New York Law Journal

SERVING THE BENCH AND BAR SINCE 1888

Web address: http://www.nylj.com

VOLUME 234—NO. 69 FRIDAY, OCTOBER 7, 2005 ALM

OUTSIDE COUNSEL

BY MARK A. BERMAN AND AARON ZERYKIER

Are Private E-Mails Really Private?

In litigation between an employee and his or her former employer, the employer will often seek to recover materials stored on the former employee's computer or on its computer network, with the goal of uncovering e-mails or other electronic materials that could incriminate the employee or help the employer's case.

Even if relevant materials are found on the employer's computers, a court may suppress their use at trial or, if a preemptory motion is made by the employee to preclude such information's recovery, may not permit its retrieval by the employer.[1] While it may appear counterintuitive, it is not axiomatic that an employer will have "free reign" to utilize such materials in a litigation against a former employee.

Courts have expressed concern that an employer should not be able to sift through an employee's "private" documents stored at the office for incriminating evidence. Courts have suggested that "private" electronic materials, such as e-mails, deserve some level of privacy from an employer's review and/or use, notwithstanding that such materials, if relevant, may well be required to be produced to the employer if they had not been found on the employer's computers.

Privacy Concerns

The decisions below are illustrative of the privacy concerns courts have raised regarding "private" e-mails maintained on a company's computer, stored on a corporate e-mail system or reviewed with company resources.

In *Silverberg*, a law firm found that an attorney it had laid off had "password protected" an e-mail account, as well as files on a shared network hard drive. Plaintiff deciphered the passwords and accessed both the materials on the hard drive and the e-mail account. Based on the law firm's review of these materials, plaintiff alleged that defendant had been servicing his own clients while working for the law firm. Defendant, pursuant to CPLR §4506,[2] sought to suppress the use of this electronic information. In denying the motion to suppress, the court relied upon *Muick v. Glenayre Electronics*, 280 F3d 741 (7th Cir. 2002)[3] and noted that

Mark A. Berman *Aaron Zerykier*

Courts have expressed concern that an employer should not be able to sift through an employee's "private" documents stored at the office for incriminating evidence.

"[p]rotecting files with a password may not be used to bootstrap a privacy claim where (a) the recognized expectation is that none exists ["in the Fourth Amendment context, as a general proposition, areas within the employer's control do not have or create an expectation of privacy for employees"]; and (b) the act purportedly used to create it is wrongful to begin with." Id., at 3-4. The court found that accepting defendant's position would mean that:

> no employer can view the contents of an employee's computer without the consent of the employee. This would grant to the employee a level of privacy specifically rejected by the Seventh Circuit [in *Muick*] and contrary to the Supreme Court's elaboration of the reasonable expectation of privacy, *Ortega*, supra. The expectation of privacy for data placed on an office network computer hard drive shared by all personnel with access to it is inconsistent with any reasonable expectation of privacy. And, the subjective belief, based upon the unauthorized creation and use of an exclusive password, cannot create a reasonable expectation where none exists to begin with. The plaintiff did not do anything other than view files on its shared hard drive. Id., at 4-5.

'Cardace'

In *Cardace*, the plaintiffs sought, pursuant to CPLR §4506, to suppress certain e-mails and attachments that had been sent between them. The e-mails at issue were obtained by plaintiffs' employer from the company's network and included e-mails transmitted via both the company's network and noncompany e-mail accounts.

The court denied the motion to suppress the e-mails, finding, inter alia, that plaintiffs did not have an "expectation of privacy in their e-mails at work because they were transmitted on the companies' computers" and, even if they did, defendant's "legitimate business interest in protecting its employees from harassment in work place would likely trump plaintiffs' privacy interests." Id., at 4-5. The court stated that "e-mails…generated on a computer owned by [the company], recovered on [the company's] hard drive, and by utilizing [the company's] e-mail system, do not constitute the crime of eavesdropping." Id., at 5. The court further found that "[e]mails either made from the company e-mail system or to the computer e-mail system do not have a reasonable expectation of privacy." Id.

The court also rejected plaintiffs' motion on the grounds that the supporting "sworn affidavits of fact do not as a matter of law support the ground alleged." The court found that plaintiffs failed to specify which e-mails they wanted suppressed and failed to allege with specific facts how the e-mails allegedly had been manipulated. The court rejected the argument that the e-mails were obtained through a violation of the Fourth Amendment, finding that defendant was a private party acting on its own initiative. Lastly, the court found no violation of New York Penal Law 250.05.

Mark A. Berman *is a partner of Ganfer & Shore, LLP.* **Aaron Zerykier** *is an associate at the firm.*

When addressing whether to suppress the e-mails transmitted via noncompany e-mail addresses hosted by America Online and Optimum Online, the court denied suppression, but noted, with respect to a right to privacy relating to such e-mail addresses, that:

> [t]he e-mails between private e-mail services (such as AOL and Optimum Online in this case) might be treated differently. There is more of an expectation of privacy because a private e-mail service issues its own passwords. Here there is no evidence that the defendants used the plaintiff's AOL password in accessing AOL e-mail from the company's hard drive.

'Lacher'

In *Lacher,* plaintiff law firm, in a collection action against its former clients, sought to seal certain papers filed by defendants because in such papers the former clients submitted, inter alia, copies of e-mails "recovered from computers belonging to the defendants, which were used by [plaintiff's] personnel—allegedly during billable time—while the personnel represented defendants." Id., at 3. Plaintiff's expert averred that "plaintiff's personnel shared usernames and passwords during the months they used the computers at defendants' offices" and that defendants' representatives "had access at all times to all computers used by [plaintiff]." Id., at 6 n.4. In denying plaintiff's motion to seal, the court held that:

> it would seem that plaintiff's personnel—using computers that *belonged to defendants* and were *located in defendants' offices*—did not have a reasonable expectation of privacy for content on those computers. It is common knowledge that the content of shared computers can be viewed and recovered by anyone else who uses those computers. Plaintiff has not offered any evidence that would demonstrate that these computers were meant to be used for their personal business and e-mails, and that if this were the case, that such information was to remain private. Id., at 6. (emphasis in original)

'Asia Global'

In the recent case of *Asia Global,* the issue was whether executives' use of the company e-mail system to communicate with their personal attorney destroyed the attorney-client privilege, work product or joint defense privilege, where the executives and their former employer's trustee had become adversaries. Id., at 251. The court noted that the "prevailing view is that lawyers and clients may communicate confidential information through unencrypted e-mail with a reasonable expectation of confidentiality and privacy." Id., at 256. The court further noted that New York State has enacted laws that provide some protection to e-mail communications. See CPLR §4548. In *Asia Global,* the subject e-mails sent over the company-owned and -maintained computer system were communications between the company's executives and their personal attorney which "apparently concerned actual or potential disputes with the debtor." Id.

The court noted that it had not located any decisions that discussed the confidentiality of an employee's e-mails in terms of the attorney-client privilege, and therefore relied upon those cases addressing an employee's expectation of privacy "in company files and e-mails." Id. at 256-57. In determining whether employee e-mails or files should not be subject to production due to privacy concerns, the court considered four factors: "(1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails and (4) did the company notify the employee, or was the employee aware, of the use and monitoring policies?" Id. at 257.

The view in New York is that a privacy right to personal e-mails does not exist to the extent the transmission of the e-mail was via a corporate e-mail address....

In reviewing these factors, the court found that Asia Global had access to its own servers and any other part of the computer system where e-mails were stored; Asia Global did not require access to employee's offices or office computers to read the executives' e-mails, and "[i]n truth, sending a message over the debtor's e-mail system was like placing a copy of that message in the company files. Short of encryption, the [subject e-mails] could be reviewed and read by anyone with lawful access to the system." Id. at 259. The court further found that the evidence was equivocal regarding the existence or notice of corporate policies banning certain uses or monitoring of employee e-mails. Accordingly, the court found that it was unable to conclude, as a matter of law, that the executives' "use of Asia Global's e-mail system to communicate with their personal attorney eliminated any otherwise existing attorney-client privilege," and therefore granted preclusion. Id. at 261.

Conclusion

In sum, there are few reported New York cases addressing whether a privacy right exists to personal e-mails maintained on a corporate computer or network. The prevailing view in New York is that such a right does not exist to the extent the transmission of the e-mail was via a corporate e-mail address, but a court may view e-mails transmitted over a personal or "private" e-mail account differently, even if such e-mails are stored on a corporate computer or network. Finally, with respect to privileged e-mails, a high threshold may well need to be met before a court would order the production of such materials, even if the e-mails were transmitted over a corporate network. In either event, when seeking to review materials residing on a corporate computer or network, attorneys and their clients must be aware that such materials may be subject to a right to privacy and should be prepared to address potential motions that may be directed against the use of such materials.

1. See, e.g., *Lacher & Lovell Taylor v. Postnieks,* Index. No. 120807/03 (New York Co. Sup. Ct. May 19, 2005); *Cardace v. Hume,* Index No. 000077/02 (Nassau Co. Sup. Ct. July 1, 2003); *Silverberg & Hunter, L.L.P. v. Aaron Fe. Futterman,* Index No. 992976/02 (Nassau Sup. Ct. July 3, 2002) and *In re Asia Global Crossing, Ltd,* 322 B.R. 247 (S.D.N.Y. 2005).

2. CPLR §4506.1 provides in pertinent part that "[t]he contents of any overheard or recorded communication, conversation or discussion, or evidence derived therefrom, which has been obtained by conduct constituting the crime of eavesdropping, as defined by section 250.05 of the penal law, may not be received in evidence at trial...."

3. In *Muick,* the court held "[n]ot that there can't be a right to privacy ... in employer-owned equipment furnished to an employee for use in his place of employment. If the employer equips the employee's office with a safe or file cabinet or other receptacle in which to keep his private papers, he can assume that the contents of the safe are private. But [the employer] had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that [the employee] might have had." Id., at 743. The *Muick* court further noted that the "laptops were [the employer's] property and it could attach whatever conditions to their use it wanted to. They didn't have to be reasonable conditions...." Id.