New York Law Journal
UPDATE
CORPORATE
Thursday, May 3, 2007
ALM

CORPORATE CRIME

Privacy and Privilege In an Electronic Age

BY HOWARD W. GOLDSTEIN

Computers are ubiquitous in the workplace. Employer-supplied desktop and laptop computers are used by employees in the office, at home, and on the road to communicate via e-mail on topics ranging from routine scheduling to highly sensitive transaction details. Employees also use those computers for personal communication and Internet access. Employers' policies about such personal use, when they exist, vary from absolute proscription to gentle discouragement.

For years now, we have been in a legal business environment in which companies are expected to develop and maintain a "compliance culture" and to investigate and self-report criminal conduct and regulatory lapses if they are to avoid potentially catastrophic corporate liability. What is the impact of computer usage on the company's ability to implement this compliance culture? To what extent and under what circumstances can an employer search the computers it makes available to its employees, or the employees' personal computers connected to the employer's system? This article explores these issues.

Workplace Searches in General

The legal principles governing an employer's search of an employee's computer are an application of the principles generally applicable to searches in the workplace. With respect to public employers and employees, the issues arise in the context of the Fourth Amendment's prohibition of unreasonable searches and seizures. With respect to private employers and employees, the issues arise in the context of invasion of privacy claims. The analyses in both contexts, however, have been similar.

In *O'Connor v. Ortega*,[1] a doctor who had been terminated from his executive position at a public hospital brought a federal civil

rights action against the executive director of the hospital and others, claiming that his Fourth Amendment rights had been violated in connection with a search of his office. The office was not shared with anyone else, and contained primarily personal materials.

In analyzing the plaintiff's claim, the Supreme Court started from the premise that "Fourth Amendment rights are implicated only if the conduct of the Hospital officials at issue in this case infringed 'an expectation of privacy that society is prepared to consider reasonable.'"[2] The Court stated that this objective analysis was context specific and, therefore, had to "be assessed in the context of the employment relation" on a case-by-case basis.[3] It concluded that the plaintiff's subjective privacy expectation was objectively reasonable, given that he had stored personal papers in his office and file cabinets for 17 years and the hospital did not have any policies discouraging such practices, although the Court noted that the absence of such a policy could not by itself create a reasonable expectation of privacy. The Court remanded the case for the District Court to address the second step of the analysis—the reasonableness of the warrantless search.

Computer Searches

The *O'Connor* context-specific approach to analyzing whether an employee has an objectively reasonable expectation of privacy—the first step in assessing the lawfulness of a search—has since been applied by most courts assessing the legality of searches of computers in the workplace. In *Leventhal v. Knapek*,[4] the Second Circuit held that an employee of a state agency had a reasonable expectation of privacy in the contents of his office computer, after reviewing the "context of the employment relation" and the degree of access to the computer possessed and actually utilized by the company.[5] The court specifically noted that the employee had a private office and exclusive use of his computer, desk, and filing cabinet, without any evidence of access by others. The court also noted that the employer (1) had not "placed [plaintiff] on notice that he should have no expectation of privacy in the contents of his office computer"; and (2) did not have "a general practice of routinely conducting searches of office computers."[6] Despite finding a legitimate expectation of privacy in the computer files, the court concluded that the search was proper, as it was "justified at its inception and of appropriate scope" to address suspicions of employee malfeasance.[7]

Cases from other circuits make clear that the presence or absence of a corporate policy on employer access to an employee's computer is a critical factor in the courts' analysis of whether an employee has an objectively reasonable expectation of privacy in the contents of a workplace computer. Thus, in *United States v. Simon*,[8] a child pornography case involving Internet access by a government employee, the Fourth Circuit held that the employee did not have a reasonable expectation of privacy in light of the employer's internet policy. The policy stated that the employer would "audit, inspect and/or monitor" employee internet usage, including all Web sites visited, and "placed employees on notice that they could not reasonably expect that their internet activity would be private."[9] Similarly, in *United States v. Angevine,*[10] another child pornography case, the Tenth Circuit held that a professor at a state university did not have a reasonable expectation of privacy in his computer files given that the university policy—displayed on the computer screen when the computer was turned on—made clear that the computer and all the contents stored on the university's system were the university's property. The policy also reserved the right to the university to audit the computer's use on a periodic basis. The policy trumped the fact that the professor subjectively demonstrated an interest in keeping the materials confidential by attempting to delete them.

Howard W. Goldstein *is a partner at Fried, Frank, Harris, Shriver & Jacobson.* **Adam B. Gottlieb,** *an associate at the firm provide research assistance in preparation for this article.*

In *United States v. Slanina*,[11] the Fifth Circuit held that the employee had a subjective expectation of privacy because he password protected his computer, and that his expectation was reasonable in view of the fact that his employer had no policy and did not monitor usage. The court nonetheless upheld the search as a reasonable employment investigation into work-related misconduct. Finally, perhaps blurring the analytical lines, the Ninth Circuit in *United State v. Ziegler*[12] held that the employee had an objectively reasonable expectation of privacy in his computer files, but that the employer, by virtue of the fact that it maintained a right of access to workplace computers and actually monitored employee usage of their computers, could give valid consent to the search.[13]

The Impact on Privilege

It is, of course, axiomatic that the attorney-client privilege applies only to confidential communications. What is the impact, if any, of corporate policies giving the employer the right to monitor, and a proprietary interest in, an employee's e-mail and Web site usage of company computers? In the last couple of years, courts have begun to address this question.

In *In re Asia Global Crossing Ltd.*,[14] the issue was "whether an employee's use of the company e-mail system to communicate with his personal attorney destroys the attorney-client, work product or joint defense privileges in the e-mails..."[15] The Bankruptcy Court first noted that use of the corporate e-mail system between corporate agents involving company business, if otherwise privileged, retains the privilege, because "the prevailing view is that lawyers and clients may communicate confidential information through unencrypted e-mail with a reasonable expectation of confidentiality and privacy."[16] The question in the case before the court, however, involved communications with the employee's personal attorney concerning actual and potential disputes with the employer. Could the employee reasonably expect that those communications would be confidential?

In the absence of any authority directly dealing with this question, the court turned to the reasonable expectation of privacy cases in the workplace computer search context. From those cases, the court reasoned that the objective reasonableness of the employee's privacy/confidentiality expectation was dependent upon "the company's e-mail policies regarding use and monitoring, its access to the e-mail system, and the notice provided to the employees."[17] The court found that, although the company clearly had access to employees' e-mail, there was insufficient evidence that there was a clear corporate policy regarding the monitoring of employees' e-mail or banning certain uses of the system. Absent such evidence—such as the pop-up warning that greeted users of the court's system upon log-in—the court found the record inadequate to determine as a matter of law that any otherwise-existing attorney-client privilege had been waived.

In *Long v. Marubeni America Corp.*,[18] and *Kaufman v. Sungard Invest. Sys.*,[19] the courts found the records before them adequate and, in both cases, concluded that corporate policies destroyed any confidentiality expectation and vitiated any claim of privilege. In *Long*, the plaintiffs used "private," password-protected e-mail accounts. However, the company employee handbook made clear that (1) all computer communications transmitted, received or stored on company systems were property of the company; (2) use of the company's computers for personal reasons was prohibited; (3) the company had the right to monitor the computer system; and (4) employees had no right of personal privacy in any matter sent or stored over the company e-mail or internet systems. In *Kaufman*, the company used a computer technician to restore certain deleted files the plaintiff had copied before returning two laptops she had been provided by the company. Among the files were e-mails between the plaintiff and her attorney. The court found that any privilege had been waived because the company policy provided that (1) e-mail and information stored in company computers were company property; (2) all e-mails were subject to monitoring, even if protected with a password; and (3) employees should not expect that any material created with or stored on company property will remain private.

In contrast, in *Curto v. Medical World Communications, Inc.*,[20] the court, framing the issue as one of "inadvertent disclosure," found that privilege had not been waived. The court relied on the facts that (1) the laptop at issue was not connected to the company's computer servers when the employee was working at home and, therefore, could not be monitored; (2) plaintiff deleted her personal files prior to returning the laptop; and (3) the lack of enforcement of the company's computer usage policy created a "false sense of security" that the policy would not be enforced.

Conclusion

As the court noted in *In re Asia Global Crossing, Ltd.*, lawyers and clients generally may conduct privileged communications via unencrypted e-mail, and the risk of unauthorized disclosure does not, by itself, destroy the privilege. Indeed, in New York and California, the privilege is protected by statutes providing that the privilege shall not be lost "for the sole reason" that it is communicated electronically or because "persons necessary for the delivery or facilitation of such electronic communication may have access to the content..."[21]

However, as the cases discussed in this article make clear, the emerging judicial trend is to find privilege claims invalid when a corporate employee communicates with non-corporate counsel through the corporate e-mail system and the employer has a policy permitting the employer unfettered access to employee e-mail communications. Outside counsel representing a corporate employee should, therefore, caution their client not to communicate substantively with counsel via e-mail using the corporate system, even if it is through a personal account with an outside service provider. And counsel retained by a company to represent an employee in an investigation should at the outset ask the company for any corporate policies governing the use of corporate computers and the internet, rather than rely on their client's knowledge of whether such a policy exists and, if so, its contents. Finally, from the company's perspective, *Leventhal* and *Curto* are reminders that having a policy in place without enforcing it may be the same as not having a policy at all.

1. 480 U.S. 709 (1987).
2. Id. at 715.
3. Id. at 716-18.
4. 255 F.3d 64 (2d Cir. 2001).
5. Id. at 73-74.
6. Id.
7. Id. at 75.
8. 206 F.3d 392 (4th Cir. 2000).
9. Id. at 398.
10. 281 F.3d 1130 (10th Cir. 2002).
11. 283 F.3d 670 (5th Cir. 2002).
12. 474 F.3d 1184 (9th Cir. 2007).
13. See also, *Muick v. Glenayre Electronics*, 280 F.3d 741 (7th Cir. 2002) (employer policy, by itself, negated any privacy expectation); *Thygeson v. U.S. Bancorp*, 2004 WL 2066746 (D. Or. Sept. 15, 2005) (corporate policy negated privacy expectation in e-mails and in Web sites visited through corporate system); *Garrity v. John Hancock Mut. Life Ins. Co.*, 2002 WL 974676 (D. Mass. May 7, 2002) (corporate policy negated privacy expectation even though company instructed employees on how to create passwords and personal e-mail folders). But see, *Haynes v. Office of Atty. Gen. Phill Klin*e, 298 F. Supp. 2d 1154 (D. Kan. 2003) (corporate policy not sufficient to negate privacy expectation where employees were told how to create public and private files, given passwords, and there was no evidence of company monitoring private files).
14. 322 B.R. 247 (S.D.N.Y. 2005).
15. Id. at 251.
16. Id. at 256.
17. Id. at 259.
18. 2006 WL 2998671 (S.D.N.Y. 2006).
19. 2006 WL 1307882 (D.N.J. 2006).
20. 2006 WL 1318387 (E.D.N.Y. 2006).
21. N.Y. C.P.L.R. 4548 (McKinney 2007). See also, Cal. Evid. Code §917(b).