

Electronic Communications In The Social Media Age: What Is An Employer To Do — Or Not To Do?

Arthur P. Murphy & Geoffrey P. Wermuth*

Use it or not, like it or not, the use of social media is exploding. Eighty percent of companies use social media as a recruitment tool; 96% of the so-called “millennial generation” (those born between 1980–1995) belong to an online social network; there are 200+ million blogs on the Internet; and approximately 12% of married couples in the United States met via social media.¹ It cannot be ignored.

In this article, we review the major sources of federal law applicable to electronic communications and associated social media situations and employment, and some state cases as exemplars of how courts are dealing with such situations. We then discuss some broad guidelines for applicable employer policies and conduct. This is a rapidly evolving area, so employers are well advised to consult with counsel before taking

any definitive actions against employees or committing themselves to particular policies.²

I. MAJOR APPLICABLE FEDERAL LAWS

A. Electronic Communications Privacy Act

The Electronic Communications Privacy Act includes the federal Wiretap Act and the Stored Communications Act.³ The Wiretap Act prohibits unauthorized and intentional “interception” of wire, oral and electronic communications, including telephone calls and e-mail. The Stored Communications Act prohibits unauthorized accessing of electronically stored communications. An exception applies to entities that provide electronic communication systems and some courts have held that this exemption

covers employers providing internal e-mail systems.⁴

However, courts are divided as to whether this exception allows employers to monitor employee use of e-mail on external servers (e.g., Hotmail, Gmail) accessed via the employer’s computers.⁵ Where the employee’s activity does not leave a “trail” on the employer’s computer system, it is inadvisable for an employer to log into or access an employee’s personal web-mail account, e.g., use of “keylogger” software to record user keystrokes and obtain password. Such activity may result in an award of actual and/or punitive damages.⁶

In one case,⁷ a jury found a Stored Communications Act violation by an employer and awarded backpay and punitive damages to a group of restaurant employees who were terminated because of their par-

*Attorneys ARTHUR P. MURPHY and GEOFFREY P. WERMUTH are partners in the Quincy, Massachusetts law firm of Murphy, Hesse, Toomey & Lehane, LLP. Both concentrate on representing employers in labor and employment matters including representation before the National Labor Relations Board and other courts and administrative agencies, as well as day-to-day advice and guidance on such matters. This article was adapted from a series of presentations developed by firm partner Katherine A Hesse, and associates Thomas Colomb and Michael MacCaro, to whom much of the credit is due.

ticipation in a Myspace.com group dedicated to “venting” about their experience working at the restaurant. The content included vulgar and sexually explicit comments, as well as references to violence and illegal drug use, but was invitation-only and password-protected. The employer obtained access by seeking personal login information from one of the employee/participants. Notably, the jury rejected the employees’ claim for breach of privacy.

B. Computer Fraud and Abuse Act

The federal Computer Fraud and Abuse Act⁸ is a statute of broad application with criminal and civil penalties (including a private right of action) where individuals access and/or destroy data without authorization. The statute prohibits:

knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and . . . obtain[ing] anything of value,⁹ and

knowingly caus[ing] the transmission of a program, information, code, or command . . . [that] intentionally causes damage without authorization to a protected computer.¹⁰

Thus, if attempting to use this statute against an employee for computer misconduct, an employer must show (1) an absence of “authorized” access; and (2) statutorily defined damage or loss.

C. Communications Decency Act

The Communications Decency Act¹¹ broadly immunizes website owners (“service providers”) from liability based on content posted by third parties. This law may come into play where employers seek to discipline employee blog-creators based on what the employer perceives to be unacceptable/disloyal information posted on that blog by others. The applicability of this law to the employer/employee relationship remains uncertain as of this writing.

D. National Labor Relations Act

While it may come as a surprise to many non-unionized employers, the National Labor Relations Act¹² (“NLRA”) applies to virtually all private sector employers in the country regardless of whether or not their employees are represented by a union.¹³ Much of the litigation over discipline of employees for off-duty conduct related to the various forms of social media has been at the National Labor Relations Board (“NLRB”) and involved non-unionized settings.¹⁴

1. Protected Concerted Activity

Section 7 of the NLRA¹⁵ provides, in relevant part, that:

Employees shall have the right to self-organization, to form, join, or assist labor organizations . . . and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection . . .”

Thus for employee activity to be insulated from employer action under the Act, the employee activity has to be both “protected” and “concerted”. “Protected” activity is activity that comes within Section 7, i.e., complaining to an employer about wages, benefits or other terms and conditions of employment.¹⁶ “Concerted” activity is activity engaged in by more than one employee, or by one employee on behalf of other employees. Put together, “protected concerted activity” is, generally speaking, activity engaged in by more than one employee, or by one employee on behalf of others, relating to that employer’s terms and conditions of employment.

For example, the Hartford, CT, NLRB Region issued an unfair labor practice complaint alleging that American Medical Response, Inc., a non-union company, illegally terminated an employee who posted negative remarks about her supervisor on her personal Facebook page.¹⁷ While this employee in the first instance acted alone, suggesting that her activity was not “concerted,” the Region focused on the fact that the employee’s postings drew sup-

Electronic Communications In The Social Media Age: What Is An Employer To Do — Or Not To Do?

portive responses from her co-workers, and then further negative comments about the supervisor from the employee. Thus this activity was “protected” because it dealt with terms and conditions of employment, and “concerted” because eventually a group of employees became involved in support. The termination was alleged to be unlawful because the Company took an adverse employment action against the employee because of her exercise of her Section 7 rights.

The complaint in that case also alleged that the Company’s blogging and Internet posting policy was overbroad and contained unlawful provisions, including one that barred employees from making disparaging remarks when discussing the company or supervisors and another that prohibited employees from depicting the company in any way over the Internet without company permission. While the parties later reached a settlement, the Company was forced to revise its allegedly “overly-broad” rules in its employee handbook on blogging, Internet posting, and communications between employees to ensure that they did not improperly restrict employees from discussing their wages, hours and working conditions with co-workers and others.

Similarly, in Hispanics United

of Buffalo,¹⁸ also involving a non-union employer, an Administrative Law Judge (“ALJ”) at the NLRB recently found that the employer unlawfully terminated five employees after they criticized staffing levels and other working conditions on Facebook. In advance of a meeting with management about working conditions, an employee posted to her Facebook page a co-worker’s allegation that employees “do not do enough” to help the organization’s clients. This post generated multiple responses from other employees — some defending the employer and their job performance, others criticizing working conditions.

The employer discharged the participating employees, claiming that their comments constituted harassment of the employee originally mentioned in the post. The ALJ ruled that the employee’s activity, even if acting alone at first, became “concerted” when other employees joined in the discussion, and it was “protected” because it dealt with the employees’ terms and conditions of employment, such as staffing levels.¹⁹ He therefore ordered (subject to potential NLRB and court review) the employer to reinstate the employees, and to make them whole for any lost wages and benefits, as well as post a notice of the employer’s viola-

tion for a period of 60 days in the workplace.

2. Electronic Communication Policies

Two major potential pitfalls exist related to the content of employer policies governing employees’ electronic communications. The first is whether the policy is unlawful on its face, *i.e.*, is the policy “overbroad” so that it impinges on employees’ Section 7 rights. The second is, assuming the policy itself is lawful, whether the policy is uniformly applied. While one might question the wisdom of having such a policy at all — and having one is not necessarily required by law (but see *ftnt.* 41) — absent a policy the default position of the NLRB certainly will be that there are no restrictions other than what the law mandates.²⁰

a. Facial Validity Of Policy

A policy that, reasonably interpreted, “chills” employees in the exercise of their Section 7 rights is unlawful on its face. In the Sears Holding case, the NLRB’s Office of the General Counsel (“OGC”) was asked to determine whether an employer’s Social Media Policy could reasonably be construed to “chill” Section 7 activity.²¹ The Social Media Policy contained the following provision:

In order to maintain the Com-

pany's reputation and legal standing, the following subjects may not be discussed by associates in any form of social media:

- Disparagement of company's or competitors' products, services, executive leadership, employees, strategy, and business prospects

The OGC determined that the policy "d[id] not violate Section 8(a)(1) because it c[ould] not reasonably be interpreted in a way that would chill Section 7 activity." The OGC looked at the policy as a whole, and not just at the language identified above in isolation; it also noted that there was no evidence that the policy was implemented in response to protected activity, or that it has been utilized to discipline Section 7 activity.

Conversely, the American Medical Response policy was alleged to be facially invalid, or overbroad. There, the policy barred employees from making disparaging remarks when discussing the company or supervisors and prohibited employees from depicting the company in any way over the Internet without company permission.

Employers should be aware that the NLRB has held that employees do not possess an inherent, statutory right to use employer's e-mail system for Section 7 purposes. "The [Em-

ployer's] communications system, including its e-mail system, is the [Employer's] property, and was purchased by the [Employer] for use in operating its business."²² Thus an employer policy prohibiting employee use of the employer's e-mail system for "non job-related solicitations" is facially valid.²³²⁴

b. Uniform/Discriminatory Enforcement Of Policy

As a practical matter there are two forms of disparate, or discriminatory, treatment, and both are to be avoided. One is treating similar types of conduct differently in a policy. This will cause the policy to be unlawful on its face. Examples include a policy stating that employees may use e-mail to solicit for one union but not another, or which permitted solicitation by anti-union employees but not by pro-union employees.²⁵

The second form of disparate or discriminatory treatment occurs when, even though a policy is facially lawful, similarly situated employees are treated differently. For example, a policy that bars employees from personal Internet use on the employer's computer is lawful on its face. But if the employer then lets John Doe use it for one personal e-mail, and Sally Moe for another personal e-mail, but refuses to let Frank Coe use it to e-mail a union

organizer, then Frank Coe may have a claim of disparate or discriminatory treatment that has nothing to do with the language of the policy.²⁶

In Register Guard, the policy at issue prohibited e-mail use for "non-job-related solicitations." The Company disciplined an employee for sending two e-mails to coworkers at their work e-mail addresses; one asked employees to wear green to support the Union's contract negotiations; the other asked employees to help with the Union's participation in an upcoming town parade. The employee was also disciplined for a third e-mail, which corrected a misstatement circulated by another employee regarding a Union rally that had taken place a few days earlier. The discipline was based on improper use of the employer's e-mail system for "union business."²⁷

The NLRB found that the Company's policy itself was lawful in prohibiting employees from using the Respondent's e-mail system for any "non-job-related solicitations." Ultimately, after remand from the Court of Appeals,²⁸ the NLRB found that the Company discriminatorily enforced its policy by disciplining the employee for sending all three e-mails, since the Company's policy did not make any distinction between types of

organizations, and there was no evidence that any other employee had ever been disciplined for violating the policy.²⁹

The teaching here, as it is in the Title VII context of employment discrimination, is that the effectiveness of even a facially neutral or lawful policy can be undermined by differing treatment of similarly situated employees for alleged policy violations. Unless there is a legitimate non-discriminatory reason for such differing treatment, the assumption will be that discriminatory animus was the motivating factor in the discipline.

3. Unlawful Surveillance

An employer's actions monitoring employee use of social media could give rise to a claim of unlawful employer surveillance (or even just the "impression" of surveillance) of employees to the extent that such monitoring provided the employer with information as to activities of a union, the views of employees with respect to union membership, or to the employees' terms and conditions of employment.

As the General Counsel wrote in Buel, Inc.,³⁰ where the claim was an employer simply viewing a Facebook page constituted surveillance, even though the employee had "friended" the supervisor:

Employer surveillance or creation of an impression of surveillance constitutes unlawful interference with Section 7 rights because employees should feel free to participate in protected activity "without the fear that members of management are peering over their shoulders[.]" An employer creates an impression of surveillance when "the employee would reasonably assume from the [employer's] statement that their [sic] union activities had been placed under surveillance.

The General Counsel found that the employee's activity was not protected or concerted, and thus there was no improper surveillance. The General Counsel also noted that where the employee had "friended" the supervisor, there could be no surveillance: "even where employees are engaging in protected activity, there can be no unlawful surveillance if the employer's agent was invited to observe." However, had that activity been protected and concerted, and/or the supervisor not a Facebook "friend," it certainly is possible the result on the surveillance issue would have come out differently.³¹

Similarly, in the MONOC case,³² certain employees provided the employer with Facebook postings made by other employees. In the face of a claim of creating an unlawful impression of surveillance, the General Counsel concluded that:

Here, the Employer did not

actually engage in surveillance; instead it obtained Ehling's Facebook pages and e-mails from other employees without soliciting them Moreover, since Ehling had restricted access to her "friends," she would not reasonably conclude that the Employer was directly monitoring her Facebook page Likewise, the Employer's labor attorney told the Union's attorney that employees had been forwarding Ehling's e-mails to managers. In these circumstances, the employees could not reasonably believe that the Employer itself was monitoring these communications. Accordingly, the Employer did not unlawfully create an impression of surveillance.

4. Disloyal Conduct

Even if employee conduct is protected and concerted and thus protected by the NLRA, some employee conduct is so disloyal that the employee may lose that protection. We caution, however, that these are very narrow situations that usually involve egregious conduct, rather than merely offensive or unpleasant conduct, and that the NLRB rarely agrees with the employer in such cases. For example, in the MONOC case,³³ the General Counsel summarized the law relating to disloyal comments about an employer by employees:

The NLRB has held that an employer's discipline of an employee based on website statements relating to terms or conditions of employment and/or a labor dispute is unlawful. In Valley Hospital Medical Center, the Employer

violated Section 8(a)(1) and (3) by suspending an employee for statements regarding patient staffing levels that disparaged the level of patient care because those statements related to terms and conditions of employment and a labor dispute and therefore were protected. The NLRB determined that the statements at issue were not “so disloyal, reckless, or maliciously untrue” as to lose protection; they were intended to pressure the Employer to increase staffing rather than to harm the Employer. Similarly, in Endicott Interconnect Technologies, Inc., the Employer violated Section (8)(1) by discharging an employee who criticized the Employer’s new owner in the press for layoffs that left “gaping holes” and stated on a public website that the company was “being tanked by a group of people that have no good ability to manage it.” The NLRB found the “requisite nexus” between the statements and ongoing labor disputes and determined that the statements were “not so egregious” as to lose the Act’s protection. (citations omitted)

On the other hand, the Endicott Interconnect case cited by the General Counsel was reversed by a federal court.³⁴ In that case, after the employer purchased a computer circuit board manufacturing facility, it permanently laid off 10% of the workforce. An employee posted the following message on a newspaper bulletin board in response to an anti-union message posted by someone else:

To Mr. House: Why do you continue to try to bundle reasons why a union is suspect and not so desirable for EIT

employees? Why do you site [sic] all the bad things about Unions, and ignore all the bad things that IBM and EIT have done to the employees and their families and the community at large? Isn’t it about time you seriously thought about the fact that no one else will help to stop the job losses, and root for the workers of the community instead of defending the likes of Bill Maines, George Pataki, and Tom Libous? Hasn’t there been enough divisiveness among the people working in this area? Isn’t it about time we stood up for our jobs, our homes, our families and our way of life here? Do you want to sit by and watch this area go to hell and dissolve into a welfare town for people over 70? This business is being tanked by a group of people that have no good ability to manage it. They will put it into the dirt just like the companies of the past that were “saved” by Tom Libous and George Pataki, i.e., “Telespectrum”, “IFT (Flex)”. When are you going to get it??? A union is not just a protection for the employees. It’s an organization that collectively fights for improvements and benefits for working people in communities like ours. Forget Jimmy Hoffa and the mob. Those people and situations are stereotypes of fools who chose to undermine the very system they vowed to protect. They are the minority and always have been. Look around. Do you think the government will help you when you lose your job and your house? Think again. A union is the beginning of a community standing up for itself. It’s [sic] time is now.

The employee was terminated. The NLRB found that the employee’s statements constituted “concerted activities” protected by the NLRA because the comments were

related to a “labor dispute.” The Court vacated the NLRB’s order and criticized it for ignoring the fact that the communications were unquestionably detrimentally disloyal at a period when the employer was struggling to get up and running under new management. Therefore, ruled the Court, there was no violation of the NLRA by discharging the employee for cause based on detrimental disloyalty.

Nevertheless, the practical reality is that in the Section 7 context, an employer is expected to have a thick skin and to tolerate a certain level of vitriol from employees. The cases are few and far between in which the NLRB has ruled in favor of an employer claiming that some statement or other made by an employee was disloyal enough to lose the protection of the NLRA.

E. Attorney-Client Privilege

There also are a number of cases dealing with whether or not an employer can use, in defending itself against a lawsuit by an employee or former employee, e-mails between the employee and the employee’s attorney either found on the employer’s e-mail system, or tracked to a personal e-mail account (Yahoo, Gmail, etc.) of the employee and accessed through the employer’s

Electronic Communications In The Social Media Age: What Is An Employer To Do — Or Not To Do?

computers. Since attorney-client privilege is a state law issue (rather than being governed by federal law), the results in these cases can vary, but there do appear to be some commonalities that can be briefly summarized.

1. Use Of Company E-mail

As a general rule, exemplified by the Holmes³⁵ case, there is no expectation of privacy even in an employee's e-mail communications with her attorney using the employer's e-mail system if there is a clear policy stating that the employer monitors its e-mail system and that an employee has no right of privacy as to messages created and received on company computers. In Holmes, the employee used her work computer and work e-mail account to send e-mails to her private attorney discussing her view that she was working in a hostile work environment.

The California Court of Appeals found that the e-mail messages did not constitute "confidential communications between client and lawyer" because the employee was aware of the company policy regarding personal use, which stated that the company monitored its computers and that employees had no right of privacy as to messages created on company

computers. The Court distinguished other cases where the employee had used a personal, password-protected e-mail account to send communications to an attorney.

On the other hand, there are cases such as Fiber Materials,³⁶ a Maine case in which the court majority, in dicta, criticized an employer's in-house attorney for reviewing a privileged memorandum found on a company laptop used by its former president. Notably, the concurring opinion took the opposite view on this issue, finding that the employee "accepted the risk" and was "fully cognizant of employer's policy providing for no expectation of privacy".

2. Use Of Company System To Access Personal E-mail Account

The cases appear uniformly to hold that an employee who uses her employer's computer system to access her own personal private e-mail account, and then uses that account to communicate with her attorney during work hours, has not waived her attorney-client privilege and thus the employer, assuming it can track those e-mails, cannot use them in defending itself.

In the Evans case from Massachusetts,³⁷ for example, prior to leaving his employment, Evans conferred with his private

attorney about his departure. Many of these attorney-client communications were conducted by e-mail, with Evans sending and receiving e-mails from his personal, password-protected Yahoo e-mail account, rather than his employee e-mail account, though he often used his employer-issued laptop to make these communications. After Evans departed, the employer sought court permission to review these e-mails, arguing that Evans' use of its laptop was governed by its policy providing that e-mails on the network, and websites visited by employees could be reviewed by the employer.

The court denied the employer's motion to compel production of the Yahoo e-mails, stating that:

if an employer wishes to read an employee's attorney-client communications unintentionally stored in a temporary file on a company-owned computer that were made via a private, password-protected e-mail account accessed through the Internet, not the company's Intranet, the employer must plainly communicate to the employee that: (1) all such e-mails are stored on the hard disk of the company's computer in a "screen shot" temporary file; and (2) the company expressly reserves the right to retrieve those temporary files and read them.

The New Jersey Supreme Court, on very similar facts, went even further.³⁸ There an employee used her company-

issued laptop to exchange e-mails regarding her allegedly hostile work environment with her attorney. The e-mails were sent through her personal, password-protected Yahoo e-mail account. The employee later filed a discrimination lawsuit against the employer. A forensic expert retrieved the e-mails.

Relying on Evans, the New Jersey Supreme Court found that the employee could reasonably expect that e-mail communications with her lawyer through her personal, password-protected, web-based e-mail account would remain private, and that sending and receiving them using a company laptop did not eliminate the attorney-client privilege that protected them. The court made two additional points that are important to employers:

- The court stated that even a more clearly written policy regarding monitoring of e-mails would not be enforceable. Simply put, such a policy would not overcome an employee's expectation of privacy concerning attorney/client communications.
- The court also suggested that an employer could not discipline employees for spending time at work re-

ceiving confidential legal advice from a private lawyer, although the Court noted that an employee who "spends long stretches of the workday" doing so may be disciplined.³⁹

F. Employer's Duty To Monitor Internet Use

It cannot be gainsaid that an employer has a right to monitor its computer system and employees' Internet use, at least with an appropriate policy in place. But does an employer have an obligation to do so?

In a New Jersey case of which employers should be aware, Doe v. XYZ,⁴⁰ an employee used his work computer to send nude pictures of his stepdaughter to a child pornography site on several occasions. The employer's IT department learned of this activity and reported it to senior management. The only action the employer took was to once tell the employee to stop. The employee's wife then sued the employer on behalf of her daughter, asserting that the employer, once it learned of the employee's activity, had a duty to act by firing the employee and/or reporting his activities to law enforcement. The court agreed, ruling that an employer may face civil liability where the employer has knowledge of an

employee's unauthorized computer use and a third party is harmed as a result.

II. DISCUSSION

So what does this all mean? Obviously we cannot address every conceivable fact pattern. But we can suggest some general rules, with consideration given to the sometimes-inconsistent decisions of the NLRB and courts.

It means that an employer should have a policy governing both computer use at work, and use of social media outside of work. It means that such policies have to be extremely carefully drafted to achieve the following objectives consistent with the potentially dizzying array of federal and state statutes that may apply:

- to protect as much as legally possible the employer's — and the employer's product's — image and reputation, and prevent disloyal or disparaging conduct;
- to eliminate any claim by an employee or former employee that he or she had a reasonable expectation of privacy in the employer's e-mail and computer system;
- to be facially valid under the National Labor Relations Act;

Electronic Communications In The Social Media Age: What Is An Employer To Do — Or Not To Do?

- to be clear to employees about what is and is not permitted use of the employer's e-mail and computer system;⁴¹
- to be clear to employees that the employer's e-mail and computer system belong to the employer, and will be constantly monitored by the employer;
- to prohibit online harassment of employees (or third parties) by other employees;
- to make clear the consequences of violations, including that employees themselves could be legally liable for misconduct directed at others;
- to comply with applicable state laws.⁴²

Employers should also consider adding certain general language to any policy. A general statement in a policy along the lines of "Nothing in this policy should be construed to interfere with employee rights under [the National Labor Relations Act] or [federal law]," can certainly mute any allegation that a reasonable employee reading the policy could conclude that it "chilled" his or her right to engage in protected concerted activity under Section 7 of the NLRA. Another helpful general statement is "In

the event of a conflict between the policy and any applicable law, the applicable law will govern." These types of statements could be effective in warding off charges that a policy is overbroad or may have a "chilling" effect.

However, such language will not help in a situation where discriminatory treatment on the basis of union activity is alleged. Thus management should take pains to ensure that any policy is uniformly enforced. The cases are legion in which alleged disparate treatment of one employee or another under a lawful policy triggered a NLRA or employment discrimination claim of some sort. If an employer is going to adopt a policy, it should be interpreted and applied even-handedly and according to its terms.

In that vein, specific instances of alleged violations must be carefully reviewed, particularly when the issue revolves around postings on a social networking site such as Facebook, which is inherently communal and thus creates potential NLRA issues even if the policy is lawful and has been violated. An independent judgment should be made as to whether or not the employee activity at issue constitutes protected concerted activity, or violates any other law, such as state invasion of privacy laws, before any action is

taken. The worst thing to do is to react in a knee-jerk manner simply because something is displeasing. The reality is, right or wrong, that in the social media environment, employers have to tolerate some degree of quasi-public grief from their employees, but this is no worse than it has been for years with respect to employees who, for example, write an unpleasant letter to the editor of a local paper; the same analysis generally applies.

Other precautionary recommendations may include, for example, telling employees who are promoted into management or into a supervisory position that they no longer can remain "friends" with employees on Facebook or other social networking sites because of the danger of perceived surveillance of employees. Employers should not try to access a private social network site, or employees' personal e-mail accounts, by devious means, such as misrepresenting itself online, or by soliciting employee passwords and user identification numbers to use for itself, or by using a forensic expert to "crack" a password. Such conduct may be unlawful in and of itself and, lawful or not, certainly will forfeit the trust and confidence of employees.

Employers also should be careful about contracting with

IT contractors or forensic investigators, since whatever they do is likely to be imputed to the employer; hence there should be provisions in any such contracting agreements that the contractor is familiar with and will comply with applicable laws, and defend and indemnify the employer from any liability for the contractor's misdeeds.

Finally, it is imperative that these types of social media/electronic communications policies be continually reviewed with counsel in light of the constantly evolving legal landscape. This is particularly important for employers with sites in multiple states who may be subject to varying state laws.

CONCLUSION

Just a few years ago, what employees did out of work, unless it involved egregious or criminal activity, generally was not much of a concern to employers, in part because there was no easy way to find out about it. Now everything some employees think or say or feel is on the Internet for the whole world to see, including your customers, clients, suppliers, and vendors, not to mention other employees and regulatory agencies. Attempts to control this situation must be leavened with common sense and consistent with applicable laws.

While there is a dizzying ar-

ray of potential concerns discussed above, in its essence the appropriate employer response should be what it always has been: a clear, concise, lawful and understandable policy about which no mistake can be made, coupled with active uniform enforcement by the employer. This is easier said than done, of course, but the same can be said of most attendance or disciplinary policies. Computers and the Internet are here for the foreseeable future and they, and employees who use them, have to be managed. In the end it is the quality of management that will carry the day, not what a policy says or does not say.

NOTES:

¹Source information drawn from the named websites and from the YouTube video "Social Media Revolution 2 (Refresh)" available at: <http://www.youtube.com/watch?v=IFZ0z5Fm-Ng>.

²We also note that state law should be consulted before making employee policy or discipline decisions. Many states, for example, have statutes prohibiting invasions of privacy. Many states also have more restrictive laws regarding electronic communications than the federal laws discussed in this article. And many states have whistleblower statutes of one sort or another, so any social media policy should not prohibit what the law would consider to be a legitimate whistleblowing activity. We also do not address issues unique to public sector employees, such as 1st Amendment free speech issues.

³18 U.S.C.A. §§ 2510-22, 2701-11.

⁴See, e.g., Fraser v. Nationwide Mut. Ins. Co., 135 F.3d 107 (3d Cir.

2004) (finding no violation of SCA where defendant insurance company retrieved from digital storage an e-mail plaintiff had sent, and which had been received by its intended recipient).

⁵See, e.g., Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879-80 (9th Cir. 2002); Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 925-26 (W.D. Wis. 2002).

⁶See Van Alstyne v. Elec. Scriptorium, Ltd., 560 F.3d 199, 209 (4th Cir. 2009); Brahmana v. Lembo, 2009 WL 1424438, at *1, *3 (N.D. Cal. 2009).

⁷Pietrylo v. Hillstone Rest. Group d/b/a Houston's, 2009 WL 3128420, at *6 (D.N.J. 2009):

⁸18 U.S.C.A. § 1030.

⁹18 U.S.C.A. § 1030(a)(4).

¹⁰18 U.S.C.A. § 1030(a)(5)(A)(i).

¹¹47 U.S.C.A. § 230.

¹²29 U.S.C.A. § 151 et seq.

¹³For example, this August the NLRB published a Final Rule requiring virtually all private sector employers to post an 11"x17" summary of employee rights under the NLRA by November 14, 2011. 76 Fed. Reg. 54006 to 54050 (August 30, 2011).

¹⁴While beyond the scope of this article, for employers who do have employees represented by one or more unions, we point out that the types of policies discussed herein generally are mandatory subjects of bargaining under the NLRA. Thus the initial promulgation of such policies, or changes to existing policies, may trigger a bargaining obligation prior to implementation under the NLRA.

¹⁵29 U.S.C.A. § 157.

¹⁶Note that under federal and state civil rights anti-retaliation laws, statements critical of the employer may also be protected "opposition" if they relate to allegedly unlawful employment practices.

¹⁷See American Medical Response of Connecticut, Inc., No. 29-CA-12576 (Oct. 27, 2010).

¹⁸Hispanics United of Buffalo, 2011 NLRB LEXIS 503 (Sept. 9, 2011).

¹⁹See also, e.g., Advice Memorandum, Buel, Inc., No. 11-CA-22936 (July 28, 2011) where the NLRB found no evidence of concerted activity: "The Charging Party did not discuss his

Electronic Communications In The Social Media Age: What Is An Employer To Do — Or Not To Do?

Facebook posts with any of his fellow employees, and none of his coworkers responded to his complaints about work-related matters. Although he had discussed the fact that the on-call dispatcher was not reachable with other drivers, there is insufficient evidence that his Facebook activity was a continuation of any collective concerns. Moreover, the Charging Party plainly was not seeking to induce or prepare for group action. Instead, he was simply expressing his own frustration and boredom while stranded by the weather, by griping about his inability to reach the on-call dispatcher.”)

²⁰If for no other reason, it is important to have a policy to defeat employee claims that they have a reasonable expectation of privacy in their work computers and e-mails.

²¹Advice Memorandum, Sears Holdings (Roebucks), No. 18-CA-19081 (Dec. 4, 2009).

²²Guard Publishing Co., 351 NLRB 1110, 1114 (2007), *enf. granted in part, denied in part* 571 F.3d 53 (2009).

²³*Id.*

²⁴Employers should be aware that NLRB law can change frequently depending on its makeup and that there can be a lack of consistency between regimes, or even between Regions, of which there are 37, each one run by a Regional Director with the independent authority to investigate charges of unfair labor practices and issue complaints. Thus it is sometimes difficult to divine consistency from NLRB decisions and General Counsel opinions, a phenomenon which tends to militate toward a conservative approach.

²⁵See note 22. In Register Guard, the NLRB adopted a new test that “unlawful discrimination consists of disparate treatment of activities or communications of a similar character because of their union or other Section 7-protected status.” That is, “an employer may draw a line between charitable solicitations and non-charitable

solicitations, between solicitations of a personal nature (e.g., a car for sale) and solicitations for the commercial sale of a product (e.g., Avon products), between invitations for an organization and invitations of a personal nature, between solicitations and mere talk, and between business-related use and non-business-related use.”

²⁶See, e.g. Guardian Indus. Corp. v. NLRB, 49 F.3d 317, 319 (7th Cir. 1995) (“A person making a claim of discrimination must identify another case that has been treated differently and explain why that case is the same in the respects the law deems relevant or permissible as grounds of action.” (internal quotation marks omitted)).

²⁷351 NLRB at 1118. See note 25.

²⁸571 F.3d 53 (2009).

²⁹Register Guard, 357 NLRB No. 27 (2011).

³⁰*Supra.* n. 19.

³¹See also Frontier Telephone of Rochester, Inc., 344 NLRB 1270, 1275–76 (2005), *enforced* 181 F.App’x 85 (2d Cir. 2006) (employer did not unlawfully create impression of surveillance where supervisor mentioned posting on union website that was forwarded to him by an employee, where employees should reasonably have assumed that their postings were subject to public dissemination by another website subscriber).

³²Advice Memorandum, MONOC, Case Nos. 22-CA-29008, 22-CA-29083, 22-CA-29084, 22-CA-29234 (May 5, 2010).

³³*Id.*

³⁴453 F.3d 532 (D.C. Cir. 2006).

³⁵Holmes v. Petrovich Development Co., LLC, 191 Cal. App. 4th 119 (3 Dist. 2011).

³⁶Fiber Materials, Inc. v. Subilia, 974 A.2d 918, 928 (Me. 2009).

³⁷National Economic Research Associates, Inc. v. Evans, 21 Mass. L. Rptr. 337 (Mass. Superior 2006).

³⁸Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010).

³⁹See also, e.g., Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) (Court prohibited employer from using in litigation e-mails that former employee sent to his private attorney via a personal, web-based account using his company-owned computer).

⁴⁰Doe v. XYZ Corp., 887 A.2d 1156 (N.J. Super.Ct. App.Div. 2005).

⁴¹Some prohibitions are just obviously appropriate, or should be, such as surfing pornography and/or child pornography sites, engaging in criminal behavior, disclosing trade secrets or patent information, harassment or stalking, conducting a personal business, competing with the employer, industrial espionage, etc. See, e.g., Martin Luther Memorial Home, 343 NLRB 646 (2004) (“the judge concluded that the Respondent’s rules prohibiting ‘abusive and profane language,’ ‘harassment,’ and ‘verbal, mental and physical abuse’ were lawful because they were intended to maintain order in the employer’s workplace and did not explicitly or implicitly prohibit Section 7 activity. We agree with the judge’s conclusion.”).

⁴²Again, for example, some states, such as Connecticut, may have statutes requiring prior written notice of the types of electronic monitoring that the employer may conduct, see, e.g., Conn. Gen. Stat. § 31-48d, so the types of monitoring that will be conducted should be in the policy, and posted if state law requires a posting. Other states, such as California, prohibit employers from disciplining employees for off-duty conduct, although this type of statute may be preempted by the NLRA. E.g., Cal. Lab. Code § 96(k) (barring employers from demoting, suspending or discharging employees “for lawful conduct occurring during nonworking hours away from the employer’s premises”).