So what is going on out there?

Employees are using social media, both at work and at home, to publish a stunning amount of information online. Email, internet web sites, social networking sites like Facebook and MySpace, Twitter, texts, blogs, video posts on YouTube and Flickr: the speed and ease with which words, photos and other graphic images are being electronically transmitted and widely disseminated on these platforms have greatly increased the concerns of employers regarding social media use and the workplace risks posed to employees. These perils are further magnified by the fact that we “live our lives in a world where the Internet records everything and forgets nothing – where every online photo, status update, Twitter post and blog entry by and about us can be stored forever.” “The Web Means the End of Forgetting.” Jeffrey Rosen, *The New York Times* (October 12, 2010).

Rampant social media use has blurred many time-honored distinctions that have long defined workplace rights, responsibilities and expectations: principles like work time versus break time, workplace activity versus private, off-duty conduct, uniquely private information versus information which an employer can appropriately use to make employment decisions.

**Here are some eye-popping statistics about electronic communications and the workplace:**

**EMAIL USE**

42% of full time employees in the workplace “frequently use” a company email account for personal communications; 29% sometimes do.

89% of workers have sent email from work to an outside party which contained jokes, gossip, rumors or disparaging remarks; 14% sent messages containing confidential or proprietary information; 9% sent sexual, romantic or pornographic images or text.
80% of organizations have written email policies, but only 47% train their workers on email risks, policies and usage.

28% of employers have fired employees for email misuse including violations of company policy (64%), inappropriate language or materials (62%), excessive personal use (26%) and breach of confidentiality rules (22%).

EMAIL MONITORING

43% of employers actively monitor employee email. Of those employers, 73% use technology to automatically monitor email, and 40% assign a manager to manually read and review email. 71% alert employees to such monitoring.

INTERNET USE

30% of employers have fired someone for misusing the Internet: viewing, downloading, or uploading inappropriate material (84%), violations of policy (48%), excessive personal use (34%).

COMPUTER and INTERNET MONITORING

66% of employers monitor employee websites visits on company computers.

43% of employers store and review employee computer files.

45% track content, keystrokes and time spent at employee keyboards.

12% monitor internet blogs to see what is being written about the company.

10% actively monitor social websites such as Facebook and MySpace for employee posts and photographs.

2010 workplace privacy study, Ponemon Institute;
2009 Electronic Business Communications Policy & Procedures Survey, American Management Association and ePolicy Institute;

This paper briefly surveys the legal landscape where social media intersects with the workplace – employer regulation of employee activity on email and social media platforms, employer monitoring and surveillance, privacy issues under federal and state law and statutes, and developing reasonable social media policies (through collective bargaining and otherwise).
I. THE NLRA: EMPLOYEE USE AND EMPLOYER REGULATION AND MONITORING OF EMAIL AND SOCIAL MEDIA.

Section 7 of the National Labor Relations Act grants employees the statutory right to engage in concerted protected activity for their mutual aid and protection. Section 7 protections extend to certain employee use of email and social media to discuss with coworkers their mutual workplace issues and their terms and conditions of employment. Because Section 7 rights are available to employees in union and nonunion workplaces alike, NLRA issues may loom large as employers increasingly seek to regulate employee use of email and social media both at work and at home.

1. Section 7 right of access to employer email.

Email has become the primary means of communication in many workplaces, with employees using email systems accessed on company computers, smart phones, and other handheld devices to do their daily jobs. Does the routine use of email in the workplace give rise to any statutory protections on the part of employees to use company email or company equipment to discuss workplace concerns?

Not for the time being. But stay tuned.

In Guard Publishing Co. d/b/a The Register-Guard, 351 NLRB 1110 (2007)[“Register Guard I], review granted and remanded on other grounds, Guard Publishing Company v. NLRB, 571 F. 3d 53 (D.C. Cir. 2009), a sharply divided NLRB held that employees do not have a Section 7 right of access to employer email systems to communicate regarding workplace concerns. With two members dissenting, the Board upheld the “basic property right” of employers to control their computer equipment, and thus to bar any non-business use of employer email systems.

Will the current or future NLRB reexamine this holding? As recently departed Board Chair Wilma Liebman said in her dissent in Register Guard I: “National labor policy must be responsive to the enormous technological changes that are taking place in our society. Where, as here, an employer has given employees access to e-mail for regular, routine use in their work, we would find that banning all nonwork-related email ‘solicitations’ is presumptively unlawful absent special circumstances.” 351 NLRB at 1121.

Moreover, the General Counsel of the NRLB has recently instructed Regional Directors to send to the Division of Advice all cases involving “whether employees have a Section 7 right to use an employer’s email system....” GC Mem. 11-11 (April 12, 2011). Whether this portends a Board reexamination of the holding in Register Guard I as to Section 7 right of access to employer email remains to be seen.
2. The discriminatory enforcement of workplace communications policies.

Section 7 of the NLRA governs employer enforcement of its employee communications policies in both union and nonunion settings. Where an employer permits reasonable personal use of email at the workplace, can the employer nonetheless prohibit employees from discussing by email their union organizing activity, or their concerns regarding compensation, working conditions or other terms of employment? Or would that treatment constitute unlawful discrimination in violation of Section 7?

In Register Guard I, a sharply divided NLRB sought to fashion a new and vastly narrowed discrimination standard to govern employer enforcement of solicitation policies, including email and internet use policies. The Board held that unlawful discrimination for purposes of Section 7 was limited to disparate treatment involving communications of a “similar character.” In other words, an employer could lawfully discipline an employee for sending union-related email (involving an organization) even if it permitted other non-business and personal use of email, so long as the prohibition ran against solicitations to all groups and organizations. On that ground, the Register Guard I Board upheld the discipline of an employee for sending various union-related emails to coworkers, even though the employer had long tolerated a wide spectrum of personal email use amongst her coworkers.

But the discrimination test fashioned in Register Guard I – which veered sharply from longstanding NLRB precedent – did not withstand appellate scrutiny. In Guard Publishing, supra, 571 F. 3d 53, the D.C. Circuit rejected Register Guard I's newly fashioned discrimination standard, calling the Board’s attempted distinctions between personal and organizational solicitations a “post hoc rationalization”—especially given that neither the Employer’s communications policy nor its past enforcement made such distinctions. On remand, Guard Publishing Co. d/b/a The Register Guard, 357 NLRB No. 27 (2011) [Register Guard II], the Board simply accepted the appellate court’s ruling as the law of the case, finding unlawful the employer's assessment of employee discipline for union-related email use, given the widespread personal use that was otherwise tolerated at the workplace.

Although the Register Guard II Board declined to generally discuss the discrimination standard which governs employer enforcement of social media policies, it is safe to say this: where an employer tolerates personal email use and social media use at work, an employer runs a substantial legal risk in singling out union-related communications, or
other communications discussing workplace grievances or concerns, as proper grounds for discipline.¹

3. **Concerted, protected activity online.**

**Employees are increasingly taking their concerns about the workplace online.**

The internet provides a very effective and ready means for employees to communicate with coworkers about labor disputes and other workplace concerns. The NLRB has long recognized that Section 7's protection of “concerted, protected activity” governs email communications, just like any other means of communication. Thus in *Timekeeping Systems Inc.*, 323 NLRB 244 (1997), the Board found that an email to coworkers criticizing the employer’s proposed changes to its vacation policy constituted concerted protected activity under the Act. But see *Amcast Automotive of Indiana, Inc.*, 348 NLRB No. 47 (2006)(internet research conducted by two employees at work regarding potential buyer of employer company, although “concerted,” was found not to be “protected” because it was not sufficiently related to working conditions.); *Washington Adventist Hospital*, 291 NLRB 95 (1988) (Board upheld discharge of employee who sent a system wide computer message complaining about management and impending layoffs, where message disrupted work of more than 100 computer terminal users, and violated a computer security agreement that the employee had signed).

**Social Media Use May Constituted Concerted, Protected Activity. And Social Media Policies May Unlawfully Chill the Exercise of Statutory Rights.**

But what of Facebook or blog posts which are communicated not solely to coworkers, but to a larger internet audience? The Supreme Court has long recognized that the NLRA protects public communications regarding workplace issues “through channels outside the immediate employer-employee relationship.” *Eastex, Inc. v. NLRB*, 437 U.S. 556, 565 (1978).

While an employee's communication of his workplace concerns to a vast internet audience should not render it statutorily unprotected, it will almost certainly heighten the severity of an employer’s response. Employers often seek to shut down employee discussion of workplace issues or personnel matters on social media – and to discipline, or threaten discipline for doing so – on grounds that the employee has improperly disclosed “private” or internal personnel matters, or has “disparaged” the employer's reputation online.

¹ NRLB Regional Directors have also been instructed to send to the Division of Advice all cases “that require application of the discrimination standard enunciated in” *Register Guard I*. GC Mem. 11-11 (April 12, 2011).
Indeed, many employers have issued social media policies that sharply restrict the online communications rights of their employees – both at work and off hours – and warn of the disciplinary consequences of violating these policies. Employers justify these restrictions by reference to the inherent and magnified risks posed to the company and its corporate brand, by online publication. Among the more common provisions in social media policies are bans on:

- disparagement of the company, coworkers or clients;
- discussion of internal procedures, personnel matters, and workplace issues;
- discussion of wages and other terms and conditions of employment;
- depiction of the employer, the workplace, or the corporate logo, in a negative way, or in any way, without employer consent.

But are these policies, and the discipline issued pursuant to them, legal under the NLRA?

The dissemination of specific workplace concerns to a vast internet audience, for purposes of mutual aid and protection, does not undermine the protected, concerted nature of any particular communication. As long as the employee is acting “with or on the authority of other employees, and not solely by or on behalf of the employee himself,” a social media post should be protected. See Meyers Industries (Meyers I), 268 NLRB 493 (1984), rev’d sub nom, Prill v. NLRB, 755 F.2d 941 (D.C. Cir. 1985), cert. denied, 474 U.S. 948 (1985), on remand, Meyers Industries (Meyers II), 281 NLRB 882 (1986), aff’d sub nom, Prill v. NLRB, 835 F.2d 1481 (D.C. Cir. 1987), cert. denied 487 U.S. 1205 (1988). In other words, where an online post relates to working conditions, and either stems from a mutually held employee concern, or seeks to involve other employees in the issue, that post should be found concerted and protected under Section 7.

Thus, in Bay Sys Technologies, LLC, 357 NLRB No. 28 (August 2, 2011), the Board granted a motion for default judgment against an employer, finding a violation based on threats and discipline against employees who complained to one another on Facebook about the employer's failure to issue timely paychecks. And in Salon/Spa at Boro, Inc., 356 NLRB No. 69 (2010), the Board affirmed an ALJ decision involving an employer’s alleged threats of employee reprisals for discussing working conditions with coworkers on Facebook. The ALJ did not question that the social media posts themselves were concerted, protected activity, but otherwise found no violation on grounds that the employer’s comments to employees – about the “public” nature of the internet and the need to exercise judgment and restraint – were “educational and almost parental in nature” and thus not coercive under the Act. Thus, although the NLRB has not squarely
considered the issue, it appears to be a given that employee communications on social media platforms can implicate concerted, protected activity.\(^2\)

Where a restrictive social media policy is enforced to prohibit an employees' Section 7 communications on social media, not only will the discipline be found unlawful, but the policy itself will likely be struck down as well. See University Medical Center, 335 NLRB 1318, 1320-22 (2001), enf'd. denied in pertinent part, 335 F.3d 1079 (D.C. Cir. 2003).

Even where a restrictive social media policy is not used as grounds for discipline, the mere maintenance of that policy may run afoul of the NLRA. If employees reasonably construe the restrictive language of a social networking policy, when viewed in its context, to prohibit Section 7 activity, it will be found unlawful. Lutheran Heritage Village – Livonia, 343 NLRB 646 (2004).

So for example, a social media policy that expressly prohibits employees from discussing their wages or working conditions on Facebook and Twitter will certainly be found to violate Section 7 rights. So too for a policy that flatly prohibits employees from mentioning the Company or its personnel policies on social media sites, or that prohibits the posting of photos depicting the company name or logo. See e.g., Claremont Resort and Spa, 344 NLRB 832, 836 (2005) (workplace policy unlawful where it prohibited “negative conversations” about managers, and gave no further example or clarification).

In a recently published Memorandum, the NLRB General Counsel has surveyed all of the social media cases considered by his Office\(^3\), providing detailed reasoning as to how those cases have been handled. Memorandum OM 11-74, Report of the General Counsel (August 18, 2011) [“GC Mem.11-74”]. In deciding when to issue ULP complaints challenging discipline assessed for Facebook posts or tweets on Twitter, or challenging employer policies that restricts employees' social media communication rights, the General Counsel has been heavily guided by the Meyers and Lutheran Heritage cases discussed above. And, while some employers have been quick to complain that the GC has gone too far in issuing ULP complaints involving social media policies and activity, the case developments in fact are squarely aligned with longstanding Board doctrine.

**GC finds concerted, protected activity:**

---

\(^2\) And of course, the General Counsel of the Board has issued numerous ULP complaints, finding social media activity to constitute concerted, protected activity under the Act. See discussion *infra*.

\(^3\) In April 2011, the Office of General Counsel instructed all NLRB Regional Directors to submit to the Division of Advice any case involving “employer rules prohibiting, or discipline of employees for engaging in, protected concerted activity using social media, such as Facebook or Twitter.” GC Mem.11-11 (April 12, 2011).
Where employees have been disciplined for using social media to discuss mutually held workplace concerns with coworkers, the General Counsel has been vigilant in issuing ULP complaints. In American Medical Response of Connecticut Inc. (AMR), Case No. 34-CA-12576 (Complaint and Notice of Hearing, October 27, 2010), for example, the GC challenged the discharge of an employee who referred to a supervisor in Facebook posts as a “scumbag” and a “17” (company shorthand for a psychiatric patient), where those posts were a means for coworkers to discuss their working conditions. The GC also challenged the employer’s Blogging and Internet Posting Policy which prohibited “disparaging, discriminatory or defamatory comments” about the Company or coworkers and which further prohibited depicting the Company in any way on the Internet without permission. The ULP settlement included revision of the policy to ensure that employees could discuss working conditions with others on social media platforms. (February 7, 2011 NLRB News Release; GC Mem.11-74 at p. 3). See Build.com (April 27, 2011 NLRB News Release) (ULP complaint challenging employee discharge for Facebook posts discussing employer and potential state labor code violations. Settlement included 60 day posting that employees have right to post social media comments about terms and conditions of employment).

And in Hispanics United of Buffalo, Case 3-CA-27872 (May 9, 2011 complaint), the General Counsel challenged the discharge of five employees for criticizing working conditions on Facebook. Although the Employer accused the employees of “cyber-bullying,” the General Counsel termed the Facebook discussion “a textbook example of concerted activity, even though it transpired on a social network platform. The discussion was initiated by the one coworker in an appeal to her coworkers for assistance.” GC Mem.11-74 at p.3. See also Karl Knauz Motors, Case 13-CA-46452 (May 20, 2011 ULP complaint)(termination of BMW salesman for Facebook posts criticizing meager refreshments at promotional sales event, where coworkers had previously complained to management that poor quality of refreshments could negatively impact sales commissions by limiting sales. Case pending) (GC Mem.11-74 at pp.5-8).

**GC finds policies overbroad:**
The General Counsel has also challenged overly broad social media policies that are reasonably construed to prohibit Section 7 communications on social media sites. Among the policy provisions that have been challenged as unlawfully restricting Section 7 activity are those that prohibit social media posts: that restrict the discussion of wages, Healthcare Ventures of Ohio, LLC, Case No. 8-CA-38825 (September 14, 2010 settlement agreement); that: “disregard the rights and reasonable expectations of privacy of any person or entity”; that constitute “embarrassment, harassment or defamation” of the employer; that might damage the reputation and goodwill of the employer; that prohibit the discussion of company business or employees, Qualitest Pharmaceuticals, Case No. 10-CA 38757 (February 23, 2011 complaint); that discuss employer investigations, Healthcare Ventures of Ohio, supra; that “could be construed as
inappropriate”; or that “they would not want their manager or supervisor to see.” See generally GC Mem.11-74 at pp. 18-20.

Given the breadth of these various prohibitions, and the absence of policy limitations or examples of what the restrictions cover, the General Counsel found that the social media policies could be reasonably interpreted as prohibiting employee discussion of wages and working conditions, as well as the posting of photos related thereto. Compare Tradesmen Int'l, 338 NRB 460, 462 (2002)(rule forbidding “slanderous” or “detrimental” statements found lawful, where it was included in a list forbidding “sexual or racial harassment” and “sabotage”); Sears Holdings, No 18-CA-19081 (Gen. Counsel Advice Memo, Dec. 4, 2009) (social media policy lawful, despite ban on disparagement of company products, services, executive leadership, employees, or strategy, where restriction appeared in a list of “plainly egregious conduct” and policy stated that it was not intended to “restrict the flow of useful and appropriate information.” Employees used internet listserve to discuss union organizing campaign, without discipline, even after policy issued).

The General Counsel has squarely acknowledged the central importance of “personal profiles” on social media in tracking down coworkers for purposes of discussing workplace concerns. Thus, the General Counsel has challenged a social media policy that prohibits employees from using their company name, address or other information on their personal profiles. Given the function that the “personal profile page” serves in allowing employees to use social media effectively to find and communicate with coworkers, this prohibition was found to be “particularly harmful to their Section 7 rights.” GC Mem.11-74 at p. 20.

**GC finds no concerted, protected activity:**
But where an employee's Facebook posts are not directed at coworkers, do not address a common concern, and do not reflect an attempt to initiate group action, those social media communications may be unprotected as not constituting “concerted” activity under Section 7. This is true even where the employee posts concern working conditions. Thus, in JT's Porch Saloon and Eatery, Case 13-CA-146689 (Advice Memorandum, July 7, 2011), the General Counsel refused to issue complaint where a bartender was fired for a Facebook post complaining about a Company tipping policy. Although the post addressed working conditions, the tipping policy had not been a collective employee concern, the employee did not discuss his post with coworkers, and did not seek group action. GC Mem.11-74 at pp. 13-14.

And where a retail store employee posted Facebook comments about an “individual gripe” with a manager, but did not seek coworker responses or group action, the General Counsel found the employee's discipline to be lawful. Wal-Mart, Case 17-CA-25030 (Advice Memorandum, July 19, 2011); accord, Rural Metro, Case No. 25-CA-31802 (June 29, 2011) (Employee post on Facebook page of Senator regarding wages and working conditions was not “concerted” where employee did not discuss comments with
coworkers before or after posting them)(GC Mem.11-74 at pp.14-15); Wal-Mart Distribution Center 6018, Case No. 26-CA (June 30, 2011 letter of dismissal of charge; employee post expressing desire that employer’s building would collapse during earthquake not protected as unrelated to working conditions).

And as for social media policies that restrict employee communications, the General Counsel continues to scrutinize the overall factual context in determining overbreadth. Thus, in Sears Holdings, No 18-CA-19081 (GC Advice Memo, Dec. 4, 2009), the General Counsel found no violation where a policy banned online disparagement of company products, services, leadership, employees, or strategy. Because the preamble assured employees that the policy was not intended to “restrict the flow of useful and appropriate information,” and because the restriction was listed amongst descriptions of other “plainly egregious conduct,” employees could not reasonably read the policy as chilling the exercise of Section 7 rights. In so finding, Advice noted that, notwithstanding the policy, employees used internet listserves to openly discuss union organizing activity without discipline.

**Loss of statutory protection:**

Even where coworkers’ social media posts clearly address working conditions or other mutually held workplace concerns, employers may seek to characterize them as unprotected under the Act where the comments are profane or disparaging. But, applying Atlantic Steel Co., 245 NLRB 814, 816-17 (1979), the General Counsel has found that many intemperate or profane posts on Facebook or Twitter are not so “opprobrious” as to lose statutory protection. See Hispanics United of Buffalo, Case 3-CA-27872 (May 9, 2011 complaint) (swearing and sarcasm in Facebook posts found protected where conversations objectively innocuous)(GC Mem.11-74 at pp. 3-4); see also NLRB News Release: Facebook Posts, (April 27, 2011); American Medical Response (employee did not lose statutory protection when Facebook posts called supervisor a “scumbag” or a “17”-- shorthand for a psychiatric patient; posts occurred outside work on nonworking time, and thus did not interrupt productivity; no accompanying verbal or physical threats)(GC Mem.11-74 at pp.4-5).

Allegations of unlawful disloyalty, based on social media posts, may be further governed by Jefferson Standard, NLRB v. IBEW Local 1229, 346 U.S. 464 (1953) and its progeny. As long as disparaging remarks posted on Facebook or Twitter relate to workplace interests or a labor dispute and are not egregious or reckless in nature, they should stand protected, notwithstanding the highly public nature of their online dissemination. See American Golf Corp., 330 NLRB 1238 (2000), petition for review denied, 86 F. Appx. 305 (9th Cir. 2004); Emarco, Inc., 284 NLRB 832 (1987); Arlington Electric, Inc., 332 NLRB 845 (2000); Allstate Insurance Co., 332 NLRB 759 (2000). The General Counsel has, for example, found protected a car salesman’s sarcastic Facebook posts, complaining of the cheap refreshments provided during a sales promotion (“overcooked hot dogs and stale buns”), and his online posting of photos of the snacks, given that the employees had
previously articulated to management their concerns that the meager refreshments would impact sales and commissions. Karl Knauz Motors, Case 13-CA-46452 (May 20, 2011 ULP complaint). The GC found the postings “neither disparaging of the employer's product nor disloyal.” GC Mem.11-74 at p.8.

But the Board and the appellate courts have long tangled on what constitutes unprotected disparagement or disloyalty. E.g. Endicott Interconnect Technologies, Inc. v. NLRB, 453 F. 3d 532 (D.C. Cir. 2006) (refusing to enforce Board order of reinstatement; employee statement to news reporter that layoffs had caused “gaping holes” in the employer’s business constituted “sharp, public and disparaging attack” on the quality of the employer’s product and policies beyond protection of Act); St. Luke’s Episcopal-Presbyterian Hospital v. NLRB, 268 F.3d 575 (8th Cir. 2001). The vast scope of an internet audience might give further fuel to arguments that online disparagement can cause particularly acute harm to an employer, and thus must be even more closely regulated by law.


Increasingly sophisticated technology and computer software now allow employers to monitor not only employee email and internet use at the workplace, but also their personal, off-duty internet posts on social media like Facebook and Twitter. Employers can use the search capacities on such freely available monitoring tools as Google Blog Search or Twitter Search, or can purchase internet monitoring services which track employee activity on social media networks outside the workplace, based on keyword searches. Employers can choose both the keywords and the particular employees to be monitored; when a keyword is used by a tagged employee on the internet, the employer is alerted. 4

And as fast as you can say Google, an employer can quickly scour the internet to obtain a comprehensive report of employee (or job applicant) information and communications on blogs, websites and even social networking sites, all free of charge.

---

Can electronic monitoring of employee activity give rise to claims of unlawful surveillance under the NLRA? Here are the basic principles which will likely guide future development of Board law.⁵

**Open and ordinary observation of union activity on or near work is generally lawful.**

“Although an employer may observe open union activity on or near its property, “[it] may not do something ‘out of the ordinary’ to give employees the impression that it is engaging in surveillance of their protected activities.”

_Sprain Brook Manor Nursing Home, LLC, 351 NLRB No. 75 (2007)._ Conspicuous surveillance of union activity on or near employer premises is generally acceptable, absent a showing that the surveillance interferes with protected activity. See _Basic Salvage & Metal, 322 NLRB 462 (1996)_ (supervisor “watching” employee interaction with union representatives near the employer’s property is not engaged in unlawful surveillance).

**But surveillance, or even the “impression of surveillance” which restrains employees in the exercise of their protected rights is illegal.**

_Golden State Foods Corp., 340 NLRB No. 56 (2003)_ (“eyes are on you and you need to watch your step”); _Alle-Kiski Med. Center, 339 NLRB 361 (2003)_ (illegal videotaping and photographing of union organizers). In general, the Board finds an unlawful impression of surveillance where the employer reveals specific information about union activity that is not generally known, and does not reveal its source. E.g. _Stevens Creek Chrysler Jeep Dodge, 353 NLRB No. 132, slip. op at 3 (2009)_ (manager told employees that “he already know” about a union meeting, and did not reveal that he learned it from another employee).

**So, too, for surveillance in retaliation for union activity.**

_Snap-on Tools, Inc., 342 NLRB No. 2 (2004)_ (employer illegally modified its practice of having security camera scan parking lot, by focusing camera on union handbilling).

**And where employer monitoring is “out of the ordinary” it may be coercive and therefore unlawful.**

---

Carry Cos. of Ill., 311 NLRB 1058 (1993) (presence of supervisor and off duty police officer 2 to 3 feet from union representative distributing literature violates 8(a)(1)).

Thus, conspicuous videotaping and photographing of union activity is unlawful, unless the employer can demonstrate the surveillance serves a legitimate security objective or that it had a reasonable basis to believe misconduct was occurring).


And the installation and use of hidden surveillance cameras in the workplace is a mandatory subject of bargaining, even where the employer wishes to install the cameras to monitor workplace misconduct.


Secret video surveillance “targeting” the leader of a union organizing effort violates the Act.

See Hialeah Hospital, 343 NLRB 391 (2004) (finding independent violations of 8(a)(1) and 8(a)(3) when employer had secretly videotaped leader of organizing campaign).

And revelation of employer knowledge of a union organizing campaign that employees believed to still be secret creates an actionable impression of surveillance.


So what does all of this mean for social media surveillance? There is scant Board precedent on the issue of social media surveillance. For example, in a 2-1 decision, with Member Liebman dissenting, the Battista Board held in Frontier Telephone of Rochester, Inc and CWA, 344 NLRB 1270 (2005), enfd 181 Fed. Appx. 85 (2006), that the employer did not create an unlawful impression of surveillance when a supervisor told an employee that he was aware of a message posted on an employee-created, “subscriber only” webpage during an organizing campaign. The Board held that, even though the supervisor had not informed the employee that the message had been shown to him by a coworker, it was unreasonable for the employee to assume that the message had been discovered through employer surveillance, given that any employee could publicly disseminate a posted message to a non-subscriber.

But in Camaco Lorain Mfg. 356 NLRB No. 143 (2011), the Liebman Board limited Frontier Telephone’s holding of no unlawful coercion to the unique facts of that earlier
The organizing campaign itself was public and generally known to everyone at the workplace, and the employee subscribers to the site had never been told to maintain the secrecy of its contents.

The course of future Board precedent in cases of electronic surveillance is unclear. The Board will likely scrutinize the relative “openness of the Section 7 activity” both at the workplace and on social media sites versus the “out of the ordinary” character of the employer surveillance in question. A blog post about union organizing, easily read by anyone on the internet, may be likened to “open union activity.” But how about more private complaints about working conditions posted on Facebook, intended to be read only by Facebook “friends”? Or email or text messages sent to specific coworkers? Does an employer's mention of a union-related post on one of these more private social media platforms carry an unlawful impression of surveillance? Does it matter that any social media post – even on a limited access site – may be disseminated by a site subscriber or “friend” to a supervisor? Camaco signals that, where the protected employee activity is less widely known, or where more care is taken to maintain the privacy of the social media site, the employer’s revelation of knowledge of “secret” online posts may be coercive and therefore illegal.

And is it inherently coercive for an employer to be conducting ongoing Google internet searches of its employees? Or to be purchasing a commercial monitoring service (e.g. Social Sentry) which will continuously search social media sites for triggering keywords? Can an employer justify such monitoring on grounds that employee posts might disparage company good will or corporate image? Does the fact that the websites are open to the internet-viewing public, or that social networking sites are open to numerous “friends” defeat the argument that employees would be coerced by such systematic monitoring? Does the fact that the electronic surveillance is “recorded” or stored in electronic computer files make it more analogous to illegally coercive taped or photographed surveillance? Does the employer’s “conspicuous” announcement of such internet surveillance make it so?

Much employer surveillance of off-duty social networking can be rightly characterized as inherently coercive, both because of the extraordinary degree of “big brother” creepiness such monitoring would carry and because the communications themselves are conducted

---

6 See Monmouth Ocean Hospital Services Corp d/b/a MONOC, Case 22-CA-29008 (Advice Memorandum, May 5, 2010), at fn. 18 (no impression of surveillance where employer discussed viewing of employee photograph on a “presumably public website.”); compare Magna International, Inc., 2001 WL 1603861 (ALJ Amchan, March 9, 2001)(unlawful impression of surveillance where supervisor made a point of telling employee that he had seen her picture on the internet; conveyed impression that he was monitoring her union activities).

7 See MONOC, supra (no violation where employer did not surveil Facebook and made clear to employee that he had received posts, unsolicited, from coworkers. Because Facebook page was limited to Facebook “friends”, coworkers could not reasonably conclude that the employer was directly monitoring).
in the private time and private life of an employee, and on the “friend-” or subscriber-
limited sites where some expectations of privacy might reasonably prevail. And
certainly, to the extent surveillance is motivated by anti-union animus, or is focused
uniquely on union activity, that surveillance surely will be found illegal under existing
Board principles.

II. FEDERAL REGULATION OF ELECTRONIC MONITORING.

Title I of the Electronic Communications Privacy Act of 1986 [“ECPA”], 18 U.S.C.
Section 2510 et. seq makes it unlawful for an individual to intentionally intercept a “wire,
oral or electronic communication”, which includes telephone conversations and voice
mails, but does not include “electronic storage of any such communication.” The
prohibited intercept must occur contemporaneously with the electronic transmission. See
U.S. v. Steiger, 318 F.3d 1039, 1047-50 (11th Cir. 2003), cert. denied, 538 U.S. 1051
(2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002), cert. denied,

Title II of ECPA, sometimes known as the Stored Communications Act [“SCA”] limits
access to electronically stored information, including computer files.

Although both titles apply to both public and private sector employees, each contains
broad exceptions that greatly limit their protection of employee rights in workplace
communications. For example, each includes a “consent” exception. Consent may be
express or implied. Certainly, a well drafted employer communications policy, reserving
to the employer the right to intercept, monitor or access emails, computer files and other
stored electronic information at the workplace will preclude employer liability under
either title of ECPA. E.g. Shefts v. Petrakis, 758 F.Supp. 2d 620 (C.D. Ill. 2010)
(implied consent to employer interception of text messages sent on employer-provided
Blackberry, given company manual that clearly stated that all communications sent and
received on employer equipment was not private, and was subject to viewing,
downloading and archiving).

Each title of ECPA also includes a “provider” exception which permits a “person or
entity providing a wire or electronic communications service” to intercept or access such
information.

Given these broad exemptions, ECPA has provided little workplace privacy to
employee computers. In Fraser v Nationwide Mutual Insurance, 352 F.3d 107 (3d Cir.
2003), for example, the Third Circuit rejected ECPA claims based on an employer search
of emails sent to and received by an independent insurance agent that were stored in the
company’s main server. The Title I claim was rejected on grounds that the search did not
constitute an unlawful “intercept” because it was not done contemporaneously with the
electronic transmission. The Title II claim was also dismissed based on the “provider” exception in the statute.

And in Bohach v. City of Reno, 932 F.Supp. 1232 (D. Nev. 1996), the court upheld a police department’s retrieval of an employee’s text messages which were stored on the department’s computer system, on grounds that the department was the “provider” of the service and “service providers may do as they wish when it comes to accessing communications in electronic storage.” But see, Adams v. City of Battle Creek, 250 F. 3d 980 (6th Cir. 2001)(reversing summary judgment in favor of defendant police department on ECPA claim where department secretly monitored phone numbers received on employee pager, given suspicions regarding drug trafficking).

But in Pietrylo and Marino v. Hillstone Restaurant Group d/b/a Houston’s, 2009 WL 3128420, 29 IER 1438 (D.N.J., Sept. 25, 2009)(unpublished slip opinion), the federal court found that Houston’s restaurant had violated the SCA and an equivalent New Jersey statute by coercing co-workers into divulging their social networking passwords in order to view employee posts on MySpace. The court upheld a jury award of both compensatory and punitive damages. (The court further found, however, that the employees had no reasonable expectation of privacy in the MySpace group under state privacy law.)

See also, Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), petition for rehearing en banc denied, 554 F.3d 769 (9th Cir. 2009), cert. granted in part, denied in relevant part, City of Ontario v. Quon, 130 S. Ct. 1011 (Dec. 14, 2009)(cell phone company violated SCA in providing transcripts of police officer’s pager texts to police department, where no individual consent given, department had no formal policy regarding monitoring and auditing of employee texts, and employee had reasonable expectation of privacy).

III. THE RIGHT TO PRIVACY AND EMPLOYEE USE OF SOCIAL MEDIA.

1. Constitutional Privacy Protections for Public Employees

Government employees may have a fourth amendment right restricting employer monitoring of their use of social media where they have a “reasonable expectation of privacy.”

The Supreme Court has long recognized that the 4th amendment prohibition against unlawful searches and seizures protects a public employee’s reasonable expectation of privacy in the workplace. However, the 4th amendment is only applicable where the employer’s conduct violates “an expectation of privacy that society is prepared to consider reasonable.” O’Connor v. Ortega, 480 U.S. 709 (1987), quoting United States v.
Jacobsen, 466 U.S. 109, 113 (1984). This standard is applied on a case by case basis. The employee must also demonstrate a subjective expectation of privacy. See Shaul v. Central Valley-Springfield Central School District, 363 F.3d. 177 (2d Cir. 2004).

A public employee may have a reasonable expectation of privacy with respect to the contents of her work computer.

See, e.g., Leventhal v. Knapek, 266 F.3d 64 (2nd Cir. 2001) (reasonable expectation of privacy regarding work computer where employee occupies private office and maintains exclusive use of the office computer, desk and filing cabinet). See also United States v. Slanina, 283 F.3d (829) (5th Cir. 2002)(reasonable expectation of privacy in password protected computer in locked office, even though coworkers had master key access to office and network administrator could access computer files), cert. granted, judgment vacated on other grounds and remanded, 537 U.S. 802 (2002).

A public employer can create a reasonable expectation of privacy by notifying its employees that they can maintain both public and private files on their computer, with the private files not accessible to others. See, e.g., Haynes v. Office of the Attorney General, 298 F. Supp.2d 1154 (D. Kan. 2003); Maes v. Folberg, 504 F. Supp.2d 339 (N.D. Ill 2007)(university professor had reasonable expectation of privacy in laptop computer, in the absence of university policy); see also United States v. Stults, 575 F.3d 834 (8th Cir. 2009), cert. denied, 130 S.Ct. 1309 (2010)(no reasonable expectation of privacy in personal computer files accessible to others through peer-to-peer file sharing software, even if defendant unaware of such access); United States v. Borowy, 2010 WL 537501 (9th Cir. 2010)(no reasonable expectation of privacy where defendant tried unsuccessfully to engage privacy feature in peer-to-peer file sharing program).

In City of Ontario v. Quon, __ U.S. __, 130 S. Ct. 2619 (2010), the Supreme Court recently delved into workplace privacy issues with marked restraint. The Court left standing a Ninth Circuit decision finding that a phone company violated the SCA in providing to the employer written transcripts of employee text messages on employer-issued pagers. It granted certiorari solely on the Fourth amendment issue whether the employer – a police department – must either have a warrant or the employee’s consent to view his text messages. The police department had a computer use policy that did not, on its face, apply to text messages, and an informal policy that “text messages would not be audited” if the employee paid for the overages beyond maximum allowable characters.

Citing the rapidly changing landscape regarding social media technology and societal acceptance of its use, the Court declined to fashion a far-reaching rule to govern privacy expectations in communications on employer owned electronic equipment. The Court instead assumed that the employee had a reasonable expectation of privacy in his text messages. The Court’s reasoning is worth quoting at length:
Rapid changes in the dynamics of communication and information transmission are evident not just in technology itself but in what society accepts as proper behavior. Many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency. The law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications. At present it is uncertain how workplace norms, and the law’s treatment of them, will evolve.

130 S.Ct. at 2629-30.

The Quon Court therefore simply assumed a reasonable expectation of privacy, and went on to find that the police department’s search of the employee’s text messages was reasonable and therefore lawful under the Fourth amendment. The Court held that the employer’s text message audit was justified by operational needs (namely, to determine whether the department needed to increase its text message limits under its contract with Arch Wireless), was reasonably related to that goal, and was not excessively intrusive. (The employer had limited the employee audit to two months’ use, and had redacted all messages sent off duty). Thus, the employer search of the employee text messages was lawful.

Despite the Supreme Court’s refusal in Quon to fashion a broad rule governing privacy expectations, a clear employer policy that computers are only for work use and may be monitored will likely undercut an argument that an employee has a reasonable expectation of privacy in a work computer’s contents, including stored computer files regarding the websites the employee had visited. See, e.g., U.S. v. Simons, 206 F.3d 392 (4th Cir. 2000) (downloaded child pornography found on computer held admissible in criminal prosecution), cert. denied, 534 U.S. 930 (2001); see also Quon, supra 130 S. Ct. at 2630 (“employer policies concerning communications will of course shape the reasonable expectation of their employees, especially to the extent that such policies are clearly communicated”).

But the Supreme Court’s recognition of the rapidly evolving nature of both work-based technology and societal norms regarding its use, and its express refusal to fashion a broad based rule governing privacy expectations in the face of such ongoing and rapid change, indicates that much remains in play in Fourth amendment privacy law.

2. **Common Law Right to Privacy in Private Sector.**

Employer monitoring may give rise to a state common law action for the intentional tort of invasion of privacy.
See, e.g., Doe v. Kohn, Nast & Graf, 862 F.Supp. 1310 (E.D. Pa 1994) (finding law firm partner’s search of associate’s desk and discovery of letter confirming HIV diagnosis actionable, where the letter did not involve a work-related matter); K-Mart Corp. v. Trotti, 677 S.W.2d 632 (Tex. Ct. App. 1984) (right to privacy supports damage award where manager searched employee’s locker and purse without consent and employee had placed lock on locker with employer’s knowledge).

Employees may also have a tort action based on an unauthorized disclosure, if the employer publicizes information it finds based on employees’ social media use.

See, e.g., Levias v. United Airlines, 27 Ohio App.3d 222 (Ohio App. 1985) (actionable claim where employer disclosed gynecological information to employee’s supervisors and husband); but see Romano v. Steelcase Inc., 2010 WL 3703242 (N.Y.Sup. 2010)(no reasonable expectation of privacy in information published on social media sites).

But keep in mind that, in the employment context, employers are typically only found to invade their employees’ privacy in the most extreme circumstances.

See e.g., Shefts v. Petrakis, 758 F. Supp.2d 620 (C.D. Ill 2010)(no reasonable expectation of privacy, for purposes of Illinois Eavesdropping statute, where emails sent from private Yahoo account on company computer, where company manual states that all communications sent or received on company equipment are not private and are subject to monitoring).

And that the American brand of what is “private under law” is generally limited to information one actively keeps hidden.

Will the law move away from such an “all or nothing” approach to privacy, especially where off-duty social media activity is at issue?

As the above discussion illustrates, American law generally takes an “all or nothing” approach to privacy. In order for a privacy right to be recognized, an individual must keep the information completely secret from others. Failure to take affirmative steps to fully safeguard that information is equated with an implied waiver of whatever privacy right may otherwise exist. E.g. U.S. v. Barrows, 481 F.3d 1246 (10th Cir. 2007)(employee who connected his personal computer to employer’s computer network and did not password protect his files had no expectation of privacy in files viewed by coworkers); Commonwealth of Pennsylvania v. Sodomsky, 939 A.2d 363 (Pa. Super. Ct. 2007) appeal denied, 962 A.2d 1196 (Pa. 2008), cert. denied, 129 U.S. 2776 (2009)(no privacy interest in computer files left with Circuit City for diagnostic test regarding installation of DVD drive, when employee discovered child pornography video files and reported it to police).

Courts generally have the same view of personal information posted on the internet. United States v. Gines-Perez, 214 F. Supp.2d 205, 225 (D.P.R. 2002)(“[I]t strikes the Court as obvious that a clam to privacy is unavailable to someone who places information on an indisputably public medium such as the Internet, without taking any measures to protect the information.”), vacated and remanded for clarification on other grounds, 90 F3d Appx. 3 (1st Cir. 2004); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015 at 4 (Tex. App. 1999)(no reasonable expectation of privacy in emails at work because messages can be forwarded to third parties).

But some have called for a different approach, based on notions of confidentiality rather than secrecy. As one commentator has asserted:

This all-or nothing approach to privacy may be outmoded. New forms of communication allow others to view what are intended to be at least somewhat private conversations. Protecting these conversations requires an attitudinal shift towards acceptance of the idea that just because a few people have access to

---

8 Online social networks have become the primary means of social communications amongst teenagers. While on-line message posting on a Facebook friend’s “wall” is less private than personal email, the intention is largely the same: to share the information with a few online friends, and not to the wider audience to which the posting is accessible. Teens and Social Media I (2007), http://www.pewinternet.org/pdfs/PIP_Teens_Social_Media_Final.pdf (only 14% of teenagers send daily emails to friends; among those who use social networking sites like Facebook, 84% post messages to a friend’s page or wall, even though those venues are accessible to others).
information does not mean it is no longer private. Privacy law will have to adapt to the notion that information can still be private even if it is not concealed..... Confidentiality allows limited disclosure, while privacy law demands near-total nondisclosure. Confidentiality is a better fit for modern communications in which, for example, social networks are a primary venue for social interaction....


This view recognizes that, although an employee’s internet posting may be theoretically viewed by millions, it is actually viewed by very few. And the vast amounts of information on the Internet may be equated with background “noise,” allowing for private conversations on social media similar to private face-to-face conversations in noisy public spaces. See Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. Chi. L. Rev. 919, 968-69 (2005). From this perspective, an employer’s intentional violation of that sphere of privacy – especially where the social media activity involves lawful employee conduct away from work during off duty time—may be likened to “electronic eavesdropping, and therefore an invasion of privacy.” Sprague, supra at 409.

**IV. DISCRIMINATION STATUTES AND EMPLOYER USE OF INFORMATION OBTAINED ON SOCIAL MEDIA SITES.**

The internet and its powerful search engines provide employers with ready opportunity to discover a wide range of information about employees (or job applicants) about which employers are legally prohibited from asking in the workplace – everything from race, religion and ethnicity, to pregnancy, marital status, disability, and family medical history. Given growing employer concerns regarding liability for negligent hiring, see e.g., Garcia v. Duffy, 492 So.2d 435, 438 (Fla. D.Ct. App. 1986); DiCosala v. Kay, 450 A.2d 508, 510 (N.J. 1982), more and more employers are turning to the internet to investigate or prescreen job applicants. A 2010 survey indicates that 70% of HR managers have rejected a job applicant because of information found about them online; the majority has made online screening a formal requirement of the hiring process.9

Even if it is not an employer’s intention to discover such information in monitoring the internet for employee communications and conduct, once such information is revealed, the employer must handle such information carefully in making hiring decisions. See 42 USC Section 2000e(a); 29 C.F.R. Sections 1605.3 (regulating selection practices that discriminate on grounds of religion), 1606.6 (national origin); 1604.7 (preemployment inquiries regarding sex). See EEOC guidelines regarding permissible and impermissible employment application and interview questions under Title VII. *EEOC Guide to Pre-

---

9 2010 Microsoft survey, as reported in Matthew Ingram in, “Yes, Virginia, HR Execs Check Your Facebook Page, Gigaom.com (January 27, 2010).

And at least one federal anti-discrimination statute – the Genetic Information Nondiscrimination Act of 2008 ["GINA"]— expressly prohibits an employer from acquiring genetic information (which includes family medical history) through internet and social media sites. Among the prohibited searches are: employer searches of Facebook, LinkedIn and any other social networking platforms with “limited access”; searches of websites focusing on genetic information and testing; and any internet search intended to obtain genetic information (such as a Google search with an employee’s name and a particular genetic marker). See 29 CFR Sec. 1635.8.

Thus, while an employer may justify its routine Google search of all job applicants on grounds that it has a legitimate business interest in knowing about off duty conduct which may lead to liability or which may somehow compromise or disparage the company’s public image, those searches come with the heavy legal obligation to ensure that the internet search itself, and any discovered information, are handled consistent with federal employment and discrimination statutes.

V. STATE STATUTES IMPACTING PRIVACY CONCERNS.

In many ways, state legislatures are taking the lead in addressing employee privacy concerns based in the workplace. State statutes may sometimes shield a job applicant or employee, if not from employer monitoring, at least from the adverse employment or disciplinary consequences that might flow from social media surveillance.

Some state statutes restrict employers from considering certain aspects of an applicant’s or an employee’s private life in making employment decisions.


But some state legislatures have passed laws which more generally prohibit adverse employment actions based on “use of lawful consumable products”:

Although these statutory protections have generally been limited to private conduct with no employment related consequences, they still might provide significant protection against employer use of “Google searches,” most likely in hiring decisions.\(^{10}\)

A few states have gone further, protecting off-duty conduct writ large. See, e.g., N.D. Cent. Code Section 14-02.4-03 (2004); Cal. Lab. Code Section 96 (k); Colo. Rev. Stat. Section 24-34-402.5(1) (2007); Conn. Gen. Stat. Section 31-51q (2007); NY Lab. Law Section 201-d(2)(a)-(c). But these statutes too generally provide protection only where conduct has no connection to an employer’s business concerns. See, e.g., Colo. Rev. Stat. Section 24-34-402.5 (1) (2007) (“It shall be a discriminatory or unfair employment practice …to terminate … any employee due to … lawful activity off the premises of the employer during nonworking hours unless such a restriction: (a) relates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular employee or … group of employees … or (b) is necessary to avoid a conflict of interest with any responsibilities to the employer or the appearance of such conflict of interest”); NY Lab. Law Section 201-(d)(2)(a)-(c)(no protection of activity where material conflict of interest); McCavitt v. Swiss Reinsurance Am. Corp, 237 F.3d 166, 168 (2d Cir. 2001)(does not apply to romantic relationships or extramarital affairs); (Barbee v. Household Automotive Finance, 113 Cal. App. 4th 525, 6 Cal. Rptr.  406, 20 IER 1143 (Cal. App. 2003) (no protection based on private relationship with coworker conducted away from work during off duty hours)\(^{11}\).

A few states restrict an employer’s monitoring of employee email and internet use without advance notice.

Both Delaware and Connecticut compel employers to provide notice to employees prior to monitoring their email or internet use. See Del. Code Ann. Tit. 19, Section 705 (2007); Conn. Gen Stat. Section 31-48(d) (2007). Both statutes are enforceable through modest statutory fines. But the Connecticut statute also has language limiting the restriction where an employer has a reasonable belief that an employee is engaging in unlawful conduct, conduct that violate work rules, or conduct that implicates the rights of the employer or co-workers.

---

\(^{10}\) Much press attention has been paid, for example, to the “Drunken Pirate” photo posted on Stacy Snyder’s MySpace page, showing the 25-year old college senior in a pirate costume, drinking a beverage from a plastic cup. Snyder was denied her teaching credential and dismissed from a student teaching program after teachers at the school revealed the photo to the school administration. Some of these state statutes might provide legal remedy in such a case. See e.g., Minn. Stat. Section 181.938, subdiv. 2 (2006)(defining alcohol as lawful consumable product).

\(^{11}\) The Court further rejected a state constitutional right of privacy claim on grounds that an employee had no reasonable expectation of privacy regarding intimate relationship with a coworker, citing Cal. CONST. art. 1, Section 1 (constitutional privacy provision applicable to both private and public employees).
VI. DEVELOPING A RESPONSIBLE SOCIAL MEDIA POLICY.

In unionized workplaces where the parties enjoy a collective bargaining relationship, there are many issues of mutual interest and concern regarding social media use that the parties may productively address at the bargaining table. Even in a non-union setting, the legal risks posed by an overly restrictive policy argue for the development of responsible and carefully drafted social media guidelines.

Here are some initial thoughts that might guide the development of a reasonable social media policy:

1. In a unionized setting, a social media policy regulating employee rights to communicate and post materials on the internet, either on or off the job, is a mandatory subject of bargaining. This conclusion is especially clear where disciplinary consequences may result from the breach of a social media policy. See Children’s Hospital of Pittsburgh of UPMC, Case 06-CA-37047, (issuance of ULP complaint where employer unilaterally promulgated social media policy without notice to the union).

2. So too for an employer’s monitoring or surveillance of unionized employees on social networking sites or the internet at large. See Colgate Palmolive Co., 323 NLRB 515 (1997) (installation and use of hidden surveillance equipment at the workplace is a mandatory bargaining subject).

3. Employees should be granted reasonable personal use of employer internet systems.

Employers know that employees use the internet and social media at work, and that such use is generally condoned. A “no personal use” policy will never be consistently enforced. So doesn’t it make sense to agree to a “reasonable use” policy that will eliminate concerns regarding disparate treatment and discriminatory enforcement? The parties could agree on reasonable rules (and prescribe disciplinary consequences) which define prohibited online activity, such as excessive internet use that interferes with work performance, transmission of offensive or harassing materials, visiting pornographic internet sites, and the like.

4. It makes good business sense to develop reasonable rules governing employer monitoring of employee use of the internet at work, and any surveillance by employers of employee activity on the internet (including off duty activity). An employer may seek to eliminate any “reasonable expectation of privacy” in workplace email systems, computer equipment, cell phones, pagers and the like, by warning employees that those communications systems are not private and may be subject to employer monitoring. In the same measure, if discipline may
result from social media activity discovered through employer monitoring, it makes sense to forewarn employees as to the dangers of their social networking and the reasonable rules governing their online behavior. Given further the legal risks that flow from the mishandling of employee information obtained inadvertently or otherwise from social media sites, in violation of labor and discrimination laws, employers may want to rethink their intentions regarding ongoing surveillance of social media sites.

5. **Restrictive social media policies that interfere with the ability of coworkers to communicate online about workplace concerns are likely illegal and should be avoided.** As uncomfortable as it may be to employers, employees have statutory rights to post information on their online personal profiles about their company affiliations, to discuss their wages on Facebook, to complain on social media sites about supervisors and to criticize company policies that affect their working conditions. Employees have the statutory right to post online images and photographs of company logos in the context of portraying labor disputes or other workplace concerns. Social media rules that prohibit employees from “disparaging the employer,” from “discussing internal company policies” or from “depicting the company in any way” (in text or photographs) should be carefully scrutinized as they likely violate Section 7 rights under the NLRA. **Any social media policy that restrict employee communications online should expressly recognize employee rights to discuss workplace issues and concerns, consistent with Section 7,** as long as the employee does not egregiously or recklessly disparage the employer, its products or services.

6. **A reasonable policy regarding employee use of social media should include “no coercion” rules** governing managers seeking to become “friends” on Facebook and other “limited access” social media sites. Perhaps managers and supervisors should be flatly prohibited from even asking to become online “friends” of employees. Policies should prohibit management from asking employees to reveal their passwords to allow employer monitoring of employee posts. At the very least, a social media policy should make clear that no employee will be subject to discipline or negative treatment because they refuse to “friend” a supervisor or manager.