
	The Health Care Forum 2008 The Carrot or the Stick: How employers are managing employee health care to reduce costs.	Click here for details and to register.	
---	--	---	---



Feature: Their BlackBerries—Your Problem

Their BlackBerries—Your Problem

However much employers want to provide access to their technology systems for business convenience or necessity, they also have legitimate interests in preventing their misuse. Employers will also have to do some education with employees about what happens when personal devices are used to access company systems. Employees may mistakenly believe that by using their own devices, they have bought themselves a measure of privacy and are beyond the reach of their employer.

By **Zachary A. Hummel**

For most employers, allowing employees to have mobile access to e-mail and Internet servers through their own phones, BlackBerries or other devices is an attractive proposition. Every organization wants more efficiency and productivity, and the ability to remotely access data systems with a mobile device lets employees instantly communicate with one another and respond to the business's clients and customers. With the popularity of Apple's iPhone and the competing devices now either on the market or being rushed to it, prices will continue to drop and technological capabilities will rise. In a world where work and personal life seem to merge more every day, it's increasingly difficult for organizations to limit employees to Internet or e-mail access only through company-owned devices. That's just not how business works anymore.

While the technology has tremendous advantages for employers, there is a flip side to this development. The systems that allow employees to communicate instantly with customers are also the ones employees use to communicate with friends, family and, quite literally, everyone else connected to the Internet. From pre-teens to seniors, mobile devices are increasingly the preferred device for how we communicate, whether it's e-mailing, talking or filming and posting video to YouTube.

Employers need to think carefully about giving employees access to company data systems through these devices. And employers have to decide if, when and how they will monitor the use of their systems. However much employers want to provide access to their technology systems for business convenience or necessity, they also have legitimate interests in preventing their misuse. Employers will also have to do some education with employees about what happens when personal devices are used to access company systems. Employees may mistakenly believe that by using their own devices, they have bought themselves a measure of privacy and are beyond the reach of their employer.

Once employers make decisions about the boundaries of system access and about monitoring, employers should put employees on notice, telling them what the boundaries are. They should inform employees about potential monitoring and possible access to information transmitted, conveyed or stored on their personal devices. Employers should provide these notices prior to giving employees access to the systems and, ideally, require that employees agree to the terms as a requirement of access. Employers must keep a record of the notice they have provided to employees or have a record of the employee's agreement to the terms of use for company-provided technology systems.

If an employer fails to provide clear notice to employees of the employer's right and ability to monitor usage, employees may claim that they had an expectation of privacy in their communications via the employer's data systems. If an employer creates an expectation of privacy, or fails to dispel that expectation, the monitoring of these systems may violate employee rights.

Many employers are used to addressing these issues when they provide laptop computers to employees, but they fail to realize that the issues that arise are less about the hardware used than the *access* to data

systems. Employers should carefully review existing policies to ensure that they are keeping pace with technology.

The stakes are high for employers that fail to keep tabs on their data systems. In a recent state court case in New Jersey, litigation was allowed to proceed over the objections of an employer in a lawsuit for damages stemming from an employee's misuse of employer-provided Internet access.

The plaintiff was the mother of a 12-year-old girl. The girl's stepfather, a company employee, circulated pictures of the child on a child pornography Web site, using the employer's Internet access. The mother alleged that the employer had a duty to monitor its systems and prevent their improper use. The court found that there was potentially a duty for the employer to guard against misuse of Internet access and to prevent damage to others from such misuse. While it was only a ruling on a preliminary motion, the theory that the plaintiff was using to seek damages from the employer could be used in other cases in which employers failed to monitor and prevent misuse of their systems.

Compliance with employer policies and, potentially, an affirmative duty to monitor system use may also arise in disputes over the improper use of confidential company information. Employers must act to protect proprietary and confidential information, or they could lose the ability to protect against its public use. It may turn out to be a significant issue if an employer allows employees to access documents on its servers through a personal device and fails to monitor such traffic to ensure that the device is not being used to download large amounts what could be confidential data. Monitoring the access and use of such information may be a necessary step in proving that such information was indeed confidential.

There is countervailing pressure here for employers. While they may, with proper notice, monitor or gain access to e-mails that violate non-compete or confidentiality restrictions, they should avoid accessing e-mails that communicate personal matters that are not violations of company policies. The technology exists to review the content of messages, and there is software that can look for key words and phrases in e-mails in order to sift through the volume of e-mails to get to the specific issues that cause the employer concern.

Workforce Management Online, March 2008 -- [Register Now!](#)

Zachary A. Hummel is a partner in the New York and St. Louis offices of Bryan Cave LLP. To comment, e-mail editors@workforce.com.

[Home](#) | [Research Center](#) | [Community Center](#) | [Commerce Center](#) | [Conferences](#)
[Benefits](#) | [HR Management](#) | [Recruiting & Staffing](#) | [Software & Tech](#) | [Training & Develop](#) | [Legal](#)
[Current Print Issue](#) | [Print Subscription](#) | [Subscriber Help](#) | [E-Newsletters](#)
[Contact Us](#) | [Site Help](#) | [Terms of Use](#) | [Privacy Statement](#) | [Rights & Permissions](#) | [Advertising Info](#)



Copyright © 1995-2008 Crain Communications Inc.
All Rights Reserved. [Terms of Use](#) [Privacy Statement](#)