WILMERHALE

Recent U.S. Case Law Provides Support for Position That Employees Have No Reasonable Expectation of Privacy in Electronic Communications; Germany Reaches Opposite Result

JULY 10, 2002

As employee use of the Internet and electronic mail (email) for both business and personal matters continues to be routine in the workplace, courts continue to grapple with questions about the scope of an employer's ability to monitor and control its employees' electronic communications.

As noted in our December 10, 1999 Internet Alert on the topic of employee privacy in electronic communications, there are good reasons for employers to be wary of the potential for employee abuse of electronic communication technologies. These reasons are both practical (*e.g.*, work time lost due to excessive personal email use) and legal (e.g., distribution of obscene or racist messages which could expose companies to liability). Nevertheless, employers seeking to assess the potential risks of monitoring employee use of such communications have had little guidance from the courts. The sparse case law regarding an employee's privacy interests in the context of electronic communications still leaves the question unsettled, but recent court decisions suggest that, at least in most circumstances, employees do *not* have a reasonable expectation of privacy in their employers' computers or communications systems.

Most recently, in *Garrity v. John Hancock Mutual Life Insurance Co.*, an employer obtained summary judgment in a case involving its termination of employees who used the employer's email system to share sexual jokes. The Federal District Court in Massachusetts found that the employer's review of employee email messages stored in the employer's computer system was not an unlawful invasion of employee privacy. The court also held that the employees had no reasonable expectation of privacy in their email correspondence, even though the employer had previously instructed employees about how to keep email private with personal passwords and personal email folders. In reaching its decision, the court found that any reasonable expectation of privacy was undermined by the fact that the employees in question knew of the employer's electronic communications policy (in which the employer reserved the right to review e-mail stored on the system), and also knew that recipients of their emails could forward them to third parties. The court also relied, in part, on an earlier decision, *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996), in

which a federal court in Pennsylvania held that, even in the absence of an employer email policy, employees who voluntarily communicate to others over an email system utilized by an entire company do not have a reasonable expectation of privacy in such communications.

Although *Smyth* suggested that an employer does not necessarily need to implement an electronic communications policy in order to inspect and monitor employee computer use without running afoul of privacy laws, other recent decisions in addition to *Garrity* indicate that notification to employees that their computers and electronic files may be monitored is still the best way for an employer to protect itself against invasion of privacy claims. For example, in *TBG Insurance Services Corp. v. Superior Court*, a California appellate court held that an employee who signed an electronic equipment policy consenting to having his employer-provided home computer monitored by authorized company personnel had no reasonable expectation of privacy in such computer. Similarly, in *Muick v. Glenayre Electronics*, the Seventh Circuit Court of Appeals held that an employee had no reasonable expectation of privacy in the laptop computer that his employer had lent to him for office use because the employer informed the employee that it could inspect the computer. By contrast, the Fifth Circuit Court of Appeals in *United States v. Slanina* recently held that an employee did have a reasonable expectation of privacy in a company computer where an employer failed to have a policy advising employees that computer usage would be monitored, and where there was no indication that company personnel had routine access to employee computers.

By way of comparison, under German labor and employment law, the legitimacy of reviewing an employee's emails basically depends on whether the purpose of the email is operational or private. For operational emails, reviewing both address / transfer data and content of the email has been held to be legitimate. For private emails, regardless of whether private use is permitted or prohibited, the review of the content of emails by the employer is generally forbidden. Only if there is a well-founded suspicion that the employee is using his private emails for the purpose of criminal offenses or grave violations of the employment relationship (e.g., disclosure of trade and business secrets or sexual harassment) would reviewing of the email's content be considered legitimate. The review of address / transfer data is permitted when necessary to decide whether an email is operational or private. A violation of the general prohibition of reviewing the content of a private email can lead to a claim for damages from the employee, and may even constitute a criminal offence by the employer under German law. Information received by illegally reviewing the employee's private emails cannot be used as evidence to justify a termination of the employment contract by the employer.

The developing case law demonstrates that U.S. courts have generally been willing to recognize an employer’s legitimate right to make sure that its electronic communications equipment is not being used for inappropriate or unlawful purposes. Nevertheless, it is still prudent for employers who provide email and Internet access to their employees to continue to maintain written electronic communications policies which diminish employee expectations of privacy by clearly stating, among other things, that the employer’s electronic communications equipment is being provided for business use, and that the employer reserves the right to monitor and access all employee computer usage. Such policies may not protect an employer from all potential claims, but should make it far more difficult for an employee to establish a reasonable expectation of privacy.

Laura Schneider
laura.schneider@haledorr.com

Jamie Balanoff
jamie.balanoff@haledorr.com

Manfred Schmid
manfred.schmid@haledorr.com

Authors

Laura E. Schneider

PARTNER

Chair, Labor and Employment Practice

laura.schneider@wilmerhale.com

+1 617 526 6846