

## Rules for Workplace Social Media Policies That Work

**EMPLOYEES MAY TURN TO PERSONAL SOCIAL MEDIA** accounts or private chat rooms to vent about the workplace without realizing that these communications may be read by their employers. The law recognizes that employers have legitimate interests in disciplining employees, safeguarding trade secrets, preventing disparagement of their business, and ensuring a work environment free of discrimination, harassment, and abusive conduct. At the same time, federal and state courts, state legislatures, and the National Labor Relations Board (NLRB) have recognized broad protections for employees in their internet communications.<sup>1</sup> Attorneys should advise employers that disciplining an employee for private communications about the workplace on social media may run afoul of federal or state law, including the National Labor Relations Act (NLRA) and the federal Stored Communications Act (SCA).<sup>2</sup>

Although the law on social media use is still developing, there are two principal ways the courts, legislatures, and NLRB have limited an employer's ability to regulate an employee's personal social media communications: 1) by restricting an employer's access to an employee's personal social media account, and 2) by expanding the scope of "concerted protected activity" on social media. Employers should be aware of the restrictions on accessing and regulating the personal social media use of employees and implement clear, narrowly tailored policies that balance the employer and employee rights in social media use. Overly broad social media policies, even if they are not enforced, may be interpreted as chilling or prohibiting protected concerted activity by employees and deemed an unfair labor practice.

### Restricting Access

Years before the advent of social media, the federal government enacted the SCA, aimed at protecting the privacy of Internet communications.<sup>3</sup> The SCA prohibits anyone—not just employers—from accessing electronic communications on a third-party service provider without authorization. In recent years, some states have enacted SCA-like statutes restricting an employer's ability to access an employee's personal social media site.<sup>4</sup> In California, Labor Code Section 980 prohibits employers from requiring or even requesting an employee or applicant to: 1) disclose a username or password for the purpose of accessing personal social media, 2) access personal social media in employer's presence, or 3) divulge any personal social media. The only exception occurs when the employer reasonably believes that the employee's personal social media account is relevant to an investigation of allegations of employee misconduct or violation of law.<sup>5</sup>

There are no reported cases interpreting Labor Code Section 980 or the carve-out for investigations of misconduct. However, a number of courts have found employers liable under the SCA for accessing the personal social media communications of employees. In *Pietrylo v. Hillstone Restaurant Group*, an employee of Hillstone maintained a personal chat group on Myspace during nonwork hours that was accessible only by electronic invitation from the plaintiff, and if

accepted, a personal password to access the group.<sup>6</sup> The site included language that indicated the group was private and a place where Hillstone employees could discuss the "crap/drama/and gossip" related to their workplace. Employees posted sexual and profane comments, jokes about Hillstone's customer service "specs," drug use, and a new wine list given to employees. No Hillstone upper manager was invited to join the group, and members accessed the site only during nonwork hours and on noncompany computers.

An employee member of the chat group showed the communications to her manager, who, in turn, asked the employee for her password to the account. The employee reluctantly provided the password, believing she would be in trouble if she did not. The manager accessed the chat group several times and showed it to other managers. Hillstone then fired the chat group founder and another employee for posting critical comments that it deemed offensive and violating the company's core values. The two terminated employees sued, and the jury found Hillstone liable for violation of the SCA. The plaintiffs won compensatory and punitive damages. The jury found that the employee who reluctantly turned over her password to the manager had not done so voluntarily and had not authorized Hillstone management to access the chat group multiple times without her permission. While the jury found that the employer violated the SCA, it also concluded that the employer was not liable for invasion of privacy, finding that the plaintiffs had no reasonable expectation of privacy in the MySpace group.<sup>7</sup>

Although the SCA and Labor Code Section 980 prohibit unauthorized access to employee social media accounts, they do not bar employers from viewing employee social media communications altogether. So long as the employer has done nothing unlawful to access or view the social media communications, there is no violation of these laws. In *Ebling v. Monmouth-Ocean Hospital Service*, a nurse maintained a private Facebook account on which she friended only other employees, not managers.<sup>8</sup> One of the nurse's supervisors friended her and saw a post by the nurse about a recent shooting at a holocaust museum in Washington, D.C., that stated "I blame the DC paramedics. I want to say 2 things to the DC medics. 1. WHAT WERE YOU THINKING? and 2. This was your opportunity to really make a difference! WTF!!!! And to the other guards...go to target practice." The supervisor turned over the post to a hospital manager, and the nurse sued the hospital for violation of the SCA. The court ruled for the hospital because the manager had not accessed the nurse's account and was shown the post by someone the nurse had authorized to view it.<sup>9</sup>

While it may be tempting to gain consent to access an employee's personal social media site by sending or accepting friend requests, employers should avoid friending, following, or connecting with employees on social media and maintain policies prohibiting, or at

**Kalley Aman and Ruth Seroussi practice labor and employment law and litigation with Buchalter Nemer PC in Los Angeles.**

least discouraging, managers from doing so. Social media sites are filled with a wide range of personal information about employees, such as their sexual orientation, medical issues, religion, age, national origin, or other information protected by antidiscrimination statutes. If an employer later disciplines or terminates an employee who is social media friends with a manager, the employee may claim (and may establish at least a prima facie case) that the employment decision was based on the protected information the manager learned from the social media site, and not on job-related criteria.

For example, in *TerVeer v. Billington*,<sup>10</sup> an employee of the Library of Congress sued the library and his former supervisor, alleging that he was harassed and humiliated by his supervisor and terminated after the supervisor's daughter became Facebook friends with him. TerVeer liked a page that supported a same-sex parent campaign against bullying. The supervisor's daughter commented on the post: "Don't tell me you're weird like that." TerVeer alleged that before the post, he had a great relationship with his supervisor, who had even set him up with his daughter. After his post, however, the supervisor began to harass him, mock diversity, and lecture him on the "sin" of homosexuality. The library filed a motion to dismiss, and the District Court partially denied the motion, ruling that TerVeer stated claims for sex and religious discrimination, retaliation, and hostile work environment.<sup>11</sup> This recently settled case illustrates the potential consequences of learning private information about an employee through their personal social media.

### Social Media as Concerted Activity

The National Labor Relations Act provides that "[e]mployees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection."<sup>12</sup> The act also makes it an unfair labor practice for an employer to interfere with, restrain, or coerce employees in the exercise of these rights.<sup>13</sup>

Many states, including California, have enacted similar laws protecting employees from retaliation by employers for engaging in concerted activity. California Labor Code Sections 232 and 232.5 prohibit employers from requiring employees to refrain from disclosing the amount of their wages or working conditions or discharging, disciplining, or discriminating against employees who disclose the amount of their wages or their working conditions. Section 232.5, however, specifically provides that the statute is not intended to permit an employee to disclose

an employer's proprietary information, trade secret information, or information that is otherwise subject to a legal privilege without the consent of his or her employer.

In recent years, the NLRB has been actively prosecuting employers for violations of the rights of employees to engage in concerted activities, including those of a nonunionized employee on social media. As a recent article in the *New York Times* put it, the NLRB is intervening in social media to "expand its power" and "remain relevant as private-sector unions dwindle in size and power."<sup>14</sup> The NLRB, however, claims that social media sites are the new "virtual water coolers" and that it is "merely adapting the provisions of the National Labor Relations Act, enacted in 1935, to the 21st century workplace."<sup>15</sup> Either way, employers should understand that, under certain circumstances, an employee's expression of dissatisfaction in the workplace on social media may be protected concerted activity under the NLRA, even if the employees are not union members and there is no effort to unionize and no explicit reference to hours, pay, or other working conditions.

For example, in *NLRB v. Karl Knauz Motors, Inc. d/b/a Knauz BMW*, a car salesman posted a sarcastic comment on Facebook criticizing his employer for serving cheap food at a BMW sales event, and posting pictures of colleagues handing out hot dogs and water.<sup>16</sup> Later that day, another dealership owned by the employer let a 13-year-old sit in the driver's seat of a car, and the child accidentally drove the car into a pond. The salesman posted photos of the accident on Facebook, commenting: "This is your car. This is your car on drugs." The salesman was fired one week later for the posts. The NLRB filed a complaint on the salesman's behalf, contending that the Facebook posts were protected activity. The administrative law judge concluded that the first post was protected because the terminated employee and other salespersons shared communications about the cheap food, which could have impacted sales, and thus their commissions.<sup>17</sup> The judge concluded that the second post was not protected concerted activity because it did not discuss terms and conditions of employment and, on that basis, upheld the employer's decision to terminate the salesman.<sup>18</sup>

In *NLRB v. Three D, LLC d/b/a Triple Play Sports Bar and Grille*, a Second Circuit case, two current employees responded to a Facebook post by a former employee regarding the employer's mistakes in withholding taxes, which caused the employees to owe additional state taxes.<sup>19</sup> One employee liked the former employee's initial post. The second employee, whose privacy settings permitted only her friends to view her posts, posted one comment: "I owe too. Such an a\*\*hole."<sup>20</sup>

Both employees were terminated when the employer saw the posts. The administrative law judge recognized there is a balance to be struck between the rights of employees and legitimate employer interests in protecting its reputation but concluded that the employees' posts were protected concerted activity because they were not so disloyal, disparaging, reckless, defamatory, or maliciously untrue so as to lose protection under the NLRA and were not directed at the general public.<sup>21</sup>

In *NRLB v. Design Technology Group, LLC d/b/a Bettie Page Clothing*, a group of employees complained to their supervisor and the owner about working late hours in an unsafe neighborhood. Later that night, the employees engaged in a discussion on Facebook complaining about their employer without explicitly referring to their complaints about working late hours. One employee posted that she would be bringing a "California Worker's Rights" book to work the next day and that her mother worked for a law firm specializing in labor law. Another employee showed the posts to the manager, who terminated the employees. The NLRB ruled against the employer, holding that the posts were conversations for mutual aid and protection and "concerted protected activity."<sup>22</sup>

Although the NLRB has adopted a broad interpretation of "protected concerted activity" in the social media context, mere griping about the workplace is not enough to fall within the protections of the NLRA. In *Tasker Healthcare Group d/b/a Skinsmart Dermatology*, an employee and nine other former and current employees participated in a private group chat on Facebook.<sup>23</sup> After discussing a social event, the employee began venting about a supervisor, used profanity, and wrote: "FIRE ME...Make my day." Later that morning, one of the employees in the chat showed the post to the employer. The employer terminated the employee, stating she obviously was no longer interested in working there. The NLRB concluded that the post was not protected activity as it did not involve shared employee concerns over terms and conditions of employment. Rather, the post was mere griping by an employee who failed to look forward to any action.<sup>24</sup>

While the NLRB has not established a bright line rule for what constitutes protected concerted activity, social media communications among employees concerning any condition or aspect of the workplace and contemplating future action are likely protected activity. If, however, the communications are disloyal, disparaging, reckless, defamatory, or maliciously untrue, they may lose protection under the NLRA, especially if they are directed at the general public. If an employee is merely griping about the employer and not discussing forward-looking group activity among em-

ployees, the comments are not protected.<sup>25</sup> Because each case is different, employers should exercise caution and seek counsel before taking action against an employee for his or her content on personal social media.

### Free Speech

Public employee communications on social media may also be protected by the First Amendment. In *Bland v. Roberts*, the sheriff of Hampton, Virginia ran for re-election. During the campaign, one of the deputy sheriffs liked the Facebook page of the sheriff's electoral opponent. The sheriff won re-election and fired the deputy sheriff and five other employees of the department who had shown support for the sheriff's opponent. The employees sued, claiming that the sheriff retaliated against them because they supported his opponent, and the firings violated their right of free speech. The trial court ruled that a Facebook like did not constitute protected speech, but the Fourth Circuit reversed, holding that the Facebook like was in fact protected by the First Amendment.<sup>26</sup> Although private sector employees have tried to bring claims against their employers for violation of the First Amendment arising out of their social media use, courts have rejected these claims because they do not involve state action and relate to private employment matters.<sup>27</sup>

### Ownership of Social Media Accounts

As social media proliferates, more employers are hiring employees to create and maintain company social media sites. While it may seem clear to the employer that it owns the social media sites established by and operated for the business, employees may not necessarily agree. In *Phone Dog v. Kravitz*, an employee established and operated a Twitter account for his employer under the Twitter handle @phonedog\_noah.<sup>28</sup> Over time, the Twitter account grew to approximately 17,000 followers, and advertisers paid for advertising space on the Twitter account, generating revenue for the employer. When the employee left Phone Dog, he changed the Twitter account name to @noahkravitz. Phone Dog sued, arguing that it owned the Twitter account and login information. The case settled before any ruling on the merits, but the dispute underscores the importance of maintaining a clear policy that the employer owns all company social media sites, along with their usernames and passwords.

In a similar case in England, *Whitmar Publications Ltd v. Gamage*, four senior employees set up a competing business while still employed with the plaintiff.<sup>29</sup> They used their employer's LinkedIn groups to promote their new company and refused to turn over the login information after leaving. The British court issued injunctions against the former

employees, ruling that the LinkedIn account and login information were Whitmar's protected confidential and proprietary information. The ruling in *Whitmar* emphasizes the need for clear policies stating that the employer owns all social media sites, accounts, and login information.

### Recommended Policies

Given the current state of the law, the best way for an employer to avoid disputes with employees over social media use is by drafting clear, narrowly tailored employment policies that balance the employer's and employees' legitimate interests. Among other things, social media policies should prohibit:

- Discrimination, harassment, and abusive conduct on social media.
- Disclosure of the employer's trade secrets and confidential and proprietary information.
- Use of personal social media during work hours.
- Management requests that employees provide access to, or information from, their personal social media accounts.
- Friend requests from managers to employees, along with management's following employees on social media sites or otherwise attempting to insert themselves into employee social media communications without clear, written employee consent.
- Management's acceptance of friend requests or other invitations to follow or link with employees on social media sites.

A social media policy should also clearly state that the employer owns all social media sites established, maintained, accessed, or operated by employees for the company for business purposes during their employment, including all passwords and login information. Employers should avoid any language in a social media policy that could be interpreted as prohibiting or chilling the right of employees to engage in concerted activity and, in particular, discussions over wages, hours, and working conditions. While employers may be permitted to discipline an employee for mere griping about the employer on social media, a social media policy should avoid broadly prohibiting communications by employees on social media that are "inappropriate," "disparaging," "confidential," or "embarrassing" to the company.

Finally, employers should be aware of a recent ruling concerning employee e-mail use. In *Purple Communications*, the NLRB reversed its longstanding position and ruled that an employer may not maintain a policy prohibiting employees who are given company e-mail accounts from using those accounts during nonworking hours to engage in concerted activity and discuss wages and working conditions with other employees.

An employer may only restrict these communications if they substantially disrupt or interfere with production and productivity.<sup>30</sup>

As the cases above indicate, employers face restrictions on accessing and regulating the social media posts of employees. While an employer may guard its trade secrets and business reputation, as well as act to prevent abusive employee conduct, an employer cannot prohibit the legally protected social media activities of employees. Employers that are too heavy-handed in their monitoring of the social media activities of employees may find themselves liable under state and federal law. ■

<sup>1</sup> See, e.g., *NRLB v. Pietrylo v. Hillstone Rest. Group d/b/a Houston's*, No. 06-5754 (D. N.J. Sept. 25, 2009) (unpublished); *NRLB v. Design Tech. Group, LLC d/b/a Bettie Page Clothing*, 359 NLRB No. 96 (Apr. 19, 2013); *NRLB v. Three D, LLC d/b/a Triple Play Sports Bar and Grille*, 361 NLRB No. 31. (Aug. 22, 2014).

<sup>2</sup> Labor and Management Relations Act, 29 U.S.C. §157; Stored Commc'ns Act, 18 U.S.C. §§2701 et seq.

<sup>3</sup> 18 U.S.C. §§2701 et seq.

<sup>4</sup> Many states have enacted statutes regulating access to employee social media sites. See, e.g., ARK. CODE ANN. §11-2-124; COLO. REV. STAT. §8-2-127; 820 ILL. COMP. STAT. 55/10; MD. CODE ANN., LAB. & EMPL. §3-712; MICH. COMP. LAWS SERV. §§37.271 et seq.; NEV. REV. STAT. §613.135; N.J. STAT. ANN. §§34:6b-5 et seq.; N.M. STAT. ANN. §50-4-34; OR. REV. STAT. §659a.330; UTAH CODE ANN. §§34-48-101 et seq.; WASH. REV. CODE §49.44.200.

<sup>5</sup> LAB. CODE §980(c).

<sup>6</sup> *Pietrylo v. Hillstone Res. Group*, 2008 U.S. Dist. LEXIS 108834 (D. N.J. July 24, 2008).

<sup>7</sup> *Id.*

<sup>8</sup> *Ehling v. Monmouth-Ocean Hosp. Serv.*, 872 F. Supp. 2d 369 (D. N.J. 2012).

<sup>9</sup> *Id.*

<sup>10</sup> *TerVeer v. Billington*, No. 12-cv-01290, 2014 WL 1280301 (D. D.C. Mar. 31, 2014).

<sup>11</sup> *Id.*

<sup>12</sup> 29 U.S.C. §157.

<sup>13</sup> 29 U.S.C. §158(a)(1).

<sup>14</sup> Steven Greenhouse, *Even If It Enrages Your Boss, Social Net Speech Is Protected*, N.Y. TIMES (Jan. 21, 2013), available at <http://www.nytimes.com>.

<sup>15</sup> *Id.*

<sup>16</sup> *NLRB v. Karl Knauz Motors, Inc. d/b/a Knauz BMW*, No. 13-CA-46452 (Sept. 28, 2011).

<sup>17</sup> *Id.* at 9.

<sup>18</sup> *Id.*

<sup>19</sup> *NRLB v. Three D, LLC d/b/a Triple Play Sports Bar and Grille*, 361 NLRB No. 31. (Aug. 22, 2014).

<sup>20</sup> *Id.* at 2.

<sup>21</sup> *Id.* at 5-6.

<sup>22</sup> *NRLB v. Design Tech. Group, LLC d/b/a Bettie Page Clothing*, 359 NLRB No. 96 (Apr. 19, 2013).

<sup>23</sup> *Tasker Healthcare Group d/b/a/ Skinsmart Dermatology*, No. 04-CA-094222 (May 8, 2013).

<sup>24</sup> *Id.*

<sup>25</sup> *Id.*

<sup>26</sup> *Bland v. Roberts*, 730 F. 3d 368 (4th Cir. 2013).

<sup>27</sup> *Pietrylo v. Hillstone Res. Group*, 2008 U.S. Dist. LEXIS 108834 (D. N.J. July 24, 2008).

<sup>28</sup> *Phone Dog v. Kravitz*, Case No. 11-03474 (N.D. Cal. Nov. 8, 2012).

<sup>29</sup> *Whitmar Publ'ns Ltd v. Gamage & Ors* [2013] EWHC 1881 (Ch).

<sup>30</sup> *Purple Commc'ns*, 361 NLRB No. 126 (2014).