

The Shibolet Times

Published by SHIBOLETH (NY)

A ROUNDUP OF LEGAL AND COMMUNITY NEWS IN NEW YORK & ISRAEL

Email Privacy in the Workplace: What to Expect When You're Expecting Some Privacy

Sagie Kleinlerer and Liraz Yuval, of our IP and corporate departments, reviews and summarizes recent rulings in respect to employer's right to access employee emails.

Email privacy in the workplace is a hotly debated and a much litigated issue. Despite the fact that there has been a volume of litigation on the subject, a definitive set of rules setting forth a consistent guideline to employers with respect to the "digital privacy" remains to be worked out. This area of the law is consistently subject to interpretation by the federal and state courts throughout the United States and since various courts may have different interpretations of the law no definitive unified set of rules can be provided.

Until now, the courts ruled that employees have no reasonable expectation of privacy for any communication transmitted over an employer's email system. These rulings emanated from a rationale that it is in the employer's best interest to monitor employee computer usage. Thus today, monitoring of employee computer usage is widespread and is, in fact, encouraged by the court system. The courts have ruled that if there is some expectation of privacy in an employee's email, it is generally outweighed by the employer's interests in preventing activity that is either inappropriate in the workplace or illegal.

Some of the claims made against employers have been unsuccessful since a federal statute titled Stored Communications Act allows a company to review files and emails stored on its servers. Thus, employee's claims often fail, as the interception rarely occurs during the actual transmission of the email, with such interception being barred by the law. Generally, in its review of expectation of pri-

vacuity in the workplace, the following four factors play a determinative roles for the Courts: (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-

a definitive set of rules setting forth a consistent guideline to employers with respect to the "digital privacy" remains to be worked out

mails; and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies.

However, some states have found an intrusion on the right of privacy by an employer in a situation where employees are assured that their communications are private. If such assurance is given, then a reasonable expectation of privacy could be created and an employee may be able to successfully sue the employer for intrusion. Accordingly, many courts have examined office actions and statements rather than relying on the official company policy in determination of whether an employee's expectation and right of privacy was breached or not.

Web-based email transmitted via a personal email account using a company's Internet connection is not typically stored on a company's email system but is rather stored on the servers of the third-party email provider, such as on Gmail®'s servers. Therefore, no backup copies of personal emails tend to exist on company servers. Furthermore, the court in *Thygeson v. US Bancorp* held that "most employees have a higher expectation of privacy when accessing personal internet e-mail accounts . . . even when doing so while at work."

A problem in monitoring web-based email is that an employer cannot access an employee's web-based email and know which emails were viewed from the office; as such, the employer would have the ability to access all of the employee's personal emails. Therefore, monitoring of such personal email raises difficulties. If the employee decides to store on a company computer any emails received into a personal email account then this file would be treated as any other file that the employee saved or accessed on the computer and the court defers to the corporate policy on computer usage. This would hold true even if the files were saved in a folder labeled "private" or protected by a password set by the user. If the corporate user policy permits monitoring of company devices, then any invasion of privacy claim will fail.

If a company wishes to access employee emails, it is prudent to adopt a policy in which the company explicitly notifies the employees how the company intends to act regarding emails. It appears, based upon the current state of the law, that corporations that have a company handbook or policy and notify their employees of an email monitoring scheme may be able to escape liability for any monitoring.

To access personal email or online accounts, it is necessary to expressly advise employees of employer's right to do so and obtain employees' consent

The policy should advise employees that they should have no expectation of privacy in either their email or company devices (such as a Blackberry™ or laptop), whether used in or out of the office.

To access personal email or online ac-

(Continued on page 2)



counts, it is necessary to expressly advise employees of employer's right to do so and obtain employees' consent. The court in *TBG Insurance Services v. Zieminski* outlines exactly how the employer should implement its policy, including specifically what types of information are being monitored and setting expectations regarding privacy in Internet and email usage. If the company wishes to reserve the right to review employee emails, then the policy should clearly so state. It should also state that although this policy exists, to prevent any potential criminal liability, any electronic documents saved on the company servers could be submitted to law enforcement authorities in furtherance of a civil or criminal investigation.

Further, informing and training employees on the email policy is essential. Such training allows the employees to have a full understanding of what type of information is being monitored so that their expectation of privacy can be managed appropriately as it "undermines the reasonableness of an employee's claim that he or she believed such information was private and not subject to search."

Finally, any employer that contemplates implementing or amending an email policy should consult with an attorney in that employer's state, especially since the law on the subject continues to develop and new rulings may emerge and change prior understandings and policies.

