Dinsmore&Shohl LLP
ATTORNEYS

E-mail, Texting and Privacy Rights in the Workplace

July 1, 2010

Mychal Sommer Schulz

This article was originally published in the Westlaw Journal *Telecommunications Industry* Report.

I do it. You do it. Virtually everybody does it. The "it" is using your computer at work, or your company-issued cell phone, or your work e-mail account accessed remotely, to conduct non-business-related communications. Whether they are ordering the latest electronic gadget from Amazon.com or calling their friends to confirm after-work plans, employees in a workplace increasingly depend upon e-mails, texting and cell phones, both inside and outside their physical workspaces, to achieve maximum production efficiency while also connecting with their non-work relationships. As employers struggle to deal with employee use of technology in the workplace, courts also struggle to analyze the impact of that technology in the workplace in efforts to balance an employee's expectation of privacy and the employer's right to control its own work environment.

Recent developments ensure that the privacy rights in the workplace as they relate to e-mail, texting and mobile phone communications will continue to come under judicial scrutiny. A few months ago the New Jersey Supreme Court examined an executive's expectation of privacy in e-mail messages to and from her personal attorney from her work computer in *Stengart v. Loving Care Agency*, 990 A.2d 650 (N.J. Mar. 30, 2010). Meanwhile, the U.S. Supreme Court recently issued its decision in *City of Ontario v. Quon*, No. 08-1332 (June 17, 2010), in the Court found that the City of Ontario Police Department's review of private pager/text messages sent by a police officer on his department-issued pager did not violate the police officer's Fourth Amendment rights. In addition, most observers agree that the National Labor Relations Board will likely revisit the use of e-mail solicitations in the context of union campaigning in the workplace now that President Obama's appointments to the NLRB have taken office. Together, these developments ensure that the issue of an employee's use of employer-issued computers and other electronic communications equipment will remain an area of judicial focus.

Yeah, but you didn't tell me

In *Stengart* the New Jersey Supreme Court addressed the extent to which communications between a home health care company executive and her private attorney through the executive's private e-mail account (Yahoo), which she accessed through her company-issued computer while at work, were protected by the attorney-client privilege. While the court ultimately found that Marina Stengart's communications were, in fact, protected by the attorney-client privilege, of more interest to employees and employers was the court's analysis of whether Stengart had a "reasonable expectation of privacy" in the e-mail messages.

Shortly before she left the company, Stengart accessed her personal e-mail account through her computer at work and exchanged e-mails with her attorney about her soon-to-be-former employer. While she did not save the password to her Yahoo account on the computer, Stengart testified that she was unaware the computer saved all Internet pages she accessed from the computer in a temporary file cache. Upon leaving her job, she returned the computer to the company and filed a civil complaint against it, alleging, among

other things, constructive discharge because of a hostile work environment, retaliation, and harassment based on gender, religion and national origin. Shortly after Stengart filed her complaint, the company did what many employers would have done: It retained an expert technician to create a forensic image of the computer's hard drive, which revealed in the temporary Internet file cache a number of e-mails that Stengart had exchanged with her attorney.

The company's attorneys took the position in discovery that Stengart had no reasonable expectation of privacy in any files contained on a company-owned computer as the company had the right, under its electronic communication policy, to review such files. The policy stated:

The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice. E-mail and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee. The principal purpose of electronic mail (e-mail) is for company business communications. Occasional personal use is permitted; however, the system should not be used to solicit for outside business ventures, charitable organizations, or for any political or religious purpose, unless authorized by the Director of Human Resources.

Stengart, No. A-16-09 at 8. This language, the company argued, clearly dispelled any reasonable expectation that an employee may have had in the use of company computers.

Initially, the court acknowledged that, as "businesses and private citizens alike embrace the use of computers, electronic communication devices, the Internet, and e-mail[,] [a]s those and other forms of technology evolve, the line separating business from personal activities can easily blur." *Stengart*, No. A-16-09at 2. It also conceded that, "[i]n the modern workplace, . . . occasional, personal use of the Internet is commonplace. Yet that simple act can raise complex issues about an employer's monitoring of the workplace and an employee's reasonable expectation of privacy." *Stengart*, No. A-16-09 at 2.

The court then examined the exact language of the policy and found that "[t]he scope of the written policy is not entirely clear." Specifically, the court stated:

"It is not clear from that language whether the use of personal, password-protected, web-based email accounts via company equipment is covered. The policy uses general language to refer to its 'media systems and services' but does not define those terms. Elsewhere, the policy prohibits certain uses of 'the e-mail system,' which appears to be a reference to company e-mail accounts. The policy does not address personal accounts at all. In other words, employees do not have express notice that messages sent or received on a personal, web-based e-mail account are subject to monitoring if company equipment is used to access the account." The court concluded that, as written, the policy creates ambiguity about whether personal e-mail use is company or private property.

Stengart, No. A-16-09 at 13-14.

Admittedly, the court's analysis in *Stengart* was influenced by the fact that the communications by the employee were with her attorney, and the court's decision can be interpreted to signify the New Jersey Supreme Court's zealous protection of the attorney-client privilege. Nonetheless, the court's analysis of the expectation of privacy in the workplace, and its parsing through the written company policy concerning the privacy of e-mail and other electronic messages, casts significant doubt on the extent to which an employer can write a privacy policy that is both specific enough to cover all possible uses of electronic communications equipment and yet allows sufficient flexibility to permit employees to use company equipment for personal business. Even the court in *Stengart* stated zero-tolerance policy can be unworkable and unwelcome in today's dynamic and mobile workforce.

Yeah, you told me, but my supervisor told me something different.

Only 20 days after the New Jersey Supreme Court issued its decision in *Stengart*, the United States Supreme Court heard oral argument in *Quon v. City of Ontario*, 2010 WL 2400087 (June 17, 2010). This case dealt with a police officer's expectation of privacy in messages sent and received from both his wife and his girlfriend over the pager/text device issued to him by his employer, the City of Ontario, California, Police Department. In *Quon*, the police department issued a pager device to all police officers, and each officer signed a written policy which explicitly stated that there were no privacy rights in e-mails or internet usage through the use of city computers and related electronics equipment. When the officer received the pager device, he was verbally told that the electronics policy applied to pager devices as well.

The police department claimed that the written policy was clear and dispelled any reasonable expectation of privacy that the officer could have had in the embarrassing personal messages discovered on the pager. The officer, on the other hand, claimed that the electronics policy was modified verbally when he was told by his supervisor that, if the officer paid for any monthly "overage" charges associated with the pager, then the police department would not audit the content of the messages. The officer argued that the police department's review of his racy personal messages, which was undertaken as part of an audit to determine whether the character limit for the paging device needed to be adjusted, violated the officer's right to privacy.

The 9th U.S. Circuit Court of Appeals agreed with the police officer and found that an individual retains an expectation of privacy in the content of text and pager messages sent vis-à-vis a service provider. While the 9th Circuit stated that "[w]e do not endorse a monolithic view of text message users' reasonable expectation of privacy, as this is necessarily a context-specific inquiry[,]" it found that the "operational reality" of the police department was that the messages would not be audited or reviewed if the officer paid the overage charges, which the police officer had done a few times. As such, the court found that the policy department's review of the messages violated the officer's reasonable expectation of privacy under the Fourth Amendment, a finding that the police department appealed to the Supreme Court. The Supreme Court, however, reversed the 9th Circuit and found that the police department's review of the pager messages did not violate the officer's Fourth Amendment rights.

Importantly, the Court found that its inquiry was governed by a two-step analysis under the Fourth Amendment: (1) whether the "operational realities" of a public work place led to a "reasonable expectation of privacy" and (2) if so, was the public employer's intrusion reasonable. The Court limited its holding to a finding that the police department's examination of the pager transcripts for a two month period was reasonable. It specifically refrained from ruling on whether the police officer had a reasonable expectation of privacy in the pager messages. The Court noted:

At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve….Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated. *Quon*, 2010 WL 2400087 at *10.

In making these observations, the Court clearly indicated its unwillingness to enter a theoretical discussion of when and under what circumstances an employee may have a reasonable expectation of privacy in workplace communications. It also, however, sent a message to employers -- both public and private -- that clear policies concerning the status of communications will play a large part in determining whether an expectation of privacy is reasonable or not.

You may have told me, but so what?

Employee use of electronic communications equipment is also affected by the National Labor Relations Act ("the Act"). Specifically, the National Labor Relations Board ruled in *Register-Guard*, 351 NLRB 1110 (2007), that employees have no statutory right under the Act to use an employer's e-mail system to send messages related to unions or union organization; hence, an employer's policy that prohibited the use of its e-mail system for non-job-related solicitations did not violate the Act.

In *Register-Guard*, the employer maintained a written Communications Systems policy (CSP) that provided, in relevant part, that "Communication systems are not to be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations." In the mid-1990s, the employer broadened the term "communications system" to include e-mails. In the years that followed, however, the employer did not enforce the non-solicitation ban, and employees regularly used e-mails for personal business, including to solicit for sports tickets, lunches, poker games, and community events. In 2000, an employee and local union president used the employer's e-mail system to send an e-mail encouraging employees to wear green in support of the union in upcoming bargaining negotiations and to also participate on behalf of the union in a parade. The employer disciplined the employee for violation of the CSP, and the union then filed unfair labor practices charges against the employer.

The board held that a neutral policy which does not discriminate between union-related solicitations and other types of non-work-related solicitations is proper. The board also held that the employer did not violate the Act by enforcing the CSP because there was no evidence that the employer permitted employees to use the e-mail system to solicit support for any group or organization such as had occurred in the case before it.

The union petitioned the District of Columbia Circuit Court of Appeals for a review of the board's decision. In *The Register-Guard v. NLRB*, No. 07-1528 (D.C. Cir. July 7, 2009), the court reversed the board, in part. Specifically, the court reversed the board's decision that the employer properly applied the CSP. The court noted that the CSP itself did not distinguish between solicitations on behalf of groups or organizations and personal or individual solicitations and therefore ordered the discipline be withdrawn.

Importantly, however, the court did not address whether a written policy that discriminated between solicitations on behalf of groups or organizations and on behalf of individuals would be valid under the Act. Likewise, the court did not address - because neither side appealed -- the board's determination that a facially neutral non-solicitation e-mail policy that barred all non-job-related solicitations, including union-related solicitations, did not violate the Act.

Together, the board and D.C. Circuit Court decisions stand for the proposition that a facially neutral non-solicitation policy that is evenly and uniformly applied in practice does not run afoul of the Act. With President Obama's nominations to the board now in place, however, this issue may be revisited as current board chairman Liebman (along with another member) dissented to the board's decision in Register-Guard, stating that "[w]here, as here, an employer has given employees access to e-mail for regular, routine use in their work, we would find that banning all non-work-related 'solicitations' is presumptively unlawful absent special circumstances. No special circumstances have been shown here." *Register-Guard*, 351 NLRB at 1121.

Lessons.

What lessons can be taken from recent developments? First, employers need to ensure that they have clear, well-written policies concerning an employee's use of company-issued electronic communications equipment. Second, employers need to keep such policies updated to account for technological advances and changes in the law. Third, employees should be required to read and execute a document stating they understand such policies. Better yet, employees who truly wish to maintain their privacy should assume that nothing transmitted in the workplace or transmitted on an employer-owned piece of hardware, whether by e-mail, text, phone or page, is truly private.

Meanwhile, the intersection between an individual's right to privacy and an employer's right to control the workplace in the age of technological advances will continue to be the subject of judicial scrutiny.