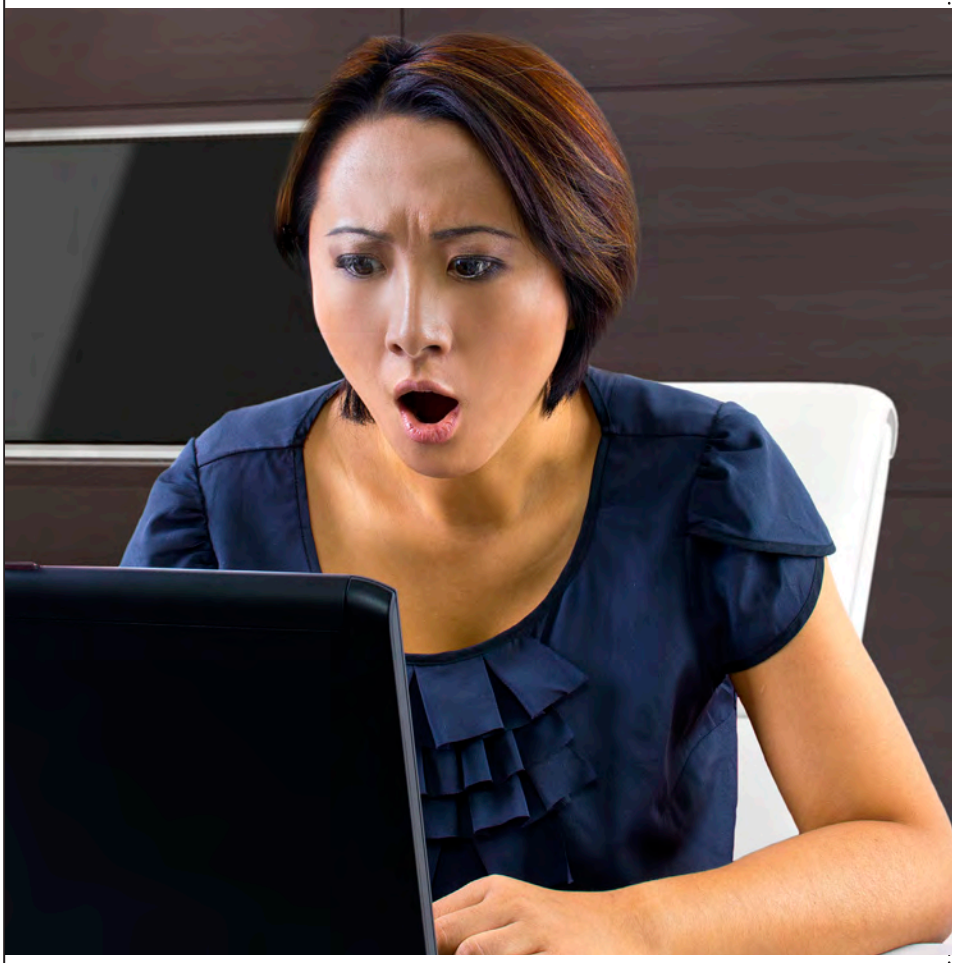
My Employee Said What on Facebook?

By Drew C. Piersall, Zashin & Rich Co., L.P.A.



"Ok we got Bin Laden . . . let's go get Kasich next . . . who's with me?" "[C]an't believe what a snake my boss is. . . . he needs to keep his [creepy] hands to himself . . . just an all around d-bag!!" "If you are on public assistance, you may not have additional children and must be on birth control (e.g. an IUD)."

These are statements that employees made on Facebook for which they received discipline, yet courts and an arbitrator reached different conclusions regarding the appropriateness of the discipline. This article addresses the issues employers face regarding social media in today's workplace, including: (1) employee conduct and discipline; (2) social media and the First Amendment; (3) government agency review of employer policies; (4) employer-issued social media and computer policies; (5) hosting social media sites; (6) public records; and (7) social media in the hiring process.

Can employers discipline employees for comments, posts, etc. that employees make while off-duty on non-employer social media sites? What standards apply to employee off-duty conduct? The arbitrator evaluating whether the Ohio Department of Rehabilitation and Correction had just cause to terminate the employee who made the Bin Laden comment above considered these issues. *State of Ohio, Ohio Dep't of Rehab. and Corr.*, (Pincus, Mar. 6, 2013). There, four employees who worked in the same correctional institution "liked" the corrections officer's Bin Laden Facebook comment, which he posted off-duty. The officer's Facebook profile included his job location and public employee status. Once the employer learned of the comments, it investigated and ultimately discharged the officer for violating the following rules: (1) threatening, intimidating, or coercive conduct; (2) compromising the employee's ability to effectively carry out his duty as a public employee; and (3) an act that brought discredit upon the employer. The arbitrator concluded that the officer's statements were nothing more than empty words. In addition, the arbitrator considered that the employer's "E-mail, Internet, and On-line Services Use" policy did not place the employee on notice that the policy covered his off-duty conduct. As such, the arbitrator concluded that while officer's alleged threat justified a 14-month suspension, the employer did not have just cause to terminate his employment.

The First Amendment protects a public employee's right "to speak as a citizen addressing matters of public concern." *Garcetti v. Ceballos*, 547 U.S. 410 (2006). A public employee must show the following to establish the First Amendment protected their speech: (1) the employee spoke as a private citizen rather than pursuant to official duties; (2) the speech involved a matter of public concern; and (3) the employee's "interest as a citizen" in commenting on the matter outweighed the State's interest, "as an employer, in promoting the efficiency of the public services it performs through its employees." *Westmoreland v. Sutherland*, 662 F.3d 714 (6th Cir. 2011).

Employees have raised the First Amendment as a defense to their social media posts in a number of contexts with varying results. For example, an Atlanta police officer claimed the Police Chief retaliated against her when he did not promote her after she criticized another law enforcement officer on Facebook. *Gresham v. City of Atlanta*, 542 Fed. App'x 817 (11th Cir. 2013). The court concluded the Police Department's legitimate interests in maintaining discipline and good working relationships outweighed the employee's interest in speaking about the matter.

In another case, the court affirmed the discharge of the Children's Services worker who made the above (and many other) comments about people who received public assistance. *Shepherd v. McGee*, 986 F.Supp. 2d 1211 (D. Or. 2013). The court reasoned that since her comments

were banter "rather than speech intended to help the public actually evaluate the performance of a public agency," they stood "on the periphery of First Amendment protection." The court also emphasized the heightened government interest that existed since the employee held a "public contact role." In addition, the employee's statements impaired her ability to do her job – testify at proceedings, since her statements raised credibility issues for prosecutors.

In an election year, a sheriff's office employee's statement ("liking" the Sheriff's opponent's campaign page) and interest in expressing his support for another candidate outweighed the incumbent sheriff's interest in providing efficient and effective services. *Bland v. Roberts*, 730 F.3d 368 (4th Cir. 2013). The sheriff's election was a matter of public concern and, as a sheriff's office employee, the employee's opinion had particular value to the public. In addition, the court found the employee's statement was "the internet equivalent of displaying a political sign in one's front yard" and, as political speech, received the highest level of protection. As these examples demonstrate, the First Amendment analysis is highly fact specific and depends on the content and audience of the social media post.

In evaluating employee conduct, discipline, and social media use, it is helpful for employers to have social media and computer use policies. However, employers must be cautious about the content and prohibitions included in such policies. The National Labor Relations Board ("NLRB") has issued numerous decisions, opinions, and guidance on social media policies. Although the NLRB's jurisdiction does not extend to Ohio public employers, since the State Employment Relations Board has largely not addressed the issue, the NLRB's guidance provides useful consideration for drafting and implementing social media and computer use policies.

The NLRB analyzes whether employers violate Section 7 of the National Labor Relations Act ("NLRA"), which guarantees employees the right to join unions and engage in "concerted activity" for the purposes of "mutual aid or protection." 29 U.S.C. §157. In the social media context, the NLRB considers whether an employee could reasonably construe a rule or policy to chill the employee's exercise of their Section 7 rights. The NLRB's memoranda and opinions provide guidance to employers drafting social media and computer use policies. For example, the NLRB has stated social media rules must not be ambiguous as to their application and should contain language that limits their application to specific activity (e.g., disclosing confidential employer information). NLRB Memorandum OM 12-59, May 30, 2012. The NLRB found an employer social media policy that contained the following lawful: (1) a prohibition against "inappropriate posting that may include discriminatory remarks, harassment and threats of violence or similar inappropriate or unlawful conduct;" (2) a provision, entitled "Be Respectful," which counseled employees to avoid posts that "could be viewed as malicious, obscene, threatening or intimidating" and explained what constituted bullying or online harassment; and (3) a rule requiring employees to maintain the confidentiality of the employer's trade secrets and private and confidential information. The NLRB has found the following policies overbroad and unlawful: (1) a general prohibition against releasing confidential guest, team member, or company information (could be construed to prohibit discussion of terms and conditions of employment); (2) a requirement that personal posts about the employer be completely accurate and not misleading; (3) a prohibition on friending co-workers; and (4) a prohibition on criticizing the employer.

The NLRB has found the following policies overbroad and unlawful: (1) a general prohibition against releasing confidential guest, team member, or company information (could be construed to prohibit discussion of terms and conditions of employment); (2) a requirement that personal posts about the employer be completely accurate and not misleading; (3) a prohibition on friending co-workers; and (4) a prohibition on criticizing the employer.

A recent decision demonstrates the extent to which the NLRB will protect employee speech. In *Three D, LLC v. NLRB*, the NLRB ruled an employee's Facebook post that the employer was "[s]uch an asshole" was concerted, protected, activity. No. 14-3284, 2015 U.S. App. LEXIS 18493 (2d Cir. Oct. 21, 2015). The NLRB found the activity concerted because it involved multiple employees and protected because it involved workplace complaints about tax withholdings. Furthermore, the statements were within the NLRA's protection because the comment at issue did not mention, let alone disparage, the employer's products. Therefore, at least according to the NLRB, an employee may call their boss an asshole on social media without repercussion.

So what can an employer include in its social media and computer use policies? While the law is ever-shifting, policies should include:

- a prohibition against accessing social media websites, blogs, or other internet forums of communication during working hours;
- a requirement that employees receive permission before speaking on behalf of the employer;
- a prohibition against disclosing confidential employer information;
- a disclaimer that employees should have no expected right of privacy for any matter "passed through, viewed, downloaded, printed, created, stored, received, sent or otherwise transmitted" from employer-provided technology and equipment;
- misuse of employer property may subject the employee to discipline;
- employee use of discrimination and harassment policies and procedures for reporting alleged misconduct, on and off duty; and
- a requirement that employees only disclose records through public records policy.

Continued on page 12

My Employee Said Cont'd from page 11

Employers also should have employees acknowledge their receipt and understanding of the social media and computer use policies.

Beyond controlling and responding to employee use of social media, additional challenges arise for employers who maintain and allow third parties to post on public websites. Those employers should: (1) clarify ownership of any "official" accounts; (2) clarify who, and under what circumstances, may create and use those "official" accounts; (3) publically inform those using the website that the employer monitors the site and posts may be deleted; (4) prohibit dissemination of non-public confidential information through the site; (5) prohibit threatening, harassing, or unlawful behavior; (6) maintain standards for deletion of off-topic, confidential, or inappropriate posts/materials; and (7) reference a records policy for deletion of records.

Public employers also must consider the interaction of public records laws with maintaining email systems, websites, and social media platforms. The Ohio Administrative Code ("OAC") defines records, for the purposes of the Public Records Act, to include "any document, device, or item, regardless of physical form or characteristic, including an electronic record . . . which serves to document the organization, functions, policies, decisions, procedures, operations, or other activities of the office." O.A.C. §149.011. Emails constitute public records under state law, are subject to public records requests, and must be maintained and deleted in accordance with the employer's public records policy. This includes public record content transmitted to or from private accounts or personal devices. Furthermore, records in the form of text and instant messages may fall under the purview of public records laws. Taking this into consideration, employers should: (1) clearly identify who is authorized to release public records; (2) amend retention policies to include the transient nature of social media sites; (3) archive websites; and (4) identify on websites that the employer may remove posts.

Finally, the prevalence of social media bleeds into the hiring process. Social media provides employers with another forum to post jobs and conduct background checks. However, employers should engage in social media background checks with caution. First, employers should consider the accuracy of the information (e.g., potential for false profiles or accounts). In addition, by viewing a prospective employee's social media account, the employer may incidentally obtain information regarding the individual's race, gender, national origin, religion, age, disability, or genetic background. This knowledge could expose the employer to claims of discrimination. Therefore, any employer who chooses to review prospective employees' social media accounts should take the following precautionary steps: (1) ensure the person reviewing social media accounts is wholly uninvolved in making the hiring decision; (2) only review publically available social media; and (3) do not request social media account passwords during the hiring process.

[A]ny employer who chooses to review prospective employees' social media accounts should take the following precautionary steps: (1) ensure the person reviewing social media accounts is wholly uninvolved in making the hiring decision; (2) only review publically available social media; and (3) do not request social media account passwords during the hiring process.

The growing prevalence of social media has created a host of potential issues for employers. Given social media's fast-paced growth and ever-changing nature, employers should constantly keep abreast of the current status of the law.



Drew C. Piersall works in Zashin & Rich Co., L.P.A.'s Columbus Office and practices in all areas of labor and employment law. If you have any questions about employee use of social media, please contact Drew (dcp@zrlaw.com) at 614.224.4411.

This article originally appeared in the November/December 2015 issue of *Cities and Villages* published by the Ohio Municipal League and is reprinted with permission. ML

