

Office and Professional Employees International Union, AFL-CIO, CLC




Michael Goodwin
President

Mary Mahoney
Secretary-Treasurer

Date: June 12, 2012

To: All Local Unions

From: Mary Mahoney 

Subject: Use of Employer Computers, Cell Phones, and Networks For Union Business: Not Private, Not Protected, All Content Available To Employer

Many, if not most OPEIU members have access to their employers' computer and e-mail systems. Many employers permit or tolerate the use of employer computers and e-mail for personal matters. Thus, it may seem convenient to use the company computers, company e-mail, and company cell phones for union business during the work day.

However, developments in monitoring software now enable employers review in detail all computer activity that occurs on company computers and cell phones, on employee-owned computers using the company's wired or wireless network, and on cell phones using the employer's wireless network. This sophisticated software enables employers to monitor every keystroke their employees make, every e-mail their employees send and receive, every screen their employees view, every cell phone call their employees make.

If you use the employer's computers or phones or networks, the software enables the employer to virtually stand over your shoulder and observe everything you do. Even if you use your own computer, or your own cell phone, as long as you use the employer's wired or wireless network, the employer can see it all and hear it all. Even if you use your own personal e-mail address, as long as you use the employer's network to access that e-mail, your supposedly private e-mail is available to the employer.

In addition, even where monitoring software has not been installed, the employer can access an employee's company computer when the employee is not at work to review the employee's computer activity, and even reconstruct deleted documents or e-mails.

Almost all employer computer use policies state that employees using the employer's system have no expectation of privacy. Depending on the provisions of the employer's policy, information obtained by the employer can be used as the basis for discipline and/or discharge of employees doing union business or personal business on the employer's system.

An even greater danger may lie where the employer does not discipline employees for conducting union business on the company system, but rather allows the union representatives to use the company system without objection. This allows the employer to obtain confidential information about pending grievances, arbitration arguments, bargaining strategies, union finances, and internal issues, without ever alerting the union that its communications have been intercepted.

80 Eighth Avenue, 20th Floor ■ New York, NY 10011
Tel: 212.675.3210 ■ Fax: 212.727.3466
E-Mail: opeiu@opeiu.org

Website: www.opeiu.org

80 Eighth Avenue, Suite 610 ■ New York, NY 10011
Tel: 212.367.0902 ■ Fax: 212.727.2087
E-Mail: opeiu@opeiu.org

So far, the National Labor Relations Board (NLRB) has not extended any special protections to employees using their employers' computer systems or strayed from the analyses it has offered regarding traditional types of employer communications equipment. In its 2007 Register-Guard decision, 351 NLRB 1110, the NLRB ruled that employees have no statutory right to use the employer's computer equipment for union purposes and recognized that an employer has a legitimate interest in maintaining the efficient operation of its e-mail system. The Board further recognized that employers had valid concerns about such issues as preserving server space, protecting against computer viruses and dissemination of confidential information, and avoiding company liability for employees' inappropriate e-mails.

The NLRB has not, however, considered the question of whether employer monitoring of activity on its system constitutes illegal surveillance of union activities or whether it is legal activity protecting the employer's interests in good order and productivity. The Board's repeated recognition of employer concerns concerning its computer and e-mail system does not provide reason for optimism regarding surveillance issues. Furthermore, even if the NLRB does find employer monitoring to be surveillance, where the employer does not discipline employees or otherwise reveal its monitoring activities, the union will never know that its communication are being intercepted and that it is the subject of employer surveillance.

Given the state of the monitoring technology, union members and representatives should not use employer computers and networks for union business. If the employer permits the union to use the company system for notices and other public communications to members, that is fine. However, use of the employer's system for anything beyond public communications likely provides the employer with easy access to all the confidential affairs of the union. Play it safe. Use the computers and networks in the union office, the officers' or employees homes, or other non-employer controlled areas.

* * *