

January 2004 What Would You Do?

On the printer, you find an e-mail that employee Tina Traitor wrote to one of your competitors. In the e-mail, Tina tells the competitor that some of your company's customers are dissatisfied and asks if the competitor would be interested in obtaining more information. As a result of this e-mail, senior management wants to search Tina's computer, including her e-mails, to see if she has sent any confidential information outside the company. They want to be careful, however, not to violate any law. What Would You Do?

Over the last few years, the Internet and e-mails have become essential tools in conducting an effective business. Their prevalence, however, is not without employment concerns. One of the most common of these concerns is how to balance the employer's desire to protect against inappropriate use of its computer system with the employees' privacy interest in information that is viewed or sent over the Internet. By asking for your guidance in conducting a search of Tina's computer, your management is essentially asking you how to properly manage this balance.

To assist your company in conducting a search that will meet its goal of determining whether Tina has sent confidential business or customer information outside the company but not create a legal quagmire, there are two primary legal issues that you should consider: (1) statutory rules regarding interception of electronic communications; and (2) Tina's privacy rights.

The Electronic Communications Privacy Act

The Electronic Communications Privacy Act ("ECPA"), which amended the federal wiretapping act to protect e-mail users, constitutes the primary statutory limitation on an employer's freedom to monitor employee e-mail use. Employees who claim that a company's search or monitoring of their computers or e-mails violates the ECPA generally rely on either: (1) the ECPA's Interception prong; or (2) the ECPA's Stored Information prong.

A. ECPA Title I – Interception of Electronic Communications

Title I of the ECPA prohibits unauthorized "intercepts" of electronic communications, which includes receiving or monitoring an employee's privately owned e-mail or internet properties. 18 U.S.C. § 2511(1)(a). Courts, however, have rarely found employers liable under the ECPA for an unauthorized interception of an electronic communication.

1. Courts hold that interception must be contemporaneous with transmission.

Most frequently, courts deny ECPA interception claims by narrowly interpreting the word "intercept" to mean an interception that occurs contemporaneously with transmission. The Fifth Circuit was one of the first Appeals Courts to reach the conclusion – holding that stored e-mails

could not be intercepted within the meaning of the ECPA because there was no contemporaneous acquisition of the information. *Steve Jackson Games v. U.S. Secret Service*, 36 F. 3d 457 (5th Cir. 1994). Although noting that the conclusion that stored e-mails cannot be intercepted does not fit with Congress' intent of protecting e-mail, the Third Circuit recently followed the Fifth Circuit's conclusion and held that an employer could not be liable under the ECPA for retrieving stored e-mails. *Fraser v. Nationwide Mutual Ins. Co.*, No. 01-2921 (3rd Cir. Dec. 10, 2003).

Based on these cases, if your company merely views Tina's stored e-mails and other information on her computer, you should have protection from liability under the ECPA interception prong.

2. The ECPA contains 3 applicable exceptions to the prohibition against interception of e-mails.

In addition to the case law holding that the ECPA only prohibits contemporaneous interception of an e-mail transmission, the ECPA provides three exceptions that could apply to your review of Tina's e-mails: (1) the provider exception; (2) the ordinary course of business exception; and (3) the consent exception.

a. Provider Exception

The ECPA provider exception allows network providers to intercept, disclose or use employee e-mail if the interception is within the ordinary course of business and is either: (1) necessary to the rendition of service or (2) necessary to protect the rights or property of the company. 18 U.S.C. § 2511(2)(a)(1). Under this exception, employers who provide their own e-mail systems on employer owned and operated computers may be exempt from liability for perusing and disclosing e-mail communications of employees.

In Tina's case, your company's justification for conducting a search is protection of the company's rights and property (customer information and other confidential business information). Therefore, if your company administers its own e-mail system, it likely can rely on the provider exception in searching Tina's computer.

b. Ordinary Course of Business Exception

When a device is used to intercept e-mail communications, the ECPA also provides an exception for use that is in the ordinary course of business. 18 U.S.C. § 2510(5)(a). Although courts have most often applied this exception when companies eavesdrop on telephone communications, the same principles apply to e-mail and internet monitoring. In the context of telephone

interceptions, courts have generally taken one of two approaches in determining whether the ordinary course of business exception applies:

- (1) The content approach – allowing employers to monitor “business-related” communications but prohibiting monitoring of personal communications; and
- (2) The context approach – allowing an employer to monitor its employees’ communications if it has a legitimate business reason for doing the monitoring.

Thus, if you limit the scope of your search to information that relates to the possible transfer of confidential business and customer information outside your company, and, during the search, you avoid viewing any personal information, you likely have another defense to a ECPA interception claim.

c. Consent Exception

An interception of e-mail does not violate the ECPA if the person who intercepts the e-mail is a party to the communication or if one of the parties to the communication consents to the interception. 18 U.S.C. § 2511(2)(d). If your company has a policy that allows it to monitor e-mails and Tina acknowledged her agreement to the policy by signing it, you probably have another defense to ECPA interception liability. If you do not have such a policy (or to be extra cautions even if you do), you might consider asking for Tina’s written consent before searching her computer.

B. ECPA Title II – Stored Communications

Title II of the ECPA bans unauthorized access to stored electronic communications. 18 U.S.C. § 2701(a). When employers review stored information on an e-mail system, some employees have argued that the review violates this Stored Communication portion of the ECPA. This portion of the ECPA, however, has an exception for seizure of e-mail authorized by the person or entity providing the e-mail service. Based on this language, at least one circuit court has held that companies who have their own e-mail systems are excepted from the ban on retrieving stored e-mails. *See Fraser v. Nationwide Mutual Ins. Co.*, No. 01-2921 (3rd Cir. Dec. 10, 2003)(company search of e-mails stored on its own system, which it administered, fits within exception).

Based on existing case law, if you retrieve Tina’s stored e-mails you should be protected from ECPA liability. Again, however, having a policy and Tina’s signature accepting the policy or a written consent to the actual search will make your defense even stronger because you can argue that the search was authorized.

Privacy Expectation

Recognizing the difficulty in successfully bringing a statutory claim for violation of e-mail privacy, employees have been turning to the common law cause of action for invasion of privacy. Thus, in evaluating whether your company can search Tina's computer and what parameters you should set on any such search, you should also consider the possible ramifications under privacy law.

A. Privacy Factors

In evaluating whether a particular search creates a privacy concern, courts generally look at the following factors:

- (i) whether the employee has a legitimate expectation of privacy in the thing searched (in this case, Tina's computer);
- (ii) whether the employer has provided advance notice of the intent to search;
- (iii) whether the employer has a good reason for the search; and
- (iv) whether the employer has conducted the search in a reasonable manner.

B. Privacy Case Law

Fortunately for employers, the majority of the lawsuits alleging invasion of privacy based on review of an employee's work computer have been unsuccessful. In *Smyth v. Pillsbury Co.*, for example, Smyth was terminated for transmitting inappropriate and unprofessional comments over the e-mail system. 914 F.Supp. 97 (E.D. Pa. 1996). Although the company had actually assured employees, including Smyth, that e-mail would remain confidential and privileged, the court found that Smyth did not have a reasonable expectation of privacy in his e-mails. The court reasoned that any expectation of privacy disappeared when the employee voluntarily sent e-mail to a second person over the company computer system. The court further concluded that a reasonable person would not consider the employer's interception of those communications to be a substantial and highly offensive invasion of privacy. In the balance, the court concluded that "the company's interest in preventing inappropriate and unprofessional comments or even illegal activities over its e-mail system outweighs any privacy interest the employee may have in his e-mail comments."

The Dallas Court of Appeals reached a similar conclusion in *McLaren v. Microsoft Corp.*, No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103, at *11-12 (Tex. App.--Dallas, May 28, 1999, no pet. h.)(unpublished). At issue in that case were e-mails that the employee kept in "personal

folders” and used a personal password to retrieve. Despite the employee’s steps to keep the e-mails confidential, the court found that the employee did not have a reasonable expectation of privacy in the e-mails. The court observed that the e-mails were sent from a company workstation, which included a company-owned computer that was provided so that the employee could perform his job. The court, therefore, found that e-mail messages saved on that company computer were not the employee’s personal property, but were an inherent part of the office environment, the Company’s property. The court concluded further that a reasonable person would not have found the interception of these communications to be highly offensive. Following *Smyth*, the court explained that a company’s interest in preventing inappropriate, unprofessional or illegal activities over its e-mail system outweighed any privacy interest that an employee might have in the e-mail contents.

These cases suggest that if you search Tina’s company computer for information sent over the Company’s system, you will probably not implicate any privacy concerns. As noted previously, however, you should not throw caution to the wind in conducting your search of Tina’s computer.

What Should You Do

It appears that current federal law, as well as state statutory and common law, favors the employer when it comes to e-mail monitoring in the workplace. Based on the existing case law, therefore, you are probably justified in searching Tina’s computer to determine whether she has sent any confidential information to your competitor. You should note, however, that a sufficient body of case law does not yet exist to determine exactly how the courts will resolve future claims. Thus, you should proceed with caution in conducting your search.

A. Policies

Before discussing the recommended parameters of your search of Tina’s computer, it is important to note that there are some things that employers can do, in advance of an actual need to search, to place themselves in a better position when a situation like the one involving Tina occurs. For example, it is a good idea to have a written computer and internet policy that clearly states that computers and the e-mail system are company property and that they may be searched or monitored at any time. You should have employees sign that they have received and read this policy.

Some companies have also included provisions in their policies that ban employee use of third party email services, such as Yahoo and America Online, through the company’s network of computers. This strengthens the employers reliance on the “provider exception” to the ECPA ban on e-mail intercepts.

B. Conducting the Search

In addition to taking affirmative steps to protect yourself before you have the need to search an employee's computer or e-mails, there are precautions that you can take when you conduct an actual search that will put you in a more defensible position if the employee ever claims the search violated the law:

(1) You should only conduct searches for legitimate business reasons and you should conduct them in a nondiscriminatory manner;

(2) You should tailor any search to its limited business purpose. Thus, in Tina's case, you would search for any e-mails or other documents that show or suggest that Tina has sent confidential information to the competitor;

(3) You should limit the search to business information (i.e. if you determine that an e-mail is personal, stop reading it and do not save it);

(4) To protect against an ECPA interception claim, unless there is a strong business reason to catch e-mails immediately, you should limit your review to e-mails and information that have already been sent or received. Thus, you should avoid any temptation to eavesdrop on Tina's private cyberspace by logging on to her work site or otherwise capturing e-mails in route from Tina to the customer or any other intended recipient;

(5) It is probably best to have two members of management conduct the search and to document the business reasons that justify the search and the manner in which the search was conducted;

(6) Although not always possible, you may also want to notify Tina in advance that you are conducting the search, get Tina's written consent to perform the search and allow her to be present during the search.

Following these steps will afford the greatest level of protection to any legitimate employer search, while preserving employee dignity and privacy rights.