

Privacy Issues – The Fourth Amendment

Amy J. McKee
 Labor Relations Representative, Senior
 Department of Employee Relations
 October 8, 2002

A.	There has recently been quite a bit of activity in the judicial and legislative system on how to balance theoretical employee privacy interests with an employer's right to control and maintain the workplace.
	1. There is no place that this becomes a bigger issue than with employer provided computers and computer systems.
	2. Employees often times tend to think they have some level of privacy with their Internet and e-mail activities, but the reality of it is they simply do not.
B.	Case Law – The courts are routinely refusing to recognize a privacy interest in this developing area of the law.
	1. A United States District Court located in PA rejected an invasion of privacy claim filed by an employee who was discharged after his employer read emails the employee sent. The employer found the emails to be inappropriate, unprofessional, and offensive. <u>Smyth v. Pillsbury Co.</u> , 914 F.Supp. 97 (E.D.Pa. 1996).
	2. Another United State District court located in the same PA district recently dismissed an employee's state and federal invasion of privacy claims stemming from an incident in which the employer searched and read the employees emails. The court found that the emails were not "intercepted" because the employee had already opened and read the subject emails. Had the employer read emails that the recipient had not yet, then there would be a violation of the law. <u>Fraser v. Nationwide Mutual Ins.</u> , #98-CV-6726, (E.D.Pa. 2001).
	3. The Second Circuit recently found not privacy violation when a public sector employer (the NY/DOT) searched an employee's computer and email despite finding that that the employee did have a reasonable expectation of privacy. <u>Leventhal v. Knapek</u> , 2d. Cir., No. 00-9306, 9/26/01.
	4. The Seventh Circuit recently found the same to be true for a private sector employer seized and searched a computer located at an employee workstation. The court found the employee did not have a reasonable expectation of privacy. <u>Muick v. Glenayre Electronics</u> , 7 th Cir., No. 00-3299, 2/6/02.
	5. A MA State court found that the two discharged employees did not have a reasonable expectation of privacy when forwarding sexually explicit e-mails. The court also rejected the plaintiff's invasion of privacy claims. <u>Garrity v. John Hancock Mutual Life Ins.</u> , D.Mass. No. 00-12143-RW2, 5/7/02.
	6. A United State District Court located in New York recently found that an employer did not violate the Fourth Amendment to the U.S. Constitution by seizing a computer and computer disks when investigating employee misconduct. The court found that the employee had no reasonable expectation of privacy as the

		employer clearly articulated this fact via published policies. <u>U.S. v. Reilly</u> , S.D.N.Y., No. 01 Cr 1114, 5/31/02.
C.	Proposed Legislation	
	1.	The Notice of Electronic Monitoring Act (2000) (HR 4908), a proposed amendment to existing Federal Wiretap laws, would have required employers to provide employees very specific written notice of any intended monitoring of Internet and e-mail use. The bill stalled in conference committee and ultimately did not pass. "Witnesses Urge Fine-Tuning of Legislation Requiring Notice of Electronic Monitoring," <u>Human Resources Report</u> , Bureau of National Affairs, Vol. 18, No. 35 (9/11/00).
	2.	CA Governor Greg Davis vetoed S.B. 1822 on 9/30/00. This law would have prohibited employers from monitoring emails and computers unless the employee signed a written agreement acknowledging the employers right to do this. "California Governor vetoes Measure to Limit Employer E-Mail Monitoring," <u>Human Resources Report</u> , Bureau of National Affairs, Vol. 18, No. 39 (10/9/00).
D.	The Bottom Line: Employers need to make it crystal clear to employees that both email and Internet activities are not private and that the employer retains the right to search, seize, confiscate, and/or otherwise read or monitor anything and everything that an employee does with the employer owned computer and computer systems.	
	1.	Get a statement into agency policies regarding this fact and consider having a "sign-off" portion for the employee to acknowledge receiving and understanding the policy.
	2.	Consider adding a pop-up box to the log in process that notifies employees of this fact, and make sure that the employee has to affirmative click on an icon indicating that they have read the statement and accept the terms. Do not just have a window that pops up and after a period of time disappears.