



Social Media and the Workplace

By John R. Lanham

Social media has undergone exponential growth over the past few years, with profound consequences for employers. Social media – characterized by accessibility, interactivity, and technology – includes blogs, wikis (interlinked collaborative web sites), photo-sharing sites, and Internet forums and extends to social networking utilities like MySpace and Facebook. The public has turned to these information outlets with surprising speed. For example, Facebook had approximately 5.5 million active members in December 2005.¹ In December 2009, it reached in excess of 350 million active members.² In addition to access via computers, many social media sites are accessible using mobile phone–based applications or, like Twitter, through mobile phone SMS messaging. This allows for immediate, and often public, broadcasting of users’ opinions or conduct.

Social media technology has a significant impact on the workplace. Employees may upload personal information that an organization believes is inconsistent with its image or mission. Social media also provides a venue for groups of employees to discuss work-related issues outside of management oversight. Moreover,

an employee could inadvertently share confidential business information, such as a pending acquisition, that harms the employer or raises securities law issues. Management increasingly recognizes these risks. One recent survey revealed that sixty percent of executives say they have “‘a right to know’ how their employees portray themselves and their organizations online.”³ Only seventeen percent of the executives, however, said their company has a program for “monitoring and mitigating risks related to social networks.”⁴ Such an approach to employees’ online conduct, combined with the ever-increasing presence of social media, creates a significant liability risk for employers.

This alert provides a sampling of U.S. state and federal laws that may affect a company’s monitoring of its employees’ involvement in social media. These laws can vary significantly between jurisdictions, so it is important that an employer discuss this subject with counsel.⁵ Employees’ online communications may gain legal protection based on either the privacy or the substance of the communications. In order to avoid exposure to considerable liability, employers should develop an

approach to personal online conduct and apply that approach in both policy and practice.

I. PRIVACY ISSUES

Social media and electronic communications raise unique issues for workplace privacy. Employees in the U.S. may derive privacy rights from an array of federal and state laws. This section provides examples of these laws, which include common-law privacy rights, state constitutional rights, and statutory restrictions.

A. Common Law and State Constitutional Privacy Protections

Most states permit common-law claims for invasion of privacy, and some states, such as California, also provide constitutional privacy rights that may apply to private-sector employers. These legal theories consider whether the individual had a reasonable expectation of privacy and whether there was a serious or offensive invasion of that expectation of privacy. From an employer's perspective in monitoring social media use, a key factor is whether employees have a reasonable expectation of privacy in their social media communications. Employees' reasonable expectations of privacy may be affected by both the nature of the social media communication and the employer's electronic communications policy.

First, many social media sites make user content available to the public. Typically, employees do not have a reasonable expectation of privacy for

content they post to a public site. For example, a California court of appeal held that a MySpace user had no reasonable expectation of privacy for a post she made on her page, despite the fact that her MySpace page identified her by first name only and that she deleted the post after six days.⁶ Some social media sites, however, allow users to restrict access to information to a select group of individuals or use password protection. Under these circumstances, at least one court has suggested that an employee may have a reasonable expectation of the privacy of the communications or information.⁷

Second, a court is likely to give employee handbooks and company policies weight in determining whether an employee had a reasonable expectation of privacy. This is particularly the case when a handbook clearly states that company property is not for private use, and that the company may monitor employee e-mail and computer usage.⁸ These decisions underscore the importance of adopting a social media and electronic communications policy. Employers should note, however, that a court may consider management's practices as well as company policy. In *Quon v. City of Ontario*, the Ninth Circuit found that a manager's informal promise about privacy created a reasonable expectation of privacy, notwithstanding a written policy that reserved the employer's rights to monitor.⁹ The U.S. Supreme Court recently granted *certiorari* on

the issue of whether the manager's informal promises created a reasonable expectation of privacy.

Employers should check with counsel to determine the parameters of protection of the common law and state constitutions where they do business. In addition, some states require employers to provide notice to employees who are under electronic monitoring.¹⁰ Employers should therefore have a clear policy about electronic monitoring.

B. Statutory Privacy Protections

Employees' electronic communications may also trigger statutory privacy protections. Electronic and wire communications are subject to a variety of laws, including the Federal Wiretap Act, the Stored Communications Act ("SCA"),¹¹ and state surveillance and wiretap statutes. The most common cause of action for social media-related claims has been the Stored Communications Act (SCA). The SCA prohibits the knowing or intentional unauthorized access to "a facility through which an electronic communication service is provided."¹² Practically speaking, this includes unauthorized access to a password-protected e-mail account or social networking group. State statutes covering electronic communications and wiretaps also exist, so employers should consult with counsel concerning all of the surveillance laws to which they may be subject.

The SCA permits a person to authorize a third party's access to stored electronic communications if (i) the person is the provider of the service, or (ii) the person is a user of the service and the communication is from or intended for that user.¹³ Accordingly, the SCA usually allows an employer to access stored communications located on its own systems. In comparison, the SCA limits an employer's ability to access stored communications that are maintained by a third-party service provider, without the user's authorization.¹⁴ In theory, therefore, an employee could authorize a supervisor to access a password-protected third-party social media site, such as by providing his or her login information. In practice, however, employers must exercise caution with this exception. A jury recently found that an employer violated the SCA by accessing a restricted-access employee chat group on MySpace, using an employee's login information. The jury rejected the employer's argument that the employee had authorized her managers to access the chat group, following the employee's testimony that she felt she "had" to give management her password to a private MySpace group and that she thought she "probably would have gotten in trouble" if she did not turn over the password.¹⁵ Additionally, courts have interpreted this exception narrowly. For example, the Ninth Circuit concluded that an employee was not a "user" who could authorize

access to a website because, while he was on a list of people allowed access, there was no evidence that he had actually logged in to the website.¹⁶ Moreover, the consequences of a SCA violation can be serious. The statute creates criminal liability for intentional unauthorized access and courts may allow recovery of punitive damages and attorney fees without a showing of actual damages.¹⁷ State statutes may contain similar restrictions and penalties.

II. PROTECTIONS BASED ON THE SUBSTANCE OF THE COMMUNICATION

In addition to privacy considerations, employers setting a social media policy should also consider laws that protect the substance of employees' online conduct. It will surprise some employers to learn that, even in a state with at-will employment, there may be restrictions on disciplining employees for their comments and actions. For example, in some states employers are restricted in disciplining employees for their legal conduct outside the workplace. In addition, employers need to carefully approach statements regarding workplace conditions or the terms of employment, even if they are critical of the company.

A. *Off-Duty Conduct Statutes*

Some states, including Colorado and New York, have enacted legislation to protect employees' conduct outside the workplace.¹⁸ These statutes vary in scope and effect,

so employers should consult with counsel if they operate in a state with an off-duty conduct statute. Generally, however, these statutes restrict an employer's ability to discipline employees for engaging in legal activities while not at work. In the social media context, these statutes may, for example, limit an employer's ability to terminate an employee who posts photographs of himself drinking alcohol and smoking tobacco.

New York's off-duty conduct restricts employers' ability to take adverse employment action (including hiring, pay, workplace conditions, and termination) against employees engaged in recreational activities.¹⁹ The statute contains exceptions, such as restrictions based on conflicts with the employer's business interests. In application, courts have taken a fairly limited view of what constitutes a "recreational activity." For example, courts have found romantic relationships²⁰ and picketing²¹ not entitled to protection.

Colorado's off-duty conduct statute is slightly narrower than New York's version, as the Colorado statute only protects employees from termination. The Colorado statute also provides three exceptions for: (i) restrictions relating to a bona fide occupational qualification; (ii) restrictions relating to employment activities of a particular employee or group of employees rather than all employees; and (iii) restrictions

necessary to avoid a conflict of interest or the appearance of a conflict of interest with employees' responsibilities.²² In *Marsh v. Delta Air Lines*, a Colorado U.S. District Court found that an implied duty of loyalty with regard to public communications was a bona fide occupational qualification under the statute.²³ The court then concluded that an employee's letter in a local newspaper, criticizing Delta's customer service, breached his duty of loyalty and that the off-duty conduct statute did not protect him from termination. But it is insufficient to assume that an employee may be terminated for off-site comments that relate to his or her employment. A Colorado appellate court recently questioned *Marsh's* precedential value and read the off-duty conduct statute to protect an employee complaint about workplace safety made to OSHA on the employee's personal time.²⁴ Colorado employers could try to avoid this uncertainty by establishing a handbook policy that employees owe the company a duty of loyalty.

If an employer does business in a state with an off-duty conduct statute, it should work with counsel to ensure its approach to social media and electronic communications does not conflict with applicable law. It should also discuss any specific concerns about off-site conduct in order to determine if statutory exceptions could apply.

B. National Labor Relations Act

In addition to legal off-site conduct, employees' communications regarding the terms and conditions of employment may enjoy legal protection. The National Labor Relations Act ("NLRA") protects employees involved in unions and collective bargaining. In addition, the NLRA gives employees the right to "engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection."²⁵ This does not mean, however, that employees have *carte blanche* to criticize an employer under the NLRA. Generally, the independent actions of a single employee are not considered concerted activity, unless he or she is attempting to enlist other employees, or is acting based on prior concerted activity.²⁶ The employee's actions must also relate to the terms and conditions of employment.²⁷ Additionally, egregious or profane statements not made "in the heat of discussion" may not be protected, even if the conduct occurred in the course of otherwise protected activity.²⁸ Even with these qualifications, it is conceivable that an employee's communications about working conditions or a difficult manager could become concerted activity, particularly if the employee directs these communications at other employees.

C. Whistleblowing and Retaliation

A patchwork of federal and state statutes protects employees who

report wrongdoing within their employer company. For example, both the Sarbanes-Oxley Act and OSHA protect whistleblowing employees.²⁹ Many states have also enacted protections for whistleblowers. Courts have not clearly established that whistleblower protections apply to social media, and it is not certain that a social media communication satisfies some statutes' requirements to assist in an investigation. Nonetheless, employers should take whistleblower protections into account when creating a social media policy. This will also provide a good opportunity for assessing internal reporting systems and reminding employees about the proper ways to raise their concerns.

Additionally, federal and state anti-discrimination laws may restrict an employer's ability to discipline employees for communications that could be viewed as complaints of discrimination. For instance, Title VII of the Civil Rights Act of 1964 makes it "an unlawful employment practice for an employer to discriminate against any of his employees . . . (1) because he has opposed any practice made an unlawful employment practice by this subchapter, or (2) because he has made a charge, testified, assisted, or participated in any manner in an investigation, proceeding, or hearing under this subchapter."³⁰ The Supreme Court recently construed "oppose" broadly to include actions beyond active or consistent behavior.³¹ Under this

broad definition, it is possible that making a complaint through social media could constitute opposition. It is therefore important that employers take seriously any comments related to the treatment of a protected class, regardless of the form of the communication.

D. Wrongful Termination

Similar to Fourth Amendment unreasonable search concerns, private employers typically do not confront First Amendment freedom of speech issues. Some courts, however, have considered whether the First Amendment, or similar rights in state constitutions, might create a clear mandate of public policy for wrongful termination torts against private employers.³² In addition, state statutes may specifically create a cause of action against private employers for disciplining employees' exercise of First Amendment rights.³³

E. Attorney-Client Privilege

If a dispute over an employee's online activities ends in litigation, counsel should exercise caution in reviewing employee electronic communications. An employee's communications with a personal attorney may be privileged even if they were made using company property. In *Stengart v. Loving Care Agency, Inc.*, a New Jersey appellate court recently held that an employee's e-mails with her attorney, made using a web-based e-mail account on a company computer, remained privileged even in the presence of a company electronic communications

policy.³⁴ The court found that the attorney-client privilege outweighed the company's stated policy that e-mail is not private. The court then concluded the law firm's review of the e-mail was "inconsistent with" state ethical rules and remanded for consideration of sanctions and disqualification. *Stengart* is in the process of appeal to the New Jersey Supreme Court, and has been distinguished by the employee's use of a personal, rather than corporate, e-mail service.³⁵ It serves, however, as an important reminder that attorneys should be familiar with applicable ethical rules, particularly for new issues like electronic communications.

III. EMPLOYER POLICIES

In order to mitigate the risk of liability under the laws discussed above, it is important that an employer adopt a cohesive approach to social media communications. This approach will need to be tailored to the applicable laws and the nature of the employer's organization, as well as the employer's specific concerns about social media. For example, some organizations may be concerned about their public image, while others will want to prevent the inadvertent disclosure of confidential information. Additionally, social media may be an asset to sales and client-oriented businesses, as it allows employees to keep in contact with potential customers. For such employees, companies can encourage the use of social networking sites with a professional, rather than social, emphasis. Even in these situations,

employers should clearly delineate what type of conduct is permitted. An effective social media program will take a two-pronged approach that covers both written policy and management training.

First, employers should adopt written policies governing electronic communications and ensure that employees and management observe the policies in practice. Having a written policy is important not only because it can help shape employee conduct, but also because courts afford employer policies weight in a common-law privacy analysis. The substance of an electronic communications or social media policy should take the employer's organization needs into account. For employers that value confidentiality, adopting a bright-line prohibition of social media communications related to the employer's business may sound appealing. This approach, however, could run afoul of the National Labor Relations Act, state off-duty conduct statutes, and whistleblower or anti-retaliation protections. The better approach is to urge employees to separate their personal and professional digital lives. For example, an employer could consider restricting the use of personally-owned technology at work and prohibiting the use of company-owned equipment for social media. Employers should also clearly explain that employees are prohibited from sharing any confidential information, whether through social media or otherwise. Additionally, an electronic

communications and social media policy should explain that the employer reserves and exercises the right to monitor all communications made using company property. The policy should also remind employees that they are subject to discipline for inappropriate electronic communications. Importantly, employers should offer training to employees on the appropriate use of social media under this policy.

Second, employers should train supervisors and managers on how to handle social media issues. To date, the bulk of litigation over employee social media use has focused on management's conduct, rather than the substance of the employees' communications. This training should include instruction on handling privacy issues related to employee use of technology. While a written social media and electronic communications policy may change employees' reasonable expectations of privacy, it may not affect less flexible laws like the Stored Communications Act. Employers should therefore instruct managers to contact human resources or legal counsel before attempting to gain access to non-public employee communications. Employers should also consider training management to treat employees' work-related social media comments with the same seriousness as workplace complaints.

Finally, while this alert addresses employer monitoring of employees' personal social media

communications, companies that involve themselves or their employees in social media face additional considerations. Notably, the Federal Trade Commission recently updated its Guides Concerning the Use of Endorsements and Testimonials. The updated standards provide that material connections between endorsers and advertisers must be disclosed, and specifically apply this rule to social media.³⁶ This rule may affect employees' personal social media use, such as blogs. Among other safeguards, employers should be clear that employees must identify themselves as such if they comment on a company-related issue and state that they are expressing only their own views. Employers involved in social media should also consider compliance with securities laws, including Regulation Fair Disclosure, which governs disclosure of material nonpublic information, and the applicability of safe harbor protections for forward-looking information.

Though the law in this area may be unsettled, there are no signs that the growth of social media is waning. By adopting a plan for handling social media, employers will be able to handle emerging personnel issues efficiently, consistently, and legally. ■

¹ Facebook, *Facebook: Timeline*, <http://www.facebook.com/press/info.php?statistics#/press/info.php?timeline>.

² *Id.*

³ Deloitte LLP, *2009 Ethics & Workplace Survey Results* at 2 (2009), <http://www.deloitte.com/assets/Dcom-UnitedStates/>

[Local%20Assets/Documents/us_2009_ethics_workplace_survey_220509.pdf](http://www.deloitte.com/assets/Documents/us_2009_ethics_workplace_survey_220509.pdf).

⁴ *Id.* at 5.

⁵ Laws regulating this area also vary significantly in foreign jurisdictions, such as European Union Member States.

⁶ *See, e.g., Moreno v. Hartford Sentinel, Inc.*, 172 Cal. App. 4th 1125 (Cal. Ct. App. 2009).

⁷ *See Pietrylo v. Hillstone Rest. Group*, 2008 U.S. Dist. LEXIS 108834, at *17-20 (D.N.J. Jul. 24, 2008).

⁸ The Seventh Circuit held that when an employer "announced that it could inspect the laptops that it furnished for the use of its employees," an employee could have no reasonable expectation of privacy under the Fourth Amendment for files on the laptop. *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002). Some district courts reached a similar conclusion for common-law invasion of privacy claims. *See, e.g., Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863, at *68-70 (D. Or. Sept. 15, 2004).

⁹ *See Quon v. City of Ontario*, 529 F.3d 892, 897 (9th Cir. 2008), *cert. granted*, 2009 U.S. LEXIS 9058 (U.S. Dec. 14, 2009).

¹⁰ For example, some states like Delaware and Connecticut require employers to give notice to employees who will be subject to electronic monitoring. *See Conn. Gen. Stat. § 31-48d*; 19 Del. C. § 705.

¹¹ The Wiretap Act, 18 U.S.C. § 2510 et seq., is more formally referred to as the Electronic Communications Privacy Act ("ECPA"). The Stored Communications Act is codified at 18 U.S.C. § 2701 et seq. A violation of the ECPA, unlike an SCA violation, requires "interception" of the contents of a communication contemporaneous with the communication. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878-79 (9th Cir. 2002). The ECPA is therefore a less likely cause of action for employer monitoring of social media, which typically involves accessing stored information. However, if the employer is engaged in "real-time" interception or monitoring of an employee's postings or other electronic communications, employers must consider limitations under the ECPA as well.

¹² 18 U.S.C. §§ 2701, 2707.

¹³ 18 U.S.C. § 2701(c)(2).

¹⁴ This issue arose in *Quon v. Arch Wireless*, in which the Ninth Circuit determined that the SCA did not allow an employer to receive the content of text messages sent by

This newsletter addresses recent employment law developments. Because of its generality, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.

Editor: Lloyd W. Aubry, Jr., (415) 268-6558

San Francisco

Lloyd W. Aubry, Jr. (415) 268-6558
laubry@mofocom

James E. Boddy, Jr. (415) 268-7081
jboddy@mofocom

Karen Kubin (415) 268-6168
kkubin@mofocom

Linda E. Shostak (415) 268-7202
lshostak@mofocom

Eric A. Tate (415) 268-6915
etate@mofocom

Palo Alto

Christine E. Lyon (650) 813-5770
clyon@mofocom

Joshua Gordon (650) 813-5671
jgordon@mofocom

David J. Murphy (650) 813-5945
dmurphy@mofocom

Raymond L. Wheeler (650) 813-5656
rwheeler@mofocom

Tom E. Wilson (650) 813-5604
twilson@mofocom

Los Angeles

Timothy F. Ryan (213) 892-5388
tryan@mofocom

Janie F. Schulman (213) 892-5393
jschulman@mofocom

New York

Miriam H. Wugmeister (212) 506-7213
mwugmeister@mofocom

Washington, D.C./Northern Virginia

Daniel P. Westman (703) 760-7795
dwestman@mofocom

San Diego

Craig A. Schloss (858) 720-5134
cschloss@mofocom

Denver

Steven M. Kaufmann (303) 592-2236
skaufmann@mofocom

London

Ann Bevitt 44-20-7896-5841
abevitt@mofocom

its employees through a third-party pager service—even though the employer paid for that service. *See* 592 F.3d 892.

¹⁵ *See Pietrylo v. Hillstone Rest. Group*, 2008 U.S. Dist. LEXIS 108834, at *8-10 (D.N.J. Jul. 24, 2008).

¹⁶ *Konop*, 302 F.3d at 880.

¹⁷ *Van Alstyne v. Elec. Scriptorium, Ltd.*, 560 F.3d 199, 209 (4th Cir. 2009).

¹⁸ California has also enacted an off-duty conduct statute. The statute is broadly worded and authorizes the Labor Commissioner to assert “[c]laims for loss of wages as the result of demotion, suspension, or discharge from employment for lawful conduct occurring during nonworking hours away from the employer’s premises.” Cal. Lab. Code § 96(k). California courts, however, have limited this provision to “recognized constitutional rights,” in essence concluding that it does not contain substantive protection beyond existing law. *Barbee v. Household Auto. Fin. Corp.*, 113 Cal. App. 4th 525, 534 (Cal. Ct. App. 2003).

¹⁹ N.Y. Lab. Law § 201-d.

²⁰ *State v. Wal-Mart Stores*, 207 A.D.2d 150 (N.Y. App. Div. 3d Dep’t 1995).

²¹ *Kolb v. Camilleri*, 2008 U.S. Dist. LEXIS 59549 (W.D.N.Y. Aug. 1, 2008) (decision of magistrate judge).

²² C.R.S. 24-34-402.5(1).

²³ *Marsh v. Delta Airlines*, 952 F. Supp. 1458, 1462-63 (D. Colo. 1997); *but see Watson v. Pub. Serv. Co.*, 207 P.3d 860, 864 (Colo. Ct. App. 2008) (noting no Colorado court of appeals has adopted *Marsh*), *cert. denied*, 2009 Colo. LEXIS 436 (Colo. 2009).

²⁴ *Watson*, 207 P.3d at 864.

²⁵ 29 U.S.C. § 157.

²⁶ *See generally NLRB v. Mike Yurosek & Son*, 53 F.3d 261, 264-66 (9th Cir. 1995).

²⁷ *Id.* at 266-67.

²⁸ *See Media Gen. Operations, Inc. v. NLRB*, 560 F.3d 181, 186 (4th Cir. 2009); *see also Timpte, Inc. v. NLRB*, 590 F.2d 871 (10th Cir. 1979).

²⁹ 18 U.S.C. § 1514A; 29 U.S.C. § 660.

³⁰ 42 U.S.C. § 2000e-3(a).

³¹ *Crawford v. Metro. Gov’t of Nashville & Davidson County*, 129 S. Ct. 846, 851 (U.S. 2009).

³² Courts in California and some other states have rejected private-sector wrongful discharge claims based on public policy of the First Amendment. *See, e.g., Grinzi v. San Diego Hospice Corp.*, 120 Cal. App. 4th 72, 83 (Cal. Ct. App. 2004). The Third Circuit, however, recognized a tort for wrongful discharge in violation of public policy set by the First Amendment of the U.S. Constitution and the Pennsylvania Constitution. *Novosel v. Nationwide Ins. Co.*, 721 F.2d 894, 900 (3d Cir. 1983). Other courts have questioned whether *Novosel* remains good law. *See, e.g., Tiernan v. Charleston Area Med. Ctr., Inc.*, 506 S.E.2d 578, 588-90 (W. Va. 1998); *Grinzi*, 120 Cal. App. 4th at 83.

³³ *See Conn. Gen. Stat. Ann. § 31-51q.*

³⁴ *Stengart v. Loving Care Agency*, 408 N.J. Super. 54, 61 (App. Div. 2009).

³⁵ *Alamar Ranch, LLC v. County of Boise*, 2009 U.S. Dist. LEXIS 101866 (D. Idaho Nov. 2, 2009) (finding attorney-client communications made using company e-mail, with an electronic communications policy in place, not privileged).

³⁶ For more information on the updated Guides Concerning the Use of Endorsements and Testimonials, see our legal update at <http://www.mofocom/news/updates/files/16050.html>.

If you wish to change an address, add a subscriber, or comment on this newsletter, please write to:

Wende Arrollado
Morrison & Foerster LLP
12531 High Bluff Drive, Suite 100
San Diego, California 92130
warrollado@mofocom

www.mofocom

©2010 Morrison & Foerster LLP. All Rights Reserved.

John R. Lanham is an associate in our Denver office and can be reached at (303) 592-2278 and jlhanham@mofocom.