

New York Law Journal

Labor & Employment

©2009 INCISIVE MEDIA US PROPERTIES, LLC

An incisivemedia publication

WWW.NYLJ.COM

TUESDAY, MAY 26, 2009

BY MITCHELL BOYARSKY
AND JASON A. ZOLDESSY

IT IS generally recognized that an employer may review an employee's work e-mails without the employee's consent, particularly where the company maintains a written policy stating that work e-mail belongs to the employer. The policy should make clear that the employer may access and read employee e-mails at any time, for any reason, regardless of where the e-mails were written or received.

Whether employers in New York legally may review an employee's or former employee's e-mails, which were sent from or received through a personal e-mail account (such as Gmail or Hotmail), and accessed through a company-issued computer is not so clear.

Statutory Concerns

The federal Stored Communications Act (SCA) makes it unlawful to "intentionally access without authorization a facility through which an electronic communication service is provided and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage."¹ "Electronic storage" is defined as either: (1) "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"; or (2) "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."² Another federal law, the Electronic Communications Privacy Act (ECPA), prohibits a person from "intercepting" electronic communications.³ Both statutes provide for criminal sanctions and a civil cause of action.

While the U.S. Court of Appeals for the Second Circuit has not decided what types of employee e-mails are encompassed by the definition of "electronic storage" in the SCA, *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, decided in 2008 by a magistrate judge in the U.S. District Court for the Southern District of New York, found that an employer violated the SCA by reviewing an employee's private e-mail



ISTOCK/NYLJ

Are Employees' Personal E-Mail Accounts Off Limits?

Under current case law, employer caution is in order.

account maintained on a company computer.⁴

The magistrate's report, adopted by the district court, noted that a majority of courts that have addressed the issue have found that "e-mail stored on an electronic communication service provider's systems after it has been delivered, as opposed to e-mail stored on a personal computer, is stored communication subject to the SCA."⁵ The court held that the employer's conduct did not violate the ECPA, however, because it did not access the e-mail contemporaneously with the e-mail's transmission.

The employer in *Pure Power* viewed the employee's personal e-mail account, to which it had access because the employee left the username and password on the company computer. According to the employer, the account opened automatically when the Hotmail Web site was accessed. Since the e-mail being accessed was not company e-mail, the court concluded the employer's electronic communications policy was no defense to the unauthorized access allegation.

In contrast to the 2008 decision, a 2007 case, *Rozell v. Ross-Holst*, also decided by the district court for the Southern District of New York, held that e-mails already in storage were covered by the ECPA.⁶ Here, the plaintiff brought claims against her former employer and its CFO for, inter alia, hacking into her AOL e-mail account (maintained for her by the employer) and taking sensitive information. The court disagreed with the employer's argument that the ECPA did not apply to e-mails accessed while in post-transmission storage.

Based on the state of the case law, an employer acts at its peril in accessing an employee's private e-mail account even if the employee had used a company-provided computer.

Penalties

Under the SCA, a person may seek: (1) such preliminary and other equitable or declaratory relief; (2) actual damages, but in no cases less than \$1,000; and (3) reasonable attorney's fees and other litigation costs reasonably incurred.⁷

MITCHELL BOYARSKY is a partner with the Morristown, N.J., office of Jackson Lewis and formerly assistant general counsel with the New York City Mayor's Office of Labor Relations. JASON A. ZOLDESSY is an associate in the New York City office of Jackson Lewis.

Punitive damages also can be awarded for a willful or intentional violation.

Moreover, the SCA provides for criminal penalties. For first-time violations not committed for a specified improper purpose (that is, not committed "for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act"), the penalty can be as much as 1 year imprisonment and a \$100,000 fine.⁸

For repeat violations not committed for an improper purpose, and for first-time violations committed for an improper purpose, the maximum penalty is 5 years' imprisonment and a \$250,000 fine.⁹

For repeat violations committed for an improper purpose, the maximum penalty is 10 years' imprisonment and a \$250,000 fine.¹⁰

Right-to-Privacy Concerns

Privacy concerns based on state common law also may be implicated when accessing an employee's personal e-mails. While no New York court has defined an employee's right to privacy in e-mails sent or received using a personal e-mail account on a company-issued computer, cases interpreting the attorney-client privilege and its application to communications sent using a company-provided computer provide some guidance.

For instance, in *Pure Power*, the district court found that the employee had a reasonable subjective and objective belief that his communications with his attorney using his Hotmail account would be kept confidential. Therefore, the court concluded that certain e-mails meeting the definition of an attorney-client communication were protected by the attorney-client privilege.¹¹

In a 2006 case, the U.S. District Court for the Eastern District of New York in *Curto v. Medical World Communs. Inc.* addressed whether the former employee had waived her right to assert the attorney-client privilege and work product immunity over documents retrieved from company-owned laptop computers used by the plaintiff during her employment.¹² The plaintiff worked primarily out of a home office and was assigned company equipment to use at her home. The employee sent e-mails to her attorney from a personal AOL account which did not go through the company's servers. After her termination, the company forensically analyzed her computer and obtained the communications between the employee and her attorney.

While the court did not specifically decide whether the company had the right to search through the personal e-mails, it found that the employee did not waive the right to assert the attorney-client privilege and work product immunity in connection with documents retrieved from her laptop, in large part because the company did not enforce its computer usage policy. The court limited its holding to whether an employee's use of a company-owned computer in her home waived the privilege and "does not purport

to address an employee's right to privacy in an office computer in general."

The court applied the following four-factor test to determine an individual's expectation of privacy in e-mails:

- (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 corporation notify the employee, or was the employee aware, of the use and monitoring policy?

The court in '*Pure Power Boot Camp v. Warrior Fitness Boot Camp*,' noted that a majority of courts that have addressed the issue have found that 'e-mail stored on an electronic communication service provider's systems after it has been delivered, as opposed to e-mail stored on a personal computer, is stored communication subject to the [Stored Communications Act].'

In a 2007 decision, in *Scott v. Beth Israel Med. Ctr. Inc.* the New York Supreme Court, New York County, applied the four factors above to e-mails sent by the plaintiff to his attorney with his company e-mail address. The state court found that the attorney work product privilege was waived, despite the attorney's confidentiality notice in the e-mails, because the employer maintained an e-mail policy eliminating an expectation of privacy.¹³

Looking Ahead

In New York, an employer is free to access and review an employee's e-mails in a company-provided e-mail account, particularly where it issues a written policy reserving its right to do so and making employees aware that they have no expectation of privacy in a company e-mail account. However, an employer takes significant risks when accessing an employee's personal e-mail account, even if it is on a company-issued computer.

As we continue to increase our reliance on electronic communication systems, the number of court decisions that address these issues likely will increase.

On a related note, while it has been prudent for employers to provide notice in their electronic communications policies (or elsewhere) that they monitor the company's electronic systems, legislation has been introduced in New York recently that would require employers to notify employees in writing or via e-mail of any electronic monitoring of employees.¹⁴ The notice would be given to new hires and once each year to current employees.

Employers also would be required to post a notice of the types of electronic monitoring utilized in the workplace. The notice would have to be posted in a conspicuous place. In the event the employer had a reasonable belief that an employee is engaged in misconduct that would be revealed through the electronic monitoring, the employer would not be required to provide advance written notice. However, even if enacted, this legislation primarily would pertain to monitoring of the company's electronic systems as opposed to an employee's personal e-mails.

Employers should review their written policies, especially those regarding e-mail use and access. Part of the policy should include defining company equipment and systems. Prior to an employer considering a forensic analysis of a company-provided computer that may reveal a personal e-mail account and its contents, the employer should consider consulting counsel.

1. Title II of the Electronic Communications Privacy Act (ECPA), the Stored Communications Act, 18 U.S.C. §2701.

2. 18 U.S.C. §§2510(17), 2711(1).

3. 18 U.S.C. §§2510-2511.

4. *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 08 Civ. 4810 (JGK)(THK), 2008 U.S. Dist. LEXIS 107657 (SDNY Aug. 22, 2008). Report and Recommendation adopted by the district court, Oct. 22, 2008, 587 F.Supp.2d 548 (SDNY 2008).

5. Id. at *13.

6. *Rozell v. Ross-Holst*, 05 Civ. 2936 (JGK)(JCF), 2007 U.S. Dist. LEXIS 46450 (SDNY June 21, 2007).

7. 18 U.S.C. §2707(b) and (c).

8. 18 U.S.C. §§2701(b)(2)(A), 3571(b)(5).

9. 18 U.S.C. §§2701(b)(1)(A), (b)(2)(B), 3571(b)(3).

10. 18 U.S.C. §§2701(b)(1)(B), 3571(b)(3).

11. Supra note 4.

12. *Curto v. Medical World Communs. Inc.*, 03-CV-6327 (DRH)(MLO), 2006 U.S. Dist. LEXIS 29387 (EDNY May 15, 2006).

13. *Scott v. Beth Israel Med. Ctr. Inc.*, 17 Misc.3d 934 (N.Y. S.Ct., NY County 2007).

14. A. 3871.

Reprinted with permission from the May 26, 2009 edition of the NEW YORK LAW JOURNAL. © 2009 Incisive Media US Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprintscustomerservice@incisivemedia.com. #070-05-09-39