constitutes "an invitation . . . either to confirm or deny [its] truth." *Ready Mix, Inc.*, 337 NLRB 1189, 1190 (2002). It also found that the "statement" was coercive in all the circumstances, thus rendering Sec. 8(c) inapplicable.

The Board held that baseless lawsuits are unlawful under the Act if the plaintiff's motive was to retaliate against protected rights. Here, Respondent failed to establish the five elements necessary to succeed in a libel suit in New York. No evidence existed that the employee published the statement. No evidence existed showing that the employee was responsible for any of the alleged libelous statements, and Respondent failed to investigate. Therefore, the Board concluded that Respondent violated the Act when it retaliated against employees for exercising their protected rights with a baseless lawsuit.

(5) *Purple Communications, Inc.*, 361 NLRB No. 126 (2014).

This case underscores the Agency's enforcement initiated focused on workplace policies. It sets out a new rule allowing employees access to company-owned email system for protected Section 7 activities on nonworking time thereby overruling *Register Guard* to the extent it held that employees can have no statutory right to use their employer's email systems for Section 7 purposes. 351 NLRB 1110 (2007), enfd. in relevant part and remanded sub nom.

i. Basic Facts

In 2012, the General Counsel issued a complaint against *Purple Communications, Inc.*, a deaf and hard-of-hearing communications technology company based out of California, alleging, among other things, that its company email policy was overbroad and unduly restrictive to its employees' ability to discuss working conditions and terms of employment. The relevant email and other company communications policy at issue stated: "Computers, laptops, internet access, voicemail, electronic mail (email), Blackberry, cellular telephones and/or other Company equipment is provided and maintained by Purple to facilitate Company business. All information and messages stored, sent, and received on these systems are the sole and exclusive property of the Company, regardless of the author or recipient. All such equipment and access should be used for business purposes only." *Purple Communications, Inc.*, 361 NLRB No. 126 (2014). The General Counsel's office challenged the policy after a local union conducted an unsuccessful representation election. Id.

ii. Board's Analysis

The Board agreed with the General Counsel's exception argument to overrule *Register Guard* as it failed to appreciate the importance of electronic communications among employees in the modern workforce. *Purple Communications, Inc.*, 361 NLRB No. 126 (2014). It found that a company email system is part of a "virtual workplace" where the protected communications are transmitted electronically instead of in person. The Board set out its new framework. Companies must allow employees access to the company's email system to use it to engage in protected Section 7 communications during non-working time. The Board held that other available methods of communication (e.g. face-to-face discussion, social media or personal email accounts) will not permit an employer to restrict use of company email to business related communications. Id. The majority indicated, without elaboration, that under the new rule employers may apply uniform and consistently enforced controls over email systems "to the extent that those controls are necessary to maintain production and discipline," but only in those rare situations "where special circumstances" exist will a total ban on non-work email be lawful. Id. The Board limited this decision only to email systems and no other electronic communications.

General Counsel Memorandum 15-04 on March 18, 2015 gives significant guidance to employees.

(6) *UPMC*, 362 NLRB No. 191 (2015).

The Board extended *Purple Communications* to the hospital setting when no special circumstances are established.

i. Basic Facts

Hospital has a Solicitation Policy, Electronic Mail and Messaging Policy ("email policy"), and Acceptable Use of Information Technology Resources Policy ("acceptable use policy"). All of the policies on their face infringe on Section 7 rights.

ii. Board's Analysis

The Board found that certain language in the hospital's Electronic Mail and Messaging Policy ("email policy"), and Acceptable Use of Information Technology Resources Policy ("acceptable use policy") violated Section 8(a)(1) of the Act because the language tended to chill employees' exercise of their Section 7 rights. The Board extended its *Purple Communications* holding to the hospital's solicitation policy as the policy prohibited employees from using "UPMC electronic messaging systems to engage in solicitation." The Board found that hospital employees have a presumptive right to use the hospital's email system to engage in Section 7 protected communications during nonworking time. Here, the hospital failed to establish that "special circumstances" existed to justify the policy; therefore, they failed to rebut the presumption that the solicitation policy was unlawful.

II. A Survey of State Laws and Their Protection of Employee Rights in the Context of Social Media

Outside of the NLRA, there are protections for employees with respect to any actions they may take on social media. There are also areas where employers can protect their business.

A. First amendment protections for public employees

As public employees have the State as their employer, they are protected under the First Amendment from restrictions on their free speech in their employment. Generally, a public employee's speech is protected when speaking as a citizen on a matter of public concern. However, under *Garcetti v. Ceballos*, 547 U.S. 410 (2006), workplace speech related to a person's official job duties is not protected, even if the underlying issue is of public concern.

Courts apply a balancing test, weighing the employee's First Amendment interests against the state actor employer's interest in regulating the employee's speech to promote the efficiency of the public services it is providing. *Pickering v. Bd. of Educ.*, 391 U.S. 563, 568 (1968). Further limitations may be where the conduct is harmful to the underlying mission of the employer. *See Snipes v. Volusia County*, 16-14221, --- Fed. Appx. --- (11th Cir. Aug. 21, 2017). In *Snipes*, a law enforcement employee made comments on Facebook regarding Trayvon Martin such as "Another thug gone," and he was terminated. Because his posting impeded the government's ability to perform its duties effectively (potentially inciting protests against law enforcement), were made while on duty, and were made while racial tensions were already high, the Eleventh Circuit upheld the termination.

Some states have expanded this right to private employees. For example, in Connecticut employees have the right to sue their employer if the employer disciplines or fires the employee for exercising their free speech rights under both the First Amendment to the U.S. Constitution, *and* the Connecticut Constitution. Importantly, the speech must still be of a matter of "public concern" and courts will look to see if the person is speaking in his or her capacity as a concerned citizen. Thus, criticisms of one's own personal workplace may not be protected. The Connecticut Supreme Court has declined to apply *Garcetti* fully to its own protections, applying the protection to speech related to an employee's official job duties. *Trusz v. UBS Realty Investors, LLC*, 123 A.3d 1212, 319 Conn. 175 (2015).

B. Off-duty conduct

Many states explicitly prohibit employers from discharging employees for *lawful* conduct occurring while the employee is off duty. California,[4] Colorado,[5] New York,[6] and North Dakota[7]

[4] Cal. Labor Code § 96 and 98.6 say no employee can be discharged or otherwise discriminated against for lawful conduct occurring during nonworking hours away from the employer's premises. An employee who is discharged, threatened with discharge, demoted, suspended, or discriminated against in any manner in the terms and conditions of his or her employment is entitled to reinstatement and reimbursement for lost wages and benefits.

[5] Colo. Rev. Stat. § 24-34-402.5 says it's illegal to fire an employee because that employee engaged in any lawful activity off the employer's premises during nonworking hours unless the restriction relates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of

all have such provisions. As a reminder, the employer may still terminate the employee for off-duty conduct if it directly conflicts with some other duty. For example, where an employee demonstrates through Facebook postings that she is not entitled to FMLA leave, a termination may be justified. This must be a case specific inquiry. *Jones v. Accentia*, 11th Cir. Additionally, off-the-clock harassment can create a hostile work environment. *Maldonado-Catala v. Municipality of Naranjito*, 2106 WL 1411355 (D.P.R. 2015). Nevertheless, firing an employee for complaining about discrimination on Facebook may still constitute retaliation. *Brown v. Oakland County*, 14-cv-13159, 2015 WL 5317194 (E.D. Mich. Sept. 10, 2015).

C. Privacy laws

Social media can be fertile ground for information about employees, prior to hiring, during employment, and in litigation.

Many states have instituted laws prohibiting employers from intruding onto an employee's social media. A survey of state-by-state laws, with the year of adoption, is below.

Arkansas: Prohibits employers from suggesting that an employee should disclose his or her social media username and password, add the employer as a social media contact, or change his or her social media privacy settings (2013).

California: Prohibits employers from requiring or requesting employees or applicants to disclose their username or password for their social media account, and also prohibits employers from requiring the employee or applicant access his or her social media account in the presence of the employer. However, employers may make a reasonable request that an employee divulge personal social media account information, as is relevant to an investigation of employee misconduct (2012).

Colorado: Prohibits employers from requiring an employee or applicant to disclose a username, password or other means of accessing a personal account, unless an employer is conducting an investigation for legal compliance purposes (2013).

Connecticut: Prohibits an employer from requiring or requesting an employee or applicant to provide it with a username and password or to access a personal online account in the presence of the employer (2015).

---

a particular employee or a particular group of employees; or is necessary to avoid, or avoid the appearance of, a conflict of interest with any of the employee's responsibilities to the employer.

[6] N.Y. Labor Code § 201-d says employers can't make hiring or firing decisions, or otherwise discriminate against an employee or prospective employee because of legal use of consumable products or legal recreational activities outside of work hours, off of the employer's premises, and without use of the employer's equipment or other property.

[7] N.D. Cent. Code § 14-02/4-03 (2003) says it's illegal for an employer to fail or refuse to hire a person, to discharge an employee, or to treat a person or employee adversely or unequally with respect to application, hiring, training, apprenticeship, tenure, promotion, upgrading, compensation, layoff, or a term, privilege, or condition of employment, because of participation in lawful activity off the employer's premises during nonworking hours which is not in direct conflict with the essential business-related interests of the employer.

Delaware: Unlawful for employers, subject to certain exceptions, (i) to mandate that an employee or applicant disclose password or account information that would grant the employer access the employee or applicant's personal social networking profile or account, among other requirements (2015).

Illinois: Bars employers from demanding employees or applicants reveal their usernames or passwords linked to social networking sites; also prohibits employers from forcing employees to display their social networking profiles for review (2012).

Amends the Right to Privacy in the Workplace Act; makes it unlawful for an employer or prospective employer to request or require an employee or applicant to authenticate or access a personal online account in the presence of the employer, to request or require that an employee or applicant invite the employer to join a certain group, or join an online account established by the employer; prohibits retaliation against an employee or applicant; amends the Freedom from Location Surveillance Act (2016).

Louisiana: Employers cannot require prospective or current employees to disclose their username, password, or other login information that allows access to or observation of personal social media accounts (2014).

Maine: Provides that an employer may not require or coerce an employee or employment applicant into divulging a password to access a personal social media account, divulge account information or to add an employer or agent to such account (2015).

Maryland: Prohibits employers from requesting or requiring the disclosure of usernames or passwords to personal social media accounts, and prohibits employers from taking or threatening to take any disciplinary action against employees or applicants who refuse to disclose such information (2012).

Michigan: Prohibits employers from asking for an employee's or applicant's personal Internet account information; does not prohibit an employer from conducting a work-related investigation into activity on an employee's personal Internet account (2012).

Montana: Prohibits an employer from requiring or requesting an employee or applicant to disclose a username or password, access social media in the presence of the employer, or divulge information in a social media account as a condition of employment (2015).

Nebraska
Prohibits employers from accessing an applicant or an employee's personal Internet accounts and taking adverse action against, or failing to hire, an employee or applicant for failure to provide any information related to the account; prohibits retaliation against an employee who files a complaint under the Act; prohibits an employee from downloading or transferring any private proprietary information or financial data to a personal Internet account without authorization (2016).

Nevada: Prohibits employers from requiring access to an employee's social media account as a condition of employment (2013).

New Hampshire: Employers cannot require prospective or current employees to disclose their username, password or other login information for personal social media accounts (2014).
New Jersey: Employers cannot require prospective or current employees to disclose their username, password or other means for accessing an electronic account or service (2013).

New Mexico: Employers are prohibited from requesting or requiring that prospective employees provide passwords or access to their social networking accounts (2013).

Oklahoma: Employers cannot require prospective or current employees to disclose their username, password or other login information to personal social media accounts, or require prospective or current employees to log in to personal social media accounts in the presence of the employer (2014).

Oregon: It is unlawful for an employer to request that an employee or applicant disclose his or her username and password or add the employer to his or her list of contacts (2013).

Rhode Island: Employers cannot require or request prospective or current employees to disclose personal social media account information (2014).

Tennessee: Employers cannot require or request prospective or current employees to disclose login information to personal social media accounts, or require prospective or current employees to log in to personal social media accounts in the presence of the employer (2015).

Utah: Generally prohibits employers from requesting information related to personal Internet accounts, including usernames and passwords; allows employers to investigate specific information on the employee's personal Internet account to ensure compliance with certain laws (2013).

Virginia: Prohibits employers from requiring prospective or current employees to disclose the username and password to their social media accounts (2015).

Washington: Prohibits employers from requesting personal social networking account login information from employees or applicants; allows employers to require disclosure of employees' social media content in situations where necessary to comply with a federal law (2013).

West Virginia
Prohibits an employer from requesting or requiring that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through certain electronic communications devices; prohibits an employer from taking or threatening to take, certain disciplinary actions for an employee's refusal to disclose certain password and related information (2016).

Wisconsin: Employers cannot require or request prospective or current employees to disclose login information to personal social media accounts, or require prospective or current employees to allow employers to observe their personal social media account in the employer's presence (2014).

D. Spoliation

Spoliation issues arise when a plaintiff employee deletes, or a defendant employer instructs a witness employee to delete, social media postings. Privacy settings, however, may not raise the same issues. Generally speaking, absent court order not to modify *anything* about one's social media, employees can change privacy settings mid-litigation because that does not constitute deletion. *See Thurmond v. Brown*, 199 F. Supp. 3d 686 (W.D.N.Y. 2016).

Emerging social media and related platforms raise additional issues of spoliation. The paid version of slack—a chat program used internally by many companies—deletes prior chats at regular intervals. Signal, a secure text and phone app, can be set to delete history at regular intervals. Snapchat, too, deletes images individuals have shared. All of these platforms may give rise to evidence that is gone long before litigation. Of course, if evidence is preserved elsewhere or can be recovered, it will not subject the deleting party to sanctions. Fed. R. Civ. P. 37(e). Depending on any evidence regarding whether messages existed, any pending or reasonably foreseeable litigation, and the relevance of the deleted messages, there may or may not be spoliation sanctions. *See, e.g.*, *Burlington N. & Santa Fe. Ry. Co. v. Grant*, 505 F.3d 1013, 1032 (10th Cir. 2007) (explaining spoliation analysis).

E. Defamation

State tort law may also come into play with publications on social media. Employers and employees may be subject to liability for defamation. A comment on social media will certainly satisfy the "publication" prong, and the remaining analysis will be the same as with a traditional defamation claim. This is dangerous territory for employers, as they may be subject to liability for behavior over which they have little control. The posting must be in the course and scope of employment and the inquiry will be context specific. It is certainly true that employees, as well, may be liable for defaming an employer on social media. Finally, great care must be taken with official business social media accounts, because it will be far simpler to attach liability to the business when the defamation comes attached to the business's name.

F. Non-solicitation and Non-compete

As people do more and more of their business through social media, the courts are grappling with how to apply rules. Generally speaking, they have been sparing in permitting wide-ranging restrictions on former employees' abilities to spread their wings on social media. In states that permit non-solicitation and non-compete clauses, they may serve to limit a former employee's actions on social media sites such as LinkedIn and Facebook. "Give me a call today for a quote" posted on LinkedIn can violate a non-solicitation provision. *Mobile Mini, Inc. v. Vevea*, Civil No. 17-1684, 2017 WL 3172712 (D. Minn. July 25, 2017). In contrast, merely sending or responding to a connection request does not violate a non-solicitation provision.

Bankers Life & Cas. Co. v. Am. Senior Benefits, LLC, No. 1-16-0687, -- N.E.3d --, 2017 WL 3393844 (Ill. Ct. App. Aug. 7, 2017). Finally, in a case involving a business contract—not an employment contract—promotion a new business on Facebook violated a covenant not to compete. *Joseph v. O'Laughlin*, 2017 WL 3641351 (Penn. Sup. Ct. Aug. 22, 2017).

III. Practical Tips for Managing Employee Social Media Use

Social media has emerged as a key means of disseminating workplace information both on and off the job. It provides a platform that allows employees to share workplace information – and misinformation -- with a large public audience using a few keystrokes. As a result, responsible employers should have a plan that establishes, communicates and manages social media use.

The plan should include the following components:

- Coordinated management oversight
- Policy statement(s)
- Training and communications
- Responsible monitoring and enforcement

A description of each of these components follows.

A. Coordinate Management Oversight

To ensure that the organization speaks with a single voice with respect to social media use, one organization, often Legal, HR or Corporate Communications, should be the designated lead with respect to social media policy. The designated lead should (1) take the lead on developing and implementing social media policy (discussed below), (2) seek policy input from key stakeholders, and (3) serve as an initial point of contact for questions regarding social media use.

B. Develop Policy

As discussed previously in this paper, an employer's primary challenge with social media is not that it raises new or different policy considerations, but rather that the visibility and reach of information shared on social media may have an exponentially larger impact than more traditional ways of disseminating information. Therefore, in setting policy, the social media lead should work with other stakeholders to identify existing company policies that regulate and/or restrict the way in which employees communicate about the workplace.

Many large organizations provide social-media guidance in a stand-alone, comprehensive social media policy that provides the information employees need to use social media in a responsible manner. Examples of stand-alone social media policies are included in the appendix. A stand-alone policy may cover both professional and personal use and may include a mix of guidelines, best practices, examples of appropriate and inappropriate social media use and information about where to go with questions. Common guidance includes the following employee dos and don'ts:

- When talking about the company, disclose that you are an employee along with your role
- Unless specifically authorized as a company spokesperson, make it clear that you do not speak for the company

- Never disclose company confidential and proprietary information such as customer or employee personal information, intellectual property, trade secrets or undisclosed financial information
- Be respectful and professional of co-workers, business partners, customers and competitors
- Do not allow social media activity to interfere with your work responsibilities

In addition to a stand-alone policy, companies should reinforce their expectations with respect to social media use in existing policies that cover communications about the workplace. Such policies may include:

- Code of Conduct
- Confidentiality/Trade Secrets
- Insider Trading
- Anti-Harassment/Civil Treatment

All social media policy statements should be reviewed regularly – no less than annually -- to ensure compliance with new developments under the National Labor Relations Act, state privacy and other applicable laws and regulations.

C. Communicate and Train on Policy

Whether an employer develops a stand-alone social media policy or incorporates social media-related applications into existing policies, it is important that company expectations are expressly communicated and explained to employees. Simply adding a social media policy to the company policy library is not sufficient. And while an email announcing a new social media policy is a start, that channel may be insufficient to get the attention required to understand this important policy for many employee groups. Employee training is essential.

Many organizations have a limited appetite for all-employee training; therefore it is important to calibrate the level of training to specific audiences. The information the majority of employees need may be incorporated into existing training programs. For example, Anti-Harassment training might include a vignette about co-worker cyberbullying, or Code of Conduct/Insider Trading training could include examples of when and whether financial information can be shared on social media platforms. Employment law training for managers could (and should) include a discussion of employee rights under the NLRA that includes examples of social media activity that is and is not protected.

Some stakeholder groups, particularly employees in Human Resources, should have more focused training. Recruiters should be provided guidance regarding the risks associated with relying on information available on social media during the recruiting process. Employee relations professionals and internal investigators should be thoroughly trained on the scope of employee rights under the NLRA, including when social media postings are deemed protected concerted activity, state social media privacy, off duty conduct and other applicable laws. Another organization that may be targeted for training includes marketing – particularly if your marketing department monitors social media postings about the company or asks employees to share company postings on personal social media accounts.

D. Monitor and Respond to Employee Social Media Use Responsibly

Employers have the right to monitor employee social media use that is in the public domain. Ignoring employee social media may result in serious problems both internally (harassment claims, conflicts of interest) and externally (lawsuits, regulatory action). You may discover that employees are stealing time, disclosing proprietary information, or attempting to blow the whistle on alleged corporate misconduct.

Always conduct an investigation before taking adverse action against an employee based solely on their social media use to ensure the adverse action is proportional and defensible. Investigators should be mindful of applicable social media privacy laws which may restrict the investigator's ability to request social media account access directly from the employee. Before taking any adverse action, look carefully at the circumstances surrounding and context of any posting that appears on its face to violate your social media policy and assess whether it may be considered protected under the NLRA or a whistleblower statute. Take steps to ensure that the social media policy is consistently enforced to ensure that adverse action does not lead to costly and time-consuming regulatory scrutiny and/or litigation.

E. Sample Social Media Policy (See Attached Appendix)

APPENDIX

Social Media Policy

[UPDATED DATE]

At [COMPANY] (the "Company"), we understand that social media can be a fun and rewarding way to share your life and opinions with family, friends and co-workers. 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 [COMPANY TEAM MEMBERS] ("Company Team Members").

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 the Company, as well as any other form of electronic communication. The same principles and guidelines found in the Company policies 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 team members or otherwise adversely affects members, customers, suppliers, or people who work on behalf of the Company may result in disciplinary action up to and including termination.

Know and follow the rules

Carefully read these guidelines, the Company Ethics Policy, the Company Property/Proprietary Information Policy, the Workplace Violence Prevention Policy and the Equal Employment Opportunity and Harassment Policy, and ensure your postings are consistent with these policies. Inappropriate postings that may include discriminatory remarks, harassment, or 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 team members, customers, members, suppliers and people who work on behalf of the Company. Also, keep in mind that you are more likely to resolve work related complaints by speaking directly with fellow Company Team Members 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 the Company, fellow Company Team Members, the Company members, customers, suppliers, people working on behalf of the Company or competitors.

Post only appropriate and respectful content

- Maintain the confidentiality of the Company 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.

- Do not create a link from your blog, website or other social networking site to a Company website without identifying yourself as a Company Team Member.

- Express only your personal opinions. Never represent yourself as a spokesperson for the Company. If the Company is a subject of the content you are creating, be clear and open about the fact that you are a Company team member and make it clear that your views do not represent those of the Company, fellow Company team Members, Company members, customers, suppliers or people working on behalf of the Company. If you do publish a blog or post online related to the work you do or subjects associated with the Company, make it clear that you are not speaking on behalf of the Company. 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 the Company."

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 Team Leader or consistent with the Company Equipment Policy. Do not use the Company email addresses to register on social networks, blogs or other online tools utilized for personal use.

Retaliation is prohibited

The Company prohibits taking negative action against any team member for reporting a possible deviation from this policy or for cooperating in an investigation. Any team member who retaliates against another team member 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

Team members may not speak to the media on behalf of the Company without first contacting the Communications Department. All media inquiries should be directed to the Communications Department.

For more information

If you have questions or need further guidance, please contact the Company Human Resources Department.

Social Media Policy

[DATE]

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 chat room, regardless of whether associated or affiliated with _____ (the "Company"), as well as any other form of electronic communication. Before creating online content, consider some of the risks 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 the Company or its legitimate business interests may result in disciplinary action up to and including termination.

Inappropriate Postings

Posts that include discriminatory remarks, harassment, threats of violence or similar inappropriate or unlawful conduct, and are intended to bully, disparage or harm the reputation of the company or individuals are considered inappropriate and will not be tolerated, and they may subject employees to disciplinary action, including possible termination of employment. Social media 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 also will not be tolerated. Company policies include appropriate methods for dealing with conflict, criticism and complaints.

Confidentiality

Maintain the confidentiality of Company trade secrets and private or confidential information. Trade 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.

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.

Company as a Subject in Posts

Do not represent yourself as a spokesperson for Company. If Company is a subject of your post, state that you are an associate and that your views do not represent those of Company, associates, members, customers, suppliers or people working on behalf of Company. Include a disclaimer

such as “The postings on this site are my own and do not necessarily reflect the views of Company.”

Social Media at Work

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

Outside Media Requests

Please refer to “*Guidelines for Responding to Outside Media Requests Regarding Company”* – available on PolicyTech.

Disciplinary Action

Failure to follow the Social Media Policy may result in disciplinary action, including possible termination of employment.

For more information

If you have questions or need further guidance, please contact your HR representative.