New York Law Journal

A NEW YORK LAW JOURNAL SPECIAL SECTION

ALM

INTERNET & THE LAW

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

MONDAY, SEPTEMBER 25, 2006

Where, Oh Where, Have My Employees Gone Online

If they're using company-provided computing devices, the courts often uphold employer monitoring.

BY MARTIN H. SAMSON

EMPLOYERS TODAY are increasingly taking advantage of technological developments to enhance worker productivity. Toward that end, they are furnishing employees with an ever-widening array of computing devices that go well beyond the ubiquitous personal computer. BlackBerry devices and laptops extend the workplace from the company's offices to the home and anywhere else an employee may be. These devices also extend the work day, allowing company business to be performed 24/7.

Companies have a host of reasons to monitor their employees' use of these devices, including the prevention of their misuse to further impermissible harassment, the protection of vital company information stored on such devices, and to ensure that company computers are used to achieve desired productivity, and not for personal activities. Indeed, a recent decision by a New Jersey intermediate appellate court, *Doe v. XYC Corp.*, 382 N.J. Super. 122, 126, 887 A.2d 1156, 1158 (App. Div. 2005) held that:

> an employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activities and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third-parties. No privacy interest of the employee stands in the way of this duty on the part of the employer.

Not surprisingly, company monitoring of employee computer use is widespread.

Notwithstanding their awareness of such monitoring, given the location of these devices, and the demands on their time, employees frequently use company computers for personal purposes. Employees use company devices to access personal e-mail accounts, and to communicate with their counsel. Important personal communications are stored in password-protected files located on company equipment. Employees also use the devices to surf the Web. Employees often have subjective expectations that many of these communications and activities will remain private.

As a result, efforts to monitor employee use of computing devices frequently result in lawsuits, either challenging the company's monitoring efforts, or seeking damages as a result thereof. This article will survey these lawsuits, discussing both the legal theories employees have advanced in their efforts to protect their communications, and the reception they have received in the courts. Based on this case law, we then offer advice to companies and employees wishing to avoid such suits in the future.

Hey, That Was Private!

Employees frequently resort to the Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986 (ECPA), in an effort to contest an unwanted examination of their communications. Two branches of the ECPA offer potential protection to employees.

Section 2511(1) of 18 U.S.C. prohibits the interception of e-mail "during transmission" from sender to recipient. *Eagle Investment Systems Corporation v. Tamm*, 146 F. Supp.2d 105 (D. Mass. 2001). This section "makes it an offense to 'intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral or electronic communication.'" *United States v. Councilman*, 418 F. 3d 67, 72 (1st Cir. 2005).

These provisions have been held to protect e-mail throughout its transmission, even if, at points in this process, the e-mail is temporarily held in storage pending the next leg of its journey. See e.g., *Councilman*, 418 F.3d at 85 ("We therefore conclude that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process, and hence that interception of an e-mail message in such storage is an offense under the Wiretap Act."); but see *Konop v. Hawaiian Airlines, Inc.*, 302 F. 3d 868, 878 n.6 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003).

Employees also attempt to assert claims under the branch of the ECPA commonly known as the Stored Communications Act, 18 U.S.C. §§2701 et seq. This section of the ECPA makes it a crime to "access [], without (or in excess of) authorization, an electronic communications service facility and thereby obtaining access to a wire or electronic communication in electronic storage. 18 U.S.C. §2701(a). Another provision bars electronic communications service providers from 'divulging to any person or entity the contents

Martin H. Samson *is a partner in the litigation and technology practices with Phillips Nizer.*

of a communication while in electronic storage by that service.' Id. §2702(a)(1)." *Councilman*, supra, 418 F. 3d at 81.

Employees also seek to prevent employers from accessing their e-mail communications by asserting that the employers' search constitutes an invasion of their right of privacy.

Public employees have rested such claims on the Fourth Amendment, which protects governmental employees against unreasonable governmental searches. To prevail on such a claim, the employee must establish both that he had an objectively reasonable expectation of privacy in the place searched, and that the search was unreasonable. A search is reasonable if it is both "justified at its inception" and of "appropriate scope." *Leventhal v. Knapek*, 266 F.3d 64, 75 (2d Cir. 2001).

Employees of private concerns cannot avail themselves of such claims, because of the absence of the requisite governmental search. See, e.g., *Muick v. Glenayre Elects.*, 280 F.3d 741 (7th Cir. 2002). Private employees have instead rested their claims on rights of privacy provided by state constitution, statute or common law.

A typical formulation of such a claim is found in *Thygeson v. U.S. Bancorp,* 2004 U.S. Dist. LEXIS 18863, *61 (D. Or. Sept. 15, 2004) where the court stated that "[i]n order to establish a claim for intrusion upon seclusion, a plaintiff must prove: (1) an intentional intrusion, physical or otherwise, (2) upon the plaintiff's solitude or seclusion or private affairs or concerns, (3) which would be highly offensive to a reasonable person." As with a claim under the Fourth Amendment, to prevail an employee must establish an objectively reasonable expectation of privacy in the place or matter searched.

ECPA Claims Often Fail

Employee claims challenging their employer's searches of the contents of the employee's company e-mail account, or e-mail the employee stored on a company device, under either the ECPA or the Stored Communications Act are unlikely to succeed.

The more likely claim is one advanced under the Stored Communications Act, where the employer searches an e-mail after it has been sent that is stored either on the company's servers or in the computer it assigned to the employee. Section 2701(c) exempts from the application of §2701(a) "seizures of e-mail authorized 'by the person or entity providing a wire or electronic communications service.'"

When the e-mail in question is sent from or to the company's e-mail system, the company is the provider of such an electronic communications service, and its search accordingly exempt from the statute's reach. See, e.g., *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 115 (3rd Cir. 2003) ("[W]e read §2701(c) literally to except from [the Stored Communications Act's] protection all searches by communications service providers. Thus, we hold that, because [employee's] e-mail was stored on [company's] system (which [company] administered), its search of that e-mail falls within §2701(c)'s exception to [the Stored Communications Act].").

Claims under the ECPA will likely fail, either because the interception was not contemporaneous with the e-mail's transmission (i.e. the e-mail was not intercepted in transit but rather recovered from storage) or because the employer's interception falls within a number of exceptions recognized in the Act. These include the business use exception,[1] the service provider exception[2] and the consent exception.[3]

Thus, in *Fraser*, supra, the Third Circuit affirmed the dismissal of ECPA claims arising out of a company's search of its servers for e-mails an employee had already sent because the search did not occur during the transmission of the e-mail. Said the court, "every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission;" see also *Konop*, supra, 302 F.3d at 877 ("'[I]ntercept' [requires] acquisition contemporaneous with transmission").

Right of privacy claims arising out of an employer's inspection of e-mail sent to or from a company e-mail account routinely fail if the company has a computer usage policy, of which the employee is aware, that informs employees that such e-mail, or indeed the company's devices, are subject to monitoring by company personnel.

Easy Right to Privacy Defense

Similarly, right of privacy claims arising out of an employer's inspection of e-mail sent to or from a company e-mail account routinely fail if the company has a computer usage policy, of which the employee is aware, that informs employees that such e-mail, or indeed the company's devices, are subject to monitoring by company personnel. This is true even if the employee has stored the e-mail in a password protected file, or a filed labeled "private."

Such computer usage policies have regularly been held sufficient to bar the employee from having a reasonable expectation of privacy in either e-mail sent over the company's computer network or the company computer assigned to the employee.

See e.g., *United States v. Ziegler*, 2006 U.S. App. LEXIS 20255, *20 (9th Cir. 2006) ("Employer monitoring is largely an assumed practice, and thus we think a disseminated computer-use policy is entirely sufficient to defeat any expectation [of privacy] an employee might nonetheless harbor."); *United States v. Simons*, 206 F. 3d 392, 398 (4th Cir. 2000), aff'd. without op., 246 F.3d 670 (4th Cir. 2001) ("[B]ecause of the FBIS' Internet policy, [defendant] lacked a legitimate expectation of privacy in the files downloaded from the Internet. … The policy clearly stated that FBIS would 'audit, inspect, and/or monitor' employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, 'as deemed appropriate.' This policy placed employees on notice that they could not reasonably expect that their Internet activity would be private.").

In *Garrity v. John Hancock Mut. Life Ins. Co.*, 2002 U.S. Dist. LEXIS 8343 (D. Mass., May 7, 2002) the court dismissed invasion of privacy claims arising out of an employer's review of e-mail sent and received by company employees over the company's e-mail system. The e-mail in question was located by the company in both personal password protected folders the employees maintained on the company's computers, as well as in the personal folders of other company employees who received e-mail from the plaintiff employees.

The company claimed that the plaintiffs regularly received on their office computers sexually explicit e-mails from Internet joke sites and others, which they then forwarded to co-workers via the company e-mail system. The court held that plaintiffs' invasion of privacy claims failed because they had no reasonable expectation of privacy in their personal folders, given the company's existing e-mail usage policy. In that policy, the company expressly reserved the right to "access all e-mail files."

The Court further held that such an expectation was lacking because some of the e-mail had been sent by plaintiffs to other company employees, with the expectation that they would be forwarded to third parties. Indeed, the plaintiff employees assumed that the recipients of their e-mails might forward them to others. Finally, plaintiffs had no reasonable expectation of privacy in the e-mails because, before they reached plaintiffs, they passed through portions of the company's system where others could view them.

In *Kelleher v. City of Reading*, 2002 U.S. Dist. LEXIS 9408 (E.D. Pa., May 29, 2002) the court dismissed invasion of privacy claims advanced by plaintiff Linda Kelleher, City Clerk of Reading, Pa., arising out of the defendants' alleged dissemination to the press of e-mails plaintiff sent and/or received from a City of Reading computer. The court held that Kelleher had no reasonable expectation of privacy in the subject e-mails because the City's computer usage policy expressly advised that the City could access and disclose e-mails sent from its computer network, a policy of which she was admittedly aware, having acknowledged receipt thereof in writing. More particularly, this policy provided that:

> Messages that are created, sent or received using the City's e-mail system are the property of the City of Reading. The City reserves the right to access and disclose the contents of all messages created, sent or received using the

e-mail system. The e-mail system is strictly for official City of Reading messaging.

In *Thygeson*, supra, the Magistrate Judge recommended dismissal of plaintiff employee's invasion of privacy claims, which arose out of his employer's review of both e-mails he had received and stored in a personal, non-password protected, folder on a company computer, as well as a list of Web sites the employee visited from his office computer. The e-mails in question contained nude pictures and sexually offensive jokes.

The court held that the employee had no reasonable expectation of privacy in the materials searched because the company had explicit policies advising its employees that company computer equipment could be monitored for any legitimate business purpose, including ascertaining whether the company computer had been improperly used for personal reasons or to send offensive e-mails, as was allegedly the case here.

These policies warned employees that the company "reserves the right to monitor any employee's e-mail and computer files for any legitimate business reason, including when there is a reasonable suspicion that employee use of this system violates…a company policy…Examples include…e-mails containing sexual innuendo or off-color jokes…or extensive or unauthorized use that violates Company policy."

Of like effect are the courts' decisions in *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002), cert. denied, 537 U.S. 845 (2002) and *Biby v. Bd. of Regents*, 419 F.3d 845 (8th Cir. 2005).

Company Computers @ Home

Courts have extended the reach of this doctrine to company computers used by employees in their own home.

A computer usage policy that warns the employee of the company's right to inspect computers provided to him for business use, has been held sufficient to entitle the company to inspect the contents of a company computer used by the employee in his home over the employee's objections. *TBG Ins. Services Corp. v. Superior Court*, 96 Cal. App. 4th 443, 452 (Cal. Ct. App. 2002) ("[Company's] advance notice to [Employee](the company's policy statement) gave [Employee] the opportunity to consent to or reject the very thing that he now complains about, and that notice, combined with his written consent to the policy, defeats [the] claim that he had a reasonable expectation of privacy."

Pursuant to this policy, employee "consented to have his computer 'use monitored by authorized company personnel' on an 'as needed' basis, and agreed that communications transmitted by computer were not private.") Id. at 446.

Courts have taken differing views when addressing the employee's right of privacy in the absence of a computer usage policy advising him of the company's ability to monitor.

Where Employer Has No Policy

Some courts have held that the knowing transmission of e-mail over a company e-mail system, by itself, destroys any expectation of privacy the employee may have therein.

See e.g., *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101 (E.D. Pa. 1996) ("[W]e do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."); *McLaren v. Microsoft Corp.*, 1999 Tex. App. LEXIS 4103 (Tex. App. Dallas May 28, 1999) (Court dismissed invasion of privacy claims, holding that employee had no reasonable expectation of privacy in e-mail stored on a company computer inside a password protected personal folder for the storage of e-mail supplied by Microsoft because such e-mail had first traveled through various points in Microsoft's company e-mail system, where it was accessible by Microsoft.).

When analyzing this question in the context of a criminal proceeding, however, courts have held that an employee has a reasonable expectation of privacy in the absence of both a company policy warning him that his computer could be monitored and a practice of routine monitoring.

See *Leventhal*, supra (Government employee held to have a reasonable expectation of privacy in an office computer located in his private office in light of the absence of both a computer usage policy advising him to the contrary, and a regular practice by his employer of searching the same); *United States v. Slanina*, 283 F.3d 670, 677 (5th Cir.), vacated on other grounds, 537 U.S. 802 (2002), on remand, 313 F.3d 891 (5th Cir. 2002) ("[G]iven the absence of a city policy placing [employee] on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer, we hold that [employee's] expectation of privacy was reasonable."

In the latter case the employer sought to examine an office computer located in the employee's private office, on which he had placed various passwords to limit access to files located thereon.[4]

In *Konop*, supra, the court let plaintiff employee proceed with claims that his employer violated the Stored Communications Act by accessing a secure password protected Web site the employee created to oppose various labor concessions sought by his employer. The Web site was not open to management employees. Nonetheless, a vice president of the employer had, with the permission of two employees permitted to use the site, used their identities to access it.

The Stored Communications Act excepts from liability "conduct authorized…by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. §2701(c)(2). The employer argued that its accessing of the Web site was authorized by employees who themselves were permitted to access it, and hence not a violation of the SCA.

The Ninth Circuit held that issues of fact precluded it from resolving this issue at that time. To be a "user" permitted to grant a third party such access, the "user" must both "use[] the service and [be] duly authorized to do so." Because there was no evidence that at least one of the employees who had granted management access had in fact used the site at issue, the court denied the employer's motion for summary judgment.

In *O'Brien v. O'Brien*, 899 So.2d 1133 (Dist. Ct. App. Fla. 2005), the court held that the unauthorized use of a spyware program by a wife to capture screen shots of her husband's online communications violated Florida's Security of Communications Act, modeled after the Wiretap Act. These online communications included chat conversations, instant messages and e-mails sent and received by the husband.

An intermediate Florida appellate court accordingly affirmed the trial court's decision to bar the wife from introducing these screen shots into evidence in her divorce proceeding. While obviously not a dispute between employee and employer, *O'Brien* can be relevant in addressing privacy interests in the absence of a computer usage policy consenting to monitoring.

In the absence of such a computer usage policy, the courts likely will be guided by the Supreme Court's admonition in *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987) that "given the great variety of work environments…the question whether an employee has a reasonable expectation of privacy must be addressed on a case by case basis."

Here Be Much More Careful

When it comes to searches of personal e-mail accounts that have been accessed from company devices, companies must tread far more carefully.

Copies of e-mails transmitted to and from a personal e-mail account, via a company's Internet connection, are not typically stored on a company's e-mail system. Rather, copies are stored on the servers of the third party e-mail provider. This differs significantly from the typical company e-mail system, where back-up copies are maintained on company servers.

Moreover, company policies typically do not specifically address the monitoring of personal e-mail accounts. In the absence of such policies, courts have been reluctant to dismiss employee claims arising out of the company's access to personal e-mail accounts.

In *Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp.2d 914 (W.D. Wisc. 2002), the court allowed plaintiff to proceed with claims advanced against his employer and various fellow employees under both the Stored Communications Act and Wisconsin's right to privacy statute, Wis. Stat. §895.50. These claims arose out of defendants' review of e-mails contained in a personal e-mail account plaintiff maintained with Hotmail, which account plaintiff had accessed from his work place.

As part of an investigation into workplace misconduct, the employer hired an expert who accessed the employee's personal e-mail account

and reviewed e-mail contained therein by guessing the account's password. The court denied the employer's motion for summary judgment, finding that "it is disputed whether accessing plaintiff's e-mail account is highly offensive to a reasonable person and whether plaintiff's e-mail account is a place that a reasonable person would consider private." Id. at 928.

Similarly, the court did not dismiss the employee's Stored Communications Act claim, noting that if defendants did indeed view the contents of plaintiff's Hotmail account "they would have obtained plaintiff's e-mail in violation of the act." Id. at 926.

Similarly, in *Campbell v. Woodard Photographic, Inc.*, 2006 U.S. Dist. LEXIS 36680 (N.D. Ohio June 7, 2006), plaintiff employee's invasion of privacy claim arising out of the manner in which his employer obtained information about plaintiff's activities on eBay survived a motion for summary judgment. Issues of fact existed as to whether defendant obtained this information by accessing plaintiff's password-protected eBay account, which, the court held, in the absence of an appropriate computer usage policy, could give rise to an invasion of privacy claim.

See also *Thygeson*, supra, 2004 U.S. Dist. LEXIS 18863 at *75 ("[A]n employee might have a reasonable expectation of privacy in the content of the actual e-mails he accesses and sends using a private internet e-mail account. On the other hand, this expectation of privacy might be nullified by explicit employer policies on computer use and monitoring.")

Of course, if the employee elects to store e-mails received from his personal e-mail account on his company computer, the analysis becomes far easier. In such circumstances, such a file would be treated as any other file the employee placed on his computer, whether marked private or password protected. In the face of a computer usage policy permitting monitoring of company devices of which the employee is aware, an invasion of privacy claim will fail.

Privileged Communications

Employees have also battled their employers to preserve the confidentiality of communications with personal counsel conducted over company e-mail systems or devices. The courts that have addressed this issue to date have held that the mere transmission of such e-mails over company systems, or from company devices, does not waive the attorney client privilege. However, that is not the end of the inquiry.

In *Curto v. Medical World Communs*, 2006 U.S. Dist. LEXIS 29387 (E.D.N.Y. May 15, 2006), the court held that an employee did not waive any attorney client or work product privileges that may exist in various e-mail communications with her personal counsel that she transmitted to and from her personal AOL e-mail account by using a company laptop to send them from her home. Plaintiff's employer had obtained these e-mails by "restoring" deleted files stored on the hard drives of these company laptops, which plaintiff employee had returned to the company.

The court reached this result notwithstanding the fact that the company had a computer usage policy, of which the employee was aware, that warned employees that they had no right of privacy in company computer equipment, the contents of which could be inspected by the company.

The district court analyzed this question as an inadvertent production of privileged materials, balancing five factors: "[1] the reasonableness of the precautions taken by the producing party to prevent inadvertent disclosure of privileged documents; [2] the volume of discovery versus the extent of the specific disclosure [at] issue; [3] the length of time taken by the producing party to rectify the disclosure; [4] the overarching issue of fairness;" and [5] "whether or not there was enforcement [by the employer] of any computer usage policy." Id. at *7.

Analyzing these factors, the court held that no waiver had occurred. The court was influenced by the fact that "Plaintiff's laptops were not connected to [employer's] computer server and were not located in [employer's] offices; thus [employer] was not able to monitor Plaintiff's activity in her home-based laptops or intercept her e-mails at any time." Id. at *17.

This issue was also addressed in *In re: Asia Global Crossing, Ltd.*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005). There, the court held that the use of a company's e-mail system by an employee to send personal e-mails to the employee's personal counsel does not, without more, waive any attorney client privilege in such communications. Whether a waiver had occurred must instead be resolved by examining the employee's subjective and objective expectations that the communications would be confidential.

In analyzing this question, the court looked for guidance to many of the cases that address an employee's privacy rights in e-mail sent over company e-mail system discussed above, which, as shown earlier, hinge on the resolution of a similar question—the reasonableness of an employee's expectation of privacy in such e-mails. Issues of fact as to the existence and application of company computer usage policies, and whether employees were warned that the company could inspect e-mails sent over the company's system, prevented the court from resolving the issue.

Contrary to *Curto*, the court indicated its decision would be strongly influenced by the terms of the company's computer usage policy. Said the court: "the objective reasonableness of that intent [to communicate in confidence] will depend on the company's e-mail policies regarding use and monitoring, its access to the e-mail system, and the notice provided to the employees."

Advice? Put It in Writing!

As seen by the foregoing, all the lawyers who have repeatedly urged companies to adopt a computer usage policy were correct.

If you want access, adopt a policy in which you tell your employees explicitly what you're going to do, and then do it. Advise employees they have no expectation of privacy in either their e-mail, or any company devices, whether used in or out of the office. Install automatic monitoring devices that monitor in-bound and out-bound communications for areas of concern.

The policy should further advise that all e-mail sent over the company's system is owned by the company, and may be used and disclosed as the company sees fit. E-mail is to be used for company, and not personal, purposes, and may not be used for improper or inappropriate activities.

And if you want to access personal e-mail or online accounts, be sure to expressly advise your employees of your right to do so, and to obtain their consent. As stated by the court in *TBG Insurance Services*, supra, 96 Cal. App. 4th 443 at 451-452 (citations omitted):

> [E]mployers are told they "should establish a policy for the use of e-mail and the Internet which every employee should have to read and sign. First, employers can diminish an individual employee's expectation of privacy by clearly stating in the policy that electronic communications are to be used solely for company business, and that the company reserves the right to monitor or access all employee Internet or e-mail usage. The policy should further emphasize that the company will keep copies of Internet or e-mail passwords, and that the existence of such passwords is not an assurance of the confidentiality of the communications. An electronic communications policy should include a statement prohibiting the transmission of any discriminatory, offensive or unprofessional messages. Employers should also inform employees that access to any Internet sites that are discriminating or offensive is not allowed, and no employee should be permitted to post personal opinions on the Internet using the company's access, particularly if the opinion is of a political or discriminatory nature."

For employees, the advice is simple. If you want your communication to be private, do not send it over your company's computer system, or over a company device. While you may defeat your employer's attempts to obtain such communications, odds are, in the face of a well-crafted computer usage policy, you will not.

1. See 18 U.S.C. §2510 (5)(a).
2. See 18 U.S.C. §2511 (2)(a)(i).
3. See 18 U.S.C. §2511 (2)(d).
4. It should be noted that in both *Leventhal* and *Slanina*, notwithstanding the courts' findings of a reasonable expectation of privacy, the governmental searches survived Fourth Amendment challenges because they were reasonable.