

MONITORING ELECTRONIC COMMUNICATIONS AND SOCIAL MEDIA USAGE IN THE WORKPLACE: WHAT ARE THE LIMITS?

by Galit Kierkut and Suzanne M. Cerra

Employee electronic communications continues to be one of the more challenging areas for employers. Not only is the technology and usage new and constantly changing, but the courts and Congress, in charting this evolving area, are issuing seemingly conflicting decisions and legislation.

Social media usage has further blurred the lines between public and private, and social and business communications. Those of us who draft policies and counsel corporate clients on the application of such policies are closely following each development, but the limited guidance from the cases and statutes is not always helpful in shaping policies that are comprehensive, effective, and enforceable.

Since at least 2005, we have been advising clients that if they have Internet policies that permit them to monitor and restrict employees' usage, they must do so, especially if they have reason to know of a violation of the law or policy. That advice arose from *Doe v. XYZ Corporation*,¹ where the Appellate Division's decision assumed that employers had an affirmative obligation to monitor employees' email and Internet usage when their handbook set forth a policy permitting such monitoring. The Appellate Division held that a company could be liable to a third party for

failing to detect an employee's improper Internet usage (in this case, child pornography) when it knew or should have known about such usage.

In *Doe*, the manager was aware that the employee was visiting pornographic sites while at work. Despite a policy that prohibited such activity, and actually specifying that employee use would be monitored and employees could be fired for violations, the manager never followed up with the information technology (IT) department, and therefore never discovered that the pornography was actually child pornography of the employee's stepdaughter. The Appellate Division permitted the stepdaughter to state a claim against the company.

Subsequent to the XYZ decision, which was somewhat surprising to the employment bar, we began counseling clients to be sure to enforce their policies, and pay attention to their employees' Internet usage both during work hours and with company computers. Fast forward to 2010. We now blog, tweet, Facebook, text, and instant message in the workplace on corporate equipment and outside of the workplace on company laptops and Blackberries. We of course still have personal emails, accessed either at work or on this same company-owned equipment. Moreover, the ability of employers, and their computer forensic experts, to monitor, access and retrieve employee electronic communications is increasingly more sophisticated.

Are employers now required to monitor all of this equipment and activity? Do they face liability if they do not monitor, as in XYZ? What about all of the other potential reasons employers

would want to monitor electronic communications, such as harassment issues, applicant checks, absenteeism problems, potential confidentiality breaches, and responses to production requests in litigation? How does privacy law, both common and statutory, such as the Stored Communications Act,² Genetic Information Nondiscrimination Act (GINA),³ or, for government employers, the Fourth Amendment, affect the monitoring requirements set forth in XYZ and the practical realities that employers face in this new era?

The Equal Employment Opportunity Commission (EEOC) has recently requested guidance regarding whether social media postings would fall under the "water cooler exception" to GINA, and whether the content of such postings is 'public' enough to provide employers with protection if they should inadvertently access employee's genetic information in a review of such postings. Despite such attempts at clarity, in employers' efforts to develop and enforce electronic communications policies while observing applicable privacy laws, the lines between 'public' and 'private' are far from clear.

Recent case law in both the United States and New Jersey Supreme Courts and in the New Jersey federal court has shed some light on how the courts are beginning to approach this area. These cases have uniformly held that employer rights with respect to monitoring and ownership of an employee's personal communications on a company-owned computer are not, in fact, limitless, despite language to that effect set forth in an employee handbook. Rather, each court applied a balancing test and

focused on whether the regulated conduct concerns terms and conditions of employment and reasonably furthers legitimate business interests. Generally, these courts concluded that employers do not have a legitimate business interest in the content of personal communications, but do have an interest in the fact that an employee is spending work hours engaging in business unrelated to the company, and certainly have an interest in ensuring that employees are not conducting illegal activity at the workplace.

In the recent and closely watched decision of *Stengart v. Loving Care Agency, Inc.*,⁴ the Supreme Court of New Jersey addressed whether a company's electronic communications policy gave the employer ownership of emails sent by an employee to her attorney, on a company-owned computer, via a private password-protected Internet-based email account.

Maria Stengart, a former executive director of nursing at Loving Care Agency, Inc., sued Loving Care for employment discrimination one month after her resignation. During her employment with Loving Care, Stengart was provided with a company laptop, from which she and her attorney exchanged emails using a personal password-protected Yahoo email account. Stengart did not save her password on the laptop, which she returned to Loving Care. In addition, the emails from her attorney bore the "standard hallmark" of attorney-client messages in the form of a warning that the emails were personal, confidential, and may be attorney-client privileged.⁵

Once Stengart filed suit, Loving Care sent her laptop to a forensics vendor, and had the vendor extract information from the computer which had been previously deleted, but still existed on its physical hard drive. Loving Care was then able to review emails previously sent by Stengart to her attorneys. During the discovery period, when it became evident that Loving Care had accessed and reviewed emails sent by Stengart to her attorneys, Stengart applied for a temporary restraining order. The trial court denied Stengart's application, concluding that Loving Care's electronic communications policy put Stengart on notice that her emails

would be considered company property given that they were sent on a company-owned laptop.

On appeal, the Appellate Division balanced Loving Care's right to impose reasonable regulations in the workplace against the attorney-client privilege, and found that the strong public policies underlying the employee's attorney-client privilege must prevail. By decision of March 30, 2010, a unanimous New Jersey Supreme Court modified and upheld the Appellate Division's judgment. The Court's holding drew on two principal areas: "the adequacy of the notice provided by the Policy and the important public policy concerns raised by the attorney-client privilege."⁶

The Court found Loving Care's electronic communication policy insufficient to allow its review of Stengart's emails in several ways. While the policy covered "all matters on the company's media systems and services at any time," it did not explicitly include the use of "personal, password-protected, web-based e-mail accounts via company equipment."⁷ The policy did not define "media systems and services" and did not at all address personal email accounts. Moreover, "the email system" referenced in the policy appeared to be the company email accounts.

In short, the Court concluded that, under the policy, "employees do not have express notice that the 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."⁸ The Court also noted that, while the policy provided that emails "are not to be considered private or personal to any individual employee" it ambiguously permitted "occasional personal use."⁹ In addition, the policy did not warn that emails sent via personal accounts were subject to forensic retrieval by the company.⁹

Based on the steps she took to keep her emails confidential, including use of her personal, password-protected account, and the omissions and ambiguities in Loving Care's policy, the Court concluded that Stengart had a reasonable expectation of privacy in the emails she exchanged with her attorney on Loving Care's laptop.¹⁰ Moreover, based on the nature of the emails, they were protected by the "venerable" attorney-

client privilege, "enshrined in history and practice."¹¹

The facts of another recent New Jersey case raise similar concerns about the risks to employers when accessing electronic information about their employees through social networking sites. In *Pietrylo v. Hillstone Restaurant Group*,¹² two servers at the Hillstone Restaurant Group began an invitation-only MySpace.com group for employees to "vent about any BS we deal with...(at work)."¹³ The MySpace forum included sexual remarks and used profanity toward company managers. One employee member of the forum showed the chat group page to a manager. When another manager asked the employee for her password to the forum, she gave it to him (though later claimed she was concerned about adverse action if she did not comply). When Hillstone Restaurant fired the servers who founded the forum due to the sexually inappropriate and derogatory content on the site, the servers sued, in part, for alleged violation of federal and state stored communications acts.

The jury ultimately found that Hillstone Restaurant's conduct in accessing the employees' password-protected MySpace forum violated the Stored Communications Act¹⁴ because the managers accessed the chat group without authorization from a forum user. The jury awarded the plaintiff employees over \$13,000, comprising back pay, as well as compensatory and punitive damages. The New Jersey District Court denied the company's motions for judgment as a matter of law and for a new trial.¹⁵

The court's holding in *Pietrylo* establishes that employers face significant liability when using information obtained from password-protected social networking sites to discipline or terminate employees, where that information is obtained without the requisite permission. The question left unanswered, of course, is what level of "authorization" must an employer have to access employee content on private social networking sites without fear of liability? While it would be ideal for an employer to obtain the password directly from the monitored subject and get his or her express consent to access the

site, it will not always be possible, particularly where the employee is trying to conceal his or her inappropriate, offensive, derogatory or disloyal comments.

One of the more interesting recent cases involving the intersection of employment law and electronic privacy issues involved a California police officer, Jeff Quon, who was spending large amounts of work time 'sexting' with his girlfriend and his wife on the pager supplied by his employer, the Ontario (California) Police Department. When his employer convinced the wireless company to allow them access to Quon's records, Quon, his girlfriend, and his now ex-wife all sued the city and the wireless company for violating their privacy rights.

In *Quon v. Arch Wireless Operating Company, Inc.*,¹⁶ the Ninth Circuit Court of Appeals ruled in favor of the plaintiffs, finding that they all had a reasonable expectation of privacy in their text messages and that Quon's employer could not view those messages without permission, even though they were made via department-owned equipment and during work time.¹⁷ While the city did not have a policy directed specifically at pagers, it did have a policy that provided the city with the right "to monitor and log all network activity including e-mail and Internet use" and that prohibited "inappropriate," "obscene," or "suggestive" language.¹⁸ Notwithstanding this notice, the Ninth Circuit found that there was an informal policy governing use of the pagers that undermined the stated written policy and created a reasonable expectation of privacy in the messages at issue.¹⁹

Quon's employer, the city of Ontario, California, appealed the Ninth Circuit's ruling to the Supreme Court of the United States.

The United States Supreme Court granted *certiorari* and decided the matter on June 17, 2010, in *City of Ontario, California, et al. v. Quon*.²⁰ Although much anticipated, the Supreme Court's decision in *Quon* unfortunately did not answer the question of whether or not the employees had a reasonable expectation of privacy in their text messages. The decision instead assumed, *arguendo*, the right to privacy,²¹ and then focused on the reasonableness of the

employer's search. The Court found that the search was reasonable because the employer had a legitimate purpose for it (testing the efficacy of the service plan) and it was limited in scope as it focused on a narrow time period and redacted certain information.²²

The decision is helpful and consistent with the guidance in all of the cases discussed here, insofar as it holds that a legitimate employer interest can override an employee's right to privacy. What the Court did not do, however, is provide the anticipated guidance to employers regarding the limits of what constitutes a legitimate employer purpose, or whether, if employees are given proper notice, employers can lawfully access employees' electronic communications made during work hours and/or while using company-owned equipment *without* a specifically stated purpose.

In light of these decisions, it is vital for employers to keep all company policies regarding electronic communications systems current with law and technology, and to adhere to them. The plaintiffs' initial win in the Ninth Circuit focused almost exclusively on the fact that the department's informal pager policy created a reasonable expectation of privacy for the plaintiffs, notwithstanding the written policy to the contrary.

In addition, employers should consider amending their electronic communications policies to specifically authorize the employer to review and access all electronic communications sent or received using any company-owned equipment, including but not limited to personal communications and communications on private, password-protected, web-based accounts. Employers also should ensure that the language in their policies is broadened to keep up with the ever-evolving technology their employees are using, and should be expanded to include, but not be limited to, texts, blogs, instant messages, social networking sites, tweets, and the like. Employers who intend to access information from social networking sites for employment-related purposes also need to determine how best to obtain authorization from the affected employees before accessing non-public information on those sites.

However, regardless of the breadth of any policy, employee communications with an attorney, even if on a company computer, should be treated as privileged until if and when a determination otherwise is reached.

The fast pace at which technology continues to grow and evolve will continue to present unique challenges to employers seeking to regulate and monitor electronic communications in the workplace. As employment counsel, we can protect our clients by staying current with legal and technological developments and proactively advising our clients. ■

Endnotes

1. 382 N.J. Super. 122, 887 A.2d 1156 (App. Div. 2005).
2. 18 U.S.C. § 2701.
3. P.L. 110 - 233.
4. 201 N.J.300 (March 30, 2010).
5. *Id.* at 309.
6. *Id.* at 314.
7. *Id.* at 311, 314.
8. *Id.* at 314.
9. *Id.* at 315.
10. *Id.* at 321.
11. *Id.* at 315 (citations omitted).
12. 2008 WL 6085437 (D.N.J., July 25, 2008).
13. *Id.* at * 1- 2.
14. 18 U.S.C. § 2701.
15. 2009 WL 3128420 (D.N.J., Sept. 25, 2009).
16. 529 F.3d 892 (9th Cir. 2008).
17. *Id.* at 906.
18. *Id.* at 896.
19. *Id.* at 906.
20. 130 S. Ct. 2619 (2010).
21. *Id.* at 2630.
22. *Id.* at 2631-2632.

Galit Kierkut is a partner with Greenbaum, Rowe, Smith & Davis LLP in Woodbridge. Suzanne Cerra is a partner with Nukk-Freeman & Cerra, P.C. in Short Hills. They both devote their practices to the representation of businesses in employment law matters.