BLANK ROME LLP
COUNSELORS AT LAW

www.BlankRome.com February 2010 No. 2

Whose E-Mail Is It Anyway? It Depends . . .

By Joseph G. Poluka and Michelle Gitlitz Courtney

In our earlier article *"Whose E-mail Is It Anyway,"*[1] we discussed whether the Fourth Amendment and/or the attorney-client privilege protects an employee's personal documents and e-mails stored on a company computer or sent through a company's network. Litigation in this area has continued apace–and now even the Supreme Court has stepped into the fray. One trend appears to be that the courts afford more protection to communications sent on a company computer through an employee's password-protected e-mail account such as Yahoo!, AOL, or Gmail.

Documents or e-mails created on or sent through a company computer may be confidential and/or privileged if the employee possesses a subjective expectation of confidentiality in those documents that a court finds objectively reasonable. Courts generally use a four-factor test (or some derivative thereof) to make this determination:

1. Is there a company policy banning personal use of company e-mail?
2. Does the company monitor the use of its e-mail?
3. Does the company have access to all e-mails?
4. Did the company notify the employee about these policies?

See In re Asia Global Crossing, Ltd., 322 B.R. 247, 257 (S.D.N.Y. 2005) (use of a company's e-mail system by an employee to send personal e-mails to the employee's counsel did not waive the attorney-client privilege);[2] *but see Kaufman v. SunGard Inv. System*, No. 05-cv-1236, 2006 U.S. Dist. LEXIS 28149 (D.N.J. May 10, 2006) (holding that employee had waived the attorney-client privilege by communicating with her attorney over a work e-mail system, where the company policy clearly notified employees that e-mails were "subject to monitoring, search or interception at any time . . . ."). Thus, the way in which a company drafts *and* implements its computer, e-mail, and Internet usage policy determines the degree of privacy an employee enjoys in his or her documents and e-mail.

In the much-publicized case of *Stengart v. Loving Care Agency, Inc.*, 973 A.D.2d 390 (N.J. Super. Ct. App. Div. 2009), the plaintiff was Executive Director of Nursing at Loving Care, Inc. ("Loving Care"), which provides home care services for children and adults, until she resigned in early 2008. Shortly thereafter, Stengart sued Loving Care alleging violations of New Jersey's Law Against Discrimination, including a hostile work environment that led to her constructive discharge. Prior to her resignation, Stengart communicated with her personal attorneys regarding an anticipated lawsuit against Loving Care using her password-protected Yahoo! e-mail account on a work-issued laptop. After Stengart sued Loving Care, the company extracted and created a forensic image of the laptop's hard drive and obtained Stengart's communications with her attorneys. During discovery, Stengart's attorneys learned that Loving Care possessed these e-mails and requested the identification and return of the e-mails and any copies. Loving Care's attorneys refused, and Stengart applied for a temporary restraining order. The trial judge denied Stengart's request, finding that the e-mails were not protected by the attorney-client privilege because Loving Care's electronic communications policy put Stengart on notice that her e-mails were viewed as company property.

The appellate court reversed, holding that the attorney-client privilege *trumped* Loving Care's electronic communi-

cations policy and, further, that Loving Care's counsel had acted unprofessionally in reading and refusing to disclose Stengart's privileged e-mails in violation of New Jersey Rule of Professional Conduct 4.4(b).[3] The case has now been argued on appeal to the Supreme Court of New Jersey, and we await a decision on whose interest is deemed paramount–the employer's, as the trial court found, or the employee's, as the appellate court found.

In another recent case involving the attorney-client privilege and electronic communications, *Convertino v. United States DOJ,* No. 04-0236, 2009 U.S. Dist. LEXIS 115050 (D. D.C. Dec. 10, 2009), Richard Convertino, a former federal prosecutor, contended that he had been wrongfully terminated by the DOJ after his high-profile terrorism convictions in Detroit were overturned for prosecutorial misconduct. Convertino sought e-mails written by Assistant United States Attorney Jonathan Tukel to Tukel's personal attorney from Tukel's DOJ e-mail account. Convertino believed that Tukel's e-mails would disclose the circumstances surrounding Convertino's firing. Tukel asserted the attorney-client privilege with respect to these e-mails. The court ruled that Tukel had a reasonable expectation of privacy in the e-mails, because the DOJ's policy did not ban the personal use of work e-mail, even though the policy stated that the DOJ had access to e-mails sent from its accounts. Of note was the fact that Tukel was unaware that the DOJ would regularly monitor his e-mails. *But see Alamar Ranch, LLC v. County of Boise,* No. CV-09-004, 2009 U.S. Dist. LEXIS 101866 at *11 (D. Idaho Nov. 2, 2009) ("It is unreasonable for any employee in this technological age . . . to believe that her e-mails, sent directly from her company's e-mail address over its computers, would not be stored by the company and made available for retrieval."); *Sims v. Lakeside Sch.,* No. C06-1412RSM, 2007 U.S. Dist. LEXIS 69568 at *2-3 (W.D. Wash. Sept. 20, 2007) (where the defendant advised all employees that they did not have a reasonable expectation of privacy in their company laptops, plaintiff's e-mails sent on the employer's e-mail account were not privileged; however, web-based e-mails sent by plaintiff to his counsel from the same laptop were protected by the attorney-client privilege).

Finally, in *United States v. Hatfield,* No. 06-CR-0550, 2009 WL 3806300 (E.D.N.Y. Nov. 13, 2009), a lengthy and complex decision, the court addressed, among other things, the privilege claims of defendant David Brooks relating to electronic communications between him and his personal and corporate counsel. A significant part of the decision concerns whether documents stored by Brooks on his office computer were privileged. In making its determination, the court (noting that there was no binding Second Circuit precedent) used a derivation of the four-factor test outlined in *In re Asia Global Crossing, Ltd., supra.* The court first focused on the company's policy regarding use of its equipment. The policy stated that employees were *expected* to use company equipment for business purposes only. Because the policy contained only an *expectation* that company equipment be used only for business purposes, however, the court held that the language in the policy was not strong enough to support a waiver of the attorney-client privilege. With respect to monitoring, although the policy indicated that the company was authorized to review and monitor an employee's hard drive and e-mail usage, the company did not do so in practice. The court held that this also weighed against any waiver of the privilege in documents stored on Brooks' work computer. However, the policy also stated that the company had the right of access to employee e-mails and files and, as CEO, Brooks was aware of that policy. The court then created a fifth factor–how the company interpreted its own policy with respect to the attorney-client privilege–which the court viewed as dispositive. The company's lawyer had testified that the policy was not intended to cause employees to waive the attorney-client privilege in documents stored on their computers. Thus, the court held that the documents on Brooks' computer were privileged. However, certain of Brooks' documents had "migrated" from his computer to other computers on the office network. The court ordered an evidentiary hearing to examine whether the privilege had been waived as to those documents.

Issues of electronic privacy have become so significant that they have reached the United States Supreme Court. The Supreme Court recently granted certiorari in a case involving the Fourth Amendment with respect to personal text messages sent by a police officer on his department-issued pager. *See Quon v. Arch Wireless Operating Co., Inc.,* 529 F.3d 892, 903 (9th Cir. 2008), *cert. granted, City of Ontario v. Quon,* No. 08-1332, 2009 U.S. LEXIS 9058 (U.S. Dec. 14, 2009). In *Quon,* the plaintiff police officer sent personal text messages to other officers and his wife from his department-issued pager, despite a business-use-only policy for the pager. When Quon and other officers exceeded their allotted usage limit, the city acquired text message transcripts from the pager provider and discovered that the officers had used the pagers for personal purposes. The officers and text message recipients sued the city, claiming an unlawful search in violation of the Fourth Amendment. The Ninth Circuit (reversing the trial court),

held that the officers and the text message recipients had a reasonable expectation of privacy because they did not expect that their text messages would be monitored or turned over to the police department by the text message service provider without their consent. Moreover, the officers relied on their supervisor's assurances that he would not monitor their text messages if the officers paid any overage charges. The Supreme Court granted the city's petition for *certiorari* on December 14, 2009. *See also United States v. Finley,* 477 F.3d 250, 259 (5th Cir. 2007) (defendant had a reasonable expectation of privacy in the call records and text messages on his employer-issued cell phone such that he had standing to challenge a search); *United States v. Heckenkamp,* 482 F.3d 1142, 1146-47 (9th Cir. 2007) (student had a reasonable expectation of privacy in information stored on his computer, despite a university policy stating that it could access his computer in limited circumstances while the computer was connected to the university's network); *United States v. Ziegler,* 474 F.3d 1184, 1189-90 (9th Cir. 2007) (employee had a reasonable expectation of privacy in a computer that was locked in his office, despite a company policy stating that computer usage would be monitored).

Although not litigation-proof, there are several steps employers can take if they wish to assert in litigation that personal documents and e-mails stored on a company computer or sent through a company's network belong to the company, and not the employee. First, employers should ensure that they have adopted a computer, e-mail, and Internet usage policy, and that every employee has executed an acknowledgement of receipt and understanding of that policy. Second, the policy should unequivocally state that all company-issued equipment (including laptops, desktops, servers, BlackBerries, pagers and cell phones), as well as all electronic communications (including e-mails, instant messages, and text messages) stored on, or communicated by or through, the employer's equipment or network, are the employer's property. The policy also should advise employees that the employer has the right to review any communications or files stored on its equipment, even if those communications or files are personal and were sent through an employee's password-protected e-mail account such as Yahoo!, AOL, or Gmail. Most importantly, employees should be advised that they have no expectation of privacy in any personal documents or communications sent through or stored on an employer's equipment or e-mail system. Whether or not the forthcoming *Quon* and *Stengart* decisions alter this advice remains to be seen. ■

1. *For the Defense* (June 2007), *reprinted in* PRIVACY & DATA SECURITY LAW JOURNAL, vol. 2, no. 9, at 775 (Aug. 2007).
2. Although *In re Asia Global Crossing* is a district court decision, it is widely viewed as the leading case on this issue.
3. Rule 4.4(b) forbids attorneys from reading documents that appear to have been inadvertently disclosed and states that attorneys must return such documents to whoever sent them.

White Collar, Internal & Government Investigations Practice Group

Philadelphia Office	Telephone	Washington, DC Office	Telephone
Ian M. Comisky	215.569.5646	Jane F. Barrett	202.772.5907
Norman E. Greenspan	215.569.5635	Jeanne M. Grasso	202.772.5927
Matthew D. Lee	215.569.5352	Gregory F. Linsin	202.772.5813
Joseph G. Poluka*	215.569.5624	Jennifer Peru Gary	202.772.5863
James T. Strawley	215.569.5664	Hardy Vieux	202.772.5997
New York Office	**Telephone**	Charles E. Wagner	202.772.5963
Jerry D. Bernstein	212.885.5511	Shawn M. Wright	202.772.5968
Laura A. Brill	212.885.5533	**Princeton, NJ Office**	**Telephone**
Michelle Gitlitz Courtney	212.885.5068	Nicholas C. Harbist	609.750.2991
James V. Masella III	212.885.5562	Stephen M. Orlofsky	609.750.2646
Inbal Paz	212.885.5010	John J. Pribish	609.750.2647
Marc Rothenberg	212.885.5121	*Editor	
Leonard D. Steinman	212.885.5524		