



February 2011

## ELECTRONICS AND THE RIGHT TO PRIVACY IN THE WORKPLACE

by Madeline S. Baio

### Contacts

**Cheryl M. Nicolson**

nicolson@nicolsonassoc.com

**Madeline S. Baio**

baio@nicolsonassoc.com

Rose Tree Corporate Center II  
1400 N. Providence Road  
Suite 6050  
Media, PA 19063  
610.891.0300  
[www.nicolsonassoc.com](http://www.nicolsonassoc.com)

The issue as to whether employers may review and/or monitor private emails, web histories and other electronic communications of employees on company issued computers, cell phones, pagers and the like has been the subject of much debate. This article will review several aspects of this issue and explore the responsibility of management to prevent misuse of company resources; the privacy concerns of employees whose communications may be monitored; and what relevance it all has to the day-to-day operations of a business and compliance with state and federal laws.

### The Need for Electronic Usage Policies

The prevalence of electronics in the workplace has increased efficiency, productivity and communication like few other advances in society. At the same time, however, use of technology in the workplace has heightened the concern of many employers regarding trade secret violations and the disclosure of other types of confidential information. It has also expanded the methods by which sexual harassment of co-workers, subordinates and others may occur. And, it has provided an easy vehicle for workers to spend countless non-productive hours on company time. For these reasons and other reasons, employers have had to grapple with how best to monitor and prevent such costly behavior.

While computer and other electronic monitoring seems justified from a business perspective it has, in turn, given rise to employee privacy concerns. At the heart of these concerns is whether employees have a reasonable expectation of privacy when they utilize company supplied electronic devices. In analyzing this issue, most courts have looked at whether a company maintains a written policy on electronic usage. Many Courts, including those in the

Eastern District of Pennsylvania, have found that there is no reasonable expectation of privacy on the part of employees where an employer has articulated a policy, either through company announcements, employee handbook provisions or periodic policy updates, that the electronic usage of employees will be inspected and/or monitored. On the other hand, where no such policy has been articulated or a policy, although articulated, has not been enforced, courts have often found that a reasonable expectation of privacy does exist.

Clearly then, it is advisable for employers to implement, maintain and enforce specific written policies which place limitations on the use of company issued systems and equipment and which advise employees that their use of such company issued systems and equipment will be subject to unannounced inspection and monitoring. Periodic reminders of these policies should be given and a document signed by each employee at the time of hire which acknowledges that he or she has reviewed, understands and agrees to be bound by the policies, is also advisable. Electronic usage policies should clearly state:

- Access and pass codes must be known to the company at all times. Files may not be password protected without the specific authorization of management.
- Back up copies of email and voicemail will be maintained and can be referenced later on for business and legal reasons.
- All company provided systems including email, voicemail and computer network systems should be used only for company business and not for personal purposes.
- The company's electronic systems and equipment may never be used in a manner that is disruptive or offensive to



others, including, but not limited to, the transmission of sexual content, messages, cartoons, ethnic or racial slurs, or anything that may be construed as harassment or disparagement of others either individually or as a group or class of persons.

- There is no right to privacy concerning anything stored, received or transmitted on company provided electronic devices or systems including, without limitation, web history, personal email accounts, text messages, voice mail messages, blogs and social network site communications.
- Access to or use of company issued electronic devices should never be given to those who are not actively employed by the company and individual employee access codes and/or pass codes should not be shared with co-workers unless specifically authorized in writing by management.
- Violation of the company's electronic usage policies will result in disciplinary action up to and including discharge.

Once a proper electronic usage policy is in place, employers should be fairly well protected from any privacy claims relating to management's inspection and/or monitoring of company systems or equipment.

#### **Electronic Usage Policies in Litigation**

The ability to inspect and monitor employee communications and activity can be important in a variety of situations. As previously mentioned, it has the potential to detect improper dissemination of confidential and/or proprietary information and can deter harassing or intimidating communications. Most recently, in a sexual harassment and retaliatory discharge case which previously received some media attention, Judge Gene Pratter of the United States District Court for the Eastern District of Pennsylvania denied plaintiff's motion in limine seeking to preclude emails found on her company issued computer which

contained sexual content. In that case, *Seybert v. The International Group, Inc.*, Judge Pratter held that the emails in question would be "inexorably probative" of the issue as to whether plaintiff was subjectively offended by her supervisor's statement to her at a company Recognition Dinner that "it's really good if you go down deep, into the chocolate, with your berry." Judge Pratter also found that the emails would be relevant to plaintiff's emotional distress claim. Judge Pratter reasoned as follows:

"Here, the emails with sexual content involve the same general type of humor as Mr. Marchand's comment at the Recognition Dinner- a humor rooted in sexual innuendo and supposed euphemisms. For instance, Mr. Marchand's alleged comment about going "down deep into the chocolate [dessert] with your berry" presumably could be likened to Exhibit 61, which contains a photograph of an elderly man wearing only a Santa hat and boots, resting on his stomach, with the caption, "Just Roll Me Over Darlin... 'cause I'm Laying On Yer Present." In both cases, creative imagery and base sexual wordplay are being used to construct metaphors in an apparent attempt to titillate, amuse, entertain, instruct, or simply "gross out" (in the phrase of some generations) others."

*Seybert v. IGI*, ED Pa. Civil Action No. 07-3333, October 13, 2009 Memorandum Opinion of the Honorable Gene E.K. Pratter.

#### **Electronic Usage Policies and Waiver of Privileged Communications**

Employers and employees alike should also be aware that the privileged nature of certain communications may be waived if sent or received on company issued electronic devices if there is a policy in place which specifically disclaims any reasonable expectation of privacy. Those communications include, but are not necessarily limited to, attorney/client communications. Generally speaking, if an employer has made it clear through a written

and publicized policy that no reasonable expectation of privacy exists; that this policy applies to personal email accounts on company computers and hand-held devices as well as personal computers and devices used to access company systems; and that the policy is uniformly enforced, the employee will likely be deemed to have waived the attorney/client privilege in any communications sent or received from his or her attorney.

#### **The Future of Electronic Usage Policies and the Need for Uniform Enforcement**

Finally, privacy issues reach constitutional proportions when the employer is the government. In *City of Ontario v. Quon*, 130 S.Ct. 2619, 177 L.Ed. 2d 216, 2010 U.S. LEXIS 4972 (June 17, 2010), the Ontario, California Police Department had a written "Computer Usage, Internet and E-mail Policy" which stated that use of computers for personal reasons was a violation of Department policy and that employees had "no expectation of privacy or confidentiality when using these resources." The plaintiff, Sergeant Quon, signed off on the policy and attended a meeting in which it was explained that the policy applied to pagers. Some time thereafter, however, plaintiff's lieutenant made it clear to staff and to the plaintiff in particular that he would not audit plaintiff's pager as long as he agreed to pay for any overage charges on his account. Quon agreed and paid for the overage charges three or four times without anyone auditing his text messages.

After several months, Quon's supervisor told the Department Chief that he was "tired of being a bill collector" and a decision was made to review the text messages to determine if the officers were being required to pay for work-related text messages or if the overages were for personal messages. As a result, without warning, Quon's text messages were audited by the Department and it was discovered that many of the messages sent and received on his pager



were not work-related, and some were sexually explicit.

Quon filed suit claiming Fourth Amendment violations. The trial court held that Quon had a reasonable expectation of privacy in the text messages on his pager because the no-privacy policy had been orally modified by the plaintiff's supervisor. The jury, however, determined that the audit was reasonable and therefore the District Court held that Quon's Fourth Amendment rights had not been violated. The Ninth Circuit agreed that Quon had a reasonable expectation of privacy but disagreed that the search had been reasonable. The City appealed and the United State Supreme Court granted certiorari.

Before the Supreme Court, the City of Ontario argued "that the Ninth Circuit failed to appreciate the most salient facts of the case: that Sergeant Quon was a SWAT officer using a text-messaging pager provided by the police department to facilitate SWAT operations; that the City had a written no-privacy policy that applied to the pager; and that any messages exchanged on the pager were potentially subject to disclosure under the California Public Records Act."

After hearing oral argument, the Supreme Court held that Sergeant Quon's Fourth Amendment rights had not been violated "[b]ecause the search was motivated by a legitimate work-related purpose, and

because it was not excessive in scope." Using great care to limit its decision to the facts of the case, Justice Anthony Kennedy, writing for the Court, explained:

"The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."

Justice Kennedy went on to stress that the facts in the Quon case should not be used to "establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communications devices." Recognizing the rapid changes in technology and the impact upon societal behavior and work place norms, Justice Kennedy was not willing to predict how the law's treatment of technology in the work place would evolve. He did, however, state that employer policies concerning communications will continue to shape the reasonable expectations of their employees, "especially to the extent that such policies are clearly communicated."

While the Supreme Court's decision in Quon is limited to privacy issues as they pertain to government employers, government and

private employers alike are well advised to evaluate their existing communication policies and ensure that they are carefully drafted, clearly communicated and consistently enforced.

*For over 25 years, Madeline S. Baio has counseled and defended clients in connection with employment related claims and lawsuits before the EEOC, PHRC and other state agencies as well as the State and Federal Courts. Ms. Baio has undertaken workplace investigations stemming from retaliation and harassment claims and has advised clients with regard to the drafting and implementation of employee policies and procedures. Among other things, she has defended Civil Rights Claims, FLSA claims, ERISA claims and claims of discrimination based on race, age, sex, national origin, and disability. Her clients have included national retail stores, hospitals, aerospace, defense and technology companies, trucking companies, banking institutions, country clubs, municipalities and municipal authorities, county prisons and privately owned businesses and non-profit organizations. Ms. Baio can be reached at [baio@nicolsonassoc.com](mailto:baio@nicolsonassoc.com) or by calling 610-891-0330.*

---

*Portions of this article have been reprinted with permission from the February 23, 2010 edition of the LEGAL INTELLIGENCER © 2010 ALM Media Properties, LLC.*

**Disclaimer**

*The contents of this article are for informational purposes only. The information provided may not reflect the most current legal developments. The contents of this article do not constitute legal advice and readers of this article should not act or refrain from acting based on information contained in this article. Receipt of this article does not create an attorney-client relationship.*