PROSKAUER ROSE®

Client Alert

A report for clients and friends of the firm

January 2004

Court Upholds Employer's Right to Search Worker's E-Mails

A company's decision to search e-mails of an employee stored in its main file server did not violate any provisions of the federal Electronic Communications Privacy Act or a parallel state electronic communications privacy law. Employers and employees should recognize that this latest ruling is one in a line of federal appellate decisions that give governmental and private authorities strong rights to search and review electronic communications. The case serves as the most recent reminder that employees have extremely limited privacy rights in electronic communications.

The Third Circuit Upholds Employer's Rights to Access Employee E-Mails

Following his termination on September 2, 1998, a former independent insurance agent for Nationwide Mutual Insurance Company ("Nationwide"), Richard Fraser, brought claims against the company for wrongful termination and damages in violation of the federal Electronic Communications Privacy Act of 1986 ("ECPA")[1] and the Pennsylvania counterpart to the ECPA.[2] Fraser served as an officer of the Pennsylvania chapter of the Nationwide Insurance Independent Contractors Association. Prior to his termination, the company learned that Fraser had drafted letters to two competitors expressing the trade association's dissatisfaction with Nationwide and inquiring as to whether the competitor companies would have interest in acquiring the policyholders of the trade association's agent members. Upon learning of the letters, Nationwide became concerned that Fraser might also be revealing company secrets to competitors. In response, Nationwide searched its main file server for any e-mails to or from Fraser that indicated improper behavior. Finding that information contained in Fraser's e-mails when coupled with the two letters constituted "disloyalty," the company terminated his employment.

Fraser argued that Nationwide's access to his e-mail without his express permission violated the ECPA and the parallel state statute because it constituted an unauthorized interception of electronic communications under the statutes.[3] Nationwide argued in response that it did not "intercept" Fraser's e-mail within the meaning of the statutes because the interception must occur contemporaneously with the original transmission of the message.[4] The trial court agreed with Nationwide's interpretation of the statutes, and ruled that no interception had occurred because the company did not access Fraser's e-mail until well after transmission. Fraser further argued that Nationwide had violated the ECPA and state statute provisions prohibiting unauthorized access to electronic communication that is in "electronic storage." The trial court dismissed this claim as well, holding that "electronic storage" for the purposes of the statutes applied only to "temporary, intermediate storage" or "backup" storage.[5]

On appeal, the United States Court of Appeals for the Third Circuit affirmed the trial court's statutory interpretation of "intercept," but used different reasoning to reach the same conclusion as to the "electronic storage" violation claim. The Third Circuit held that while the company's main file server could arguably be considered "backup storage" under the statutory framework, Nationwide's actions merited protection under the ECPA exception for "the person or entity

[1] 18 U.S.C. § 2510, *et seq.*
[2] 18 Pa. Cons. Stat. § 5702, *et seq.*
[3] *See Fraser v. Nationwide Mutual Insurance Co.*, No. 01-2921, at 8 (3d Cir., Dec. 10, 2003).
[4] *Id. at* 9.
[5] *Id. at* 11.

providing a wire or electronic communications service."[6] As the provider and administrator of the e-mail service, Nationwide was thus entitled to protection for all searches of e-mails stored in its system.

Prior ECPA Cases Involving E-Mail and Other Electronic Communications

As the Third Circuit noted in *Fraser*, every federal court of appeals that has interpreted the statutory language of the ECPA has held that the alleged interception must occur contemporaneously with transmission of the electronic communication. In *Steve Jackson Games, Inc. v. United States Secret Service*, the plaintiff publisher brought suit under the ECPA after the U.S. Secret Service seized the publisher's computer containing stored private e-mail messages belonging to the publisher and 365 bulletin board system customers.[7] Although the trial court ruled that the Secret Service's actions amounted to a violation of the ECPA provisions pertaining to "storage" of electronic communications, the court refused to award damages for violation of the "intercept" provisions because the interception did not occur contemporaneously.[8] On appeal, the United States Court of Appeals for the Fifth Circuit reviewed the statutory language and legislative history of the ECPA in finding that the clear language of the statute mandates that the interception must occur contemporaneously for a claim to lie under the ECPA.[9] Even though the Secret Service had confiscated the bulletin board messages before receipt by -- but subsequent to *transmission* to -- their intended recipients, the "intercept" provisions were not triggered because Congress intended for the "electronic storage" provisions of the ECPA to protect such occurrences.

In *Konop v. Hawaiian Airlines, Inc.*, a pilot sued his employer airline, alleging that officers of the airline had made an unauthorized interception of his partially secure bulletin board Web site under the federal Wiretap Act, a predecessor statute to the ECPA from which the ECPA definition for "intercept" came.[10] The plaintiff's Web site, accessible to airline employees who created a username and password, contained allegedly defamatory statements about company officers. A company vice president gained access to the site by asking an employee for use of his username and password. Upon learning of this, the plaintiff brought suit under various federal statutes, including the Wiretap Act. The United States Court of Appeals for the Ninth Circuit, in affirming the trial court's decision that no interception had occurred, ruled that even in the context of a somewhat secure bulletin board site such as the plaintiff's, the defendant must "intercept" the communication in a contemporaneous manner in order for the plaintiff to maintain a claim for damages. Otherwise, the defendant's actions merely amount to "gained access" of the communications, which is not actionable under the intercept provisions of the Wiretap Act or the ECPA. Notably, the Ninth Circuit reasoned that when Congress recently passed the USA PATRIOT Act, it amended the ECPA to include the contemporaneous requirement to voice mail communications, thereby implicitly approving of the narrow judicial interpretation of "intercept" that requires contemporaneous action.[12]

Finally, in *United States v. Steiger*, the United States Court of Appeals for the Eleventh Circuit ruled that a tip from an anonymous source leading to the defendant's arrest and convictions for sexual exploitation of children and possession of child pornography did not violate the "intercept" provisions of the Wiretap Act or the ECPA.[13] The Eleventh Circuit found no evidence to suggest that the information provided by the source was obtained in a contemporaneous manner, finding that "very few seizures of electronic communications from computers will constitute 'interceptions.'"[14] The court went on to note that in an employment context, "unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of e-mail within the prohibition of [the Wiretap Act] is virtually impossible."[15]

Ramifications for Employers and Employees

As the recent decision in *Fraser* and previous decisions across the country indicate, employees forfeit a significant amount of their privacy rights when using electronic communication that is either administered by or accessible to their employers. The recent passage of the USA Patriot Act confirms that reality, as well as placing further constraints on other forms of communication, such as voice mail. Conversely, employers gain considerable rights to legally search and review employee electronic communications, such as e-mail, that are facilitated through company owned and administered systems.

---

6 *Id.* at 11.

7 *See Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 458 (5th Cir. 1994).

8 *Id.* at 459-60.

9 *Id.* at 461-62.

10 *See Konop v. Hawaiian Airlines, Inc.*, 302 F. 3d 868, 872 (9th Cir. 2002).

11 *Id.* at 878-79.

12 *Id.* at 878.

13 *See United States v. Steiger*, 318 F.3d 1039, 1041 (11th Cir. 2003).

14 *Id.* at 1050.

15 *Id. at* 1050 (quoting Jarrod J. White, *E-Mail at Work.com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1083 (1997)).

NEW YORK LOS ANGELES
WASHINGTON BOCA RATON
NEWARK PARIS

Client Alert

Proskauer's Computer Security Practice Group counsels clients on their obligations in the event of a computer security breach and the steps that may be taken to avoid or limit legal liability from potential computer intrusions. The following individuals serve as the contact persons and would welcome any questions you might have.

Christopher Wolf
202..416.6818 — cwolf@proskauer.com

Scott Cooper
310.284.5669 — scooper@proskauer.com

Proskauer Rose is an international law firm that handles a full spectrum of legal issues worldwide.

You can also visit our Website at **www.proskauer.com**