First Amendment, Whistleblower, Employee Privacy Protections And Employer Monitoring

By **Eileen M. Baratuci**

There is complex interplay between employee privacy, the information an employee posts on social networking sites and an employer's right to take action based on this posted information. It is not clear what information an employer can act on without impacting employee Constitutional protections under free speech and freedom of association. When an employee complains about working conditions through social media this may fall within "protected concerted activity" under Section 7 of the NLRB. If any of these protections apply, termination, demotion or discipline of the employee for posting this information may result in employer liability.

Even more intricate is deciphering an employee's privacy interests and how employer policies may impact privacy rights. An employee may presume that information posted on a social networking site is private, but once posted, this information can easily be shared in ways over which the employee has no control. Is it realistic for an employee to expect privacy in information the employee intentionally "made public"? Also, can an employer lawfully regulate an employee's conduct when communicating outside of work in a social media context?

There have been a number of cases in which an employer's decision to act on information gleaned from a social networking site resulted in court action. Those cases can guide employers and employees on how this shared information should be used or avoided when making employment decisions.

Public Employee Free Speech Protections

The First Amendment to the U.S. Constitution protects **public employee's** right to free speech. A public employee does not give up the right to speak about issues of public concern simply because they are a public servant. This is a limited protection that is balanced against the employer's interests in operating efficiently and effectively. For example, confidential information (such as sensitive data or contract negotiations) cannot be disclosed. The protections are limited to non-work related speech, meaning the employee can be expected to act in the employer's best interest when carrying out official duties. However, when a public employee criticizes his/her employer in a blog on the internet, or through private e-mail, may a public employer respond to these communications in a way that disciplines the responsible employee? What if the employee's communication impairs the employer's interests (i.e. the employer is not selected for a coveted grant bid) or impairs the employee's effectiveness?

Public free speech cases are decided on a "balancing of interests" test, which takes into account the nature of the employee's speech, and the employer's business interests, plus the level of disruption the communication creates. These cases are very fact specific. If the employee's speech does not serve a public interest, the speech may not be protected. Even protected speech may be regulated if the exercise of the employee's right is clearly harmful to the employer's valid business interests.

Whistleblower Protections

To determine when an employer may respond to a harmful statement by an employee, it is helpful to understand the scope of whistleblower protections. Whistleblower protections exist for public employees and some private employees covered under specific federal industry regulations. Typically, whistleblower protections require that the

employee process a complaint through the steps provided in the whistleblower policy or regulatory statute. If the employee fails to do so, he or she may not qualify for these protections, which include a protection against retaliation.

Whistleblower protections may exempt personnel decisions and personal grievances. Instead protections focus on issues of interest to the public. For example, a public employee's complaint about misuse of public funds, corruption, abuse of power, or serious safety concerns all fall within the whistleblower protections. Many federal and State laws have unique whistleblower protections, such as reporting violations of the environmental protection laws, or violations of the financial regulatory provisions.

Fourth Amendment Protection Against Unreasonable Searches

Other protections stem from the Fourth Amendment protections from unwarranted search and seizure. The application of the Fourth Amendment to workplace searches is discussed in the frequently cited case of *O'Connor v. Ortega*, 480 U.S. 709 (1987). The Supreme Court stated even if a reasonable expectation of privacy exists, a government employer may conduct a search without a warrant for non-investigatory work related purposes, including work related misconduct, if such searches are reasonable under the circumstances. Privacy interests also stem from State Constitutional or Federal statutory privacy interests.

Federal Regulations as Sources of Privacy Protection

The Electronic Communication Privacy Act of 1986 (ECPA):

This statute prohibits the intentional interception of electronic communications, with an exception for employers who monitor their networks (phones, computers, e-mail etc.) for business purposes. The **Stored Communication Act** is a subset of the ECPA, which protects electronic data in "storage", limiting access to data protected by the ECPA.

The National Labor Relations Act (NLRA)

Workers have a right to form unions, discuss working conditions and engage in union organizational activities. Employers are prohibited from retaliating against employees engaged in these protected activities. Similar protections exist for rail and airway employees under the **Railway Labor Act**. If an employee subject to these protections participates in criticism of their working conditions through electronic communications (including social media), an employer may be precluded from disciplining the employee.

Just where that line should be drawn between protected union organizational activities and conduct that may undermine the employer's operations is still unclear. For example, if a disgruntled employee complains about his supervisor on a widely shared e-mail that results in the company losing a lucrative contract bid, can the employer take action? Can the employer at least request the harmful information be removed? The National Labor Relations Board has taken a much broader view on what is protected employee activity than employers are likely to accept, so court challenges to the NLRB decisions are likely to continue.

Regulating the Use of Employer Issued Equipment and Devices

Employers are permitted to regulate the use of employer-issued equipment to confine employee use to business purposes. In order to regulate usage, the employer may wish to monitor e-mail or other electronic communications. Before doing so, the employer must notify the employee of the employer's intent to monitor communications on employer issued devices, to prevent employees from gaining a privacy interest in their communication.

Under the Electronic Communications Privacy Act, 18 U.S.C § 2511, all electronic communications are presumed private, unless an employer adopts a clear policy to eliminate the personal use of e-mails, phones, texts or other electronic communications devices. The employer must clearly notify employees their e-mail and electronic communications will be monitored to eliminate an expectation of privacy. Then the employer must actually provide monitoring to fully eliminate an employee privacy interest. In some cases, the failure to actively monitor electronic communications gave rise to a privacy interest, even when employer policies said otherwise.

Employer Monitoring Employee Phone Conversations for Quality Control

Nothing prohibits an employer from monitoring employee business calls to evaluate employee performance. Employees must be advised of this and customers and callers must be notified as well, to make certain they consent to a recording of their call. Simply remaining on the line after being advised of the employer's practices of monitoring or recalling calls, is sufficient to indicate the caller's consent. However, if the person monitoring employee calls realizes a call is personal in nature, the person monitoring the calls must cease doing so.

Search and Monitoring Employee E-mail Communications

Let's assume an employer has adopted a policy which either prohibits the use of employer computers for personal use, or (more realistically) notifies employees of reasonable restrictions on the personal use of employer issued equipment. Adopting one of these two options in a clearly written policy is a good way to deal with the need to balance employee privacy and workplace monitoring for misuse or abuse. If the employee is notified of the policy each time they log on to their computer, or each time they turn on a personal communication device, the consistency of that reminder will be hard to ignore. The employer's policies and notices can curb employee expectations, and in doing so, can eliminate the risk of employee privacy claims.

If you have a company that monitors employee computer use but has not adopted a clear policy placing employees on notice, beware. Conversely, if you have a monitoring policy but do not actively monitor employee communications, you may have created an expectation of privacy through company inaction. If an employer had no clear policy to curb the employee's expectation of privacy, even searching an employee's work computer can pose risks, particularly if criminal activity is the focus of the search.

Employer Search of Employer Issued Text Device

In *Ontario v. Quon*, a 2010 United States Supreme Court decision clarified some of the privacy issues impacting employers and employees. Quon, a police officer for the Ontario Police Department argued his employer's search of text messages sent and received from a City issued device, violated the Store Communications Act, and his Fourth Amendment rights against unreasonable searches. The employer was conducting an audit of the text messages to determine why certain employees exceeded their contract limits for text messages, and to determine if personal use was excessive. The Supreme Court overturned a Ninth Circuit decision concluding the employer's search of City issued electronic messaging devices was unreasonable. The Supreme Court stated:

> First, because "some [government] offices may be so open . . . that no expectation of privacy is reasonable," a court must consider "[t]he operational realities of the workplace" to determine if an employee's constitutional rights are implicated. Second, where an employee has a legitimate privacy expectation, an employer's intrusion on that expectation "for non investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances". *Citations omitted*. …
>
> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve. … Petitioners' warrantless review of Quon's pager transcript was reasonable …because it was motivated by a legitimate work-related purpose, and because it

> was not excessive in scope. *O'Connor v. Ortega*, 480 U.S. 709, 726 (1987) (plurality). There were "reasonable grounds for [finding it] necessary for a non investigatory work-related purpose," … in that Chief Scharf had ordered the audit to determine whether the City's contractual character limit was sufficient to meet the City's needs. It was also "reasonably related to the objectives of the search," … because both the City and OPD had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets for work-related expenses, or, on the other hand, that the City was not paying for extensive personal communications

When the Court looked at the scope of the search and whether the search was reasonable it took into account that the employer redacted text information that was generated while Quon was off duty. Thus, sexually explicit text messages sent while on duty was conduct the employer had a legitimate interest in.

Conclusion

The issues of worker privacy and various forms of employer monitoring are part of an emerging area of the law. The first step for employers in reducing the risk of litigation is to adopt a clear set of policies limiting an employee's expectation of privacy in connection with employer issued communication devices and computers. If compliance with these policies is done by monitoring usage, the employer's efforts must be routine, as a means of ensuring that privacy expectations do not arise. If a search relating to enforcing workplace rules takes place, the scope of any warrantless search must be reasonable and tied to a legitimate employer interest. When checking e-mails and other communications, an employer may need to stop searching the content of communications the employee intended to be private, only going as far into the search as needed to determine whether a policy has been violated. Finally, when taking an adverse employment action based on social network information or private e-mails, be careful to determine whether privacy, free speech or union organizing activities are being infringed upon. Due to the unsettled nature of this area of the law, it is best to consult with an attorney before conducting a search or acting on information that may be considered private in nature.