

PRWeek

FEBRUARY 8, 2010

WWW.PRWEEKUS.COM



MICHAEL LASKY

Avoid employee invasion-of-privacy claims with updated tech guidelines

Twenty-four-seven is the new (or, in our industry, not so new) 9 to 5. Everyone has Blackberrys or other smartphones – often issued by employers. We’ve all seen companies reserving the right to monitor employees’ e-mails and Internet use in the workplace, and, until recently, we believed that employees had virtually no right of privacy in communications sent or received using company-issued equipment or servers.

Recent New York cases are redefining the scope of employer monitoring rights, making it more important than ever to implement policies that insulate employers from a growing number of invasion-of-privacy claims by current or former employees.

For example, many employees are aware that cell phones contain global positioning software (GPS). Employers may seek to review GPS data from company-issued cell phones to track employees’ whereabouts, particularly where an employee is required to travel for business, or an employer questions the employee’s whereabouts during working hours. Courts suggest that employers can rely on GPS data captured during “business hours” in making employment decisions without invading employees’ privacy rights, even where both business- and non-business-hour GPS data is captured. Just what constitutes a “business hour” in a 24/7 service-oriented business, however, is undetermined.

And what about employees’ rights to privacy in text messages sent from company-issued cell phones? A recent court held that an employer violates an employee’s right to privacy in monitoring such text messages unless the employee consents (similar to phone calls).

Moreover, courts have held that employers cannot access personal e-mail accounts of staffers via the Internet using employees’ user names and passwords, even if the user name and password are stored on a company computers/server. The same goes for accessing social

media Web sites such as Facebook, MySpace, and Twitter. On the other hand, the employer has every right to access that same e-mail content off of its own servers.

My four tips for savvy information-age employers:

1. Provide clear parameters for acceptable personal use of company-issued devices, e-mail, equipment, and servers, and clarify that such policies apply to all employees and that the company’s right to monitor e-mails extends to personal e-mails stored on company servers.
2. Implement a policy governing employees’ use of social media Web sites during work hours, also indicating permissible uses of the company’s name (if any), and emphasizing non-disclosure of company- or client-confidential information.
3. Obtain employees’ written consent to monitor all communications sent or received by company-issued devices, e-mails, or servers, including, where applicable, text messages.
4. Notify employees, where applicable, that the company reserves the right to review GPS data gathered from company-issued cell phones and/or Blackberrys.

Technology has its benefits and its burdens. Review your existing policies to ensure that they adequately protect against the growing number of employee invasion-of-privacy claims. Employees’ consent is a powerful defense in a litigation environment. ■

Michael Lasky is a senior partner at the law firm of Davis & Gilbert LLP, where he heads the PR practice group and co-chairs the litigation department. He can be reached at mlasky@dglaw.com.