

Privacy Rights of Employees Clarified

©2009

by Stacy A. Hickox, JD, Assistant Professor
Michigan State University, School of Labor and Industrial Relations

Recent decisions provide some guidance for employers on how far to go in seeking out and reviewing personal information about their employees. A recent study released on September 25, 2009, by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association found that half of all employers lack a policy to address employees' use of social networking sites outside of work.¹ At the same time, one quarter of those same employers have disciplined an employee for activities on one of those sites.

Accessing social networking sites of employees can be a violation of their privacy. One federal court in New Jersey recently held that an employer intentionally accessed "the Spec-Tator," a chat group on MySpace.com, accessed by invitation with members' MySpace accounts and passwords. The jury found that the employer had not invaded employees' common law right of privacy, because the employees had no reasonable expectation of privacy in the group. However, the court recently upheld the jury's verdict that the employer had violated the federal Stored Communications Act (SCA) and had acted maliciously, supporting a verdict for over \$17,000 in compensatory and punitive damages. The employer failed to convince the jury that its access to the Spec-Tator was authorized "by a user of that service with respect to a communication of or intended for that user," which would have disproven an SCA violation.²

That New Jersey jury properly concluded that the employer was not an authorized user under the SCA, even though log-information was provided to two managers from an authorized user of the Spec-Tator. In finding that the employer lacked authorization, the jury relied on that user's testimony that she felt coerced into giving her password to the manager because she worked for him, and that she would not have given her information to other co-workers. Based on this testimony, the jury could reasonably infer that her "authorization" was coerced or provided under pressure, and therefore the employer was not an authorized user under the SCA.

Like this New Jersey court, the California Supreme Court refused to hold a private employer liable under general protections of employee privacy.³ The installation of a concealed video surveillance camera in the office of two clerical workers intruded on their privacy, based on the assignment of those employees to that office and the fact that the office had blinds and a lock on the door. Yet the employer was not liable for "extreme and outrageous" invasion of those privacy interests where the employer was trying to control inappropriate web surfing by its employees.

¹ BNA News, Daily Labor Report, Sept. 28, 2009.

² 18 U.S.C. § 2701(c)(2).

³ Hernandez v. Hillside, Inc. No. S147552 (Cal. Aug. 3, 2009).

This employer did not violate that standard since it only turned the camera on at night and did not actually capture the employees on camera.

Another New Jersey court recently found that an employer must return e-mails sent by an employee to her attorney using a company computer.⁴ These e-mails concerned her plans to sue her employer for sexual harassment. Even though the employer owned the computer and reserved the right to search the computer, the employer was required to return the e-mails sent with that computer but through her personal e-mail account. The employer's policy had allowed "occasional personal use" of its computers, and allowed review of the use of its e-mail system, which could exclude use of a personal e-mail account. Therefore, the employee had an expectation of privacy in the content of those e-mail messages. The court concluded that the right to discipline an employee based on inappropriate computer use "does not extend to the confiscation of employee's personal communications."

Even applicants may be protected against overly invasive investigation of their backgrounds, at least by public employers. The Court of Appeals for the Ninth Circuit recently refused to review its 2008 decision that halted background checks of employees of the California Institute of Technology.⁵ These background checks were conducted under Cal Tech's contract with NASA for the work of scientists, engineers and administrative employees at NASA's Jet Propulsion Laboratory (JPL). Failure to complete the background check process resulted in discharge of current Caltech employees at JPL, as well as applicants' elimination from the hiring process.

NASA failed to show a compelling government interest to justify the broad range of questions asked of Cal Tech employees, which included residential, educational, employment, and military histories. References, employers, and landlords were sent an "Investigative Request for Personal Information", which asked whether the recipient has "any reason to question [the applicant's] honesty or trustworthiness" or has "any adverse information about [the applicant's] employment, residence, or activities" concerning "violations of law," "financial integrity," "abuse of alcohol and/or drugs," "mental or emotional stability," "general behavior or conduct," or "other matters." Most of these "broad, open-ended questions" were found to be "beyond the scope of the legitimate state interests" that NASA had proposed. The appellate court allowed the question about drug use, but not the question regarding treatment or counseling received for drug problems. This is one of the first cases that has recognized a right of privacy in information requested of job applicants, particularly where the public employer has asserted safety and security reasons for the inquiry.⁶

Based on these recent cases, employers are advised to consider employees' privacy interests in monitoring the personal behavior and communications of employees and even applicants. Specifically, employers should consider the following:

⁴ Stengart v. Loving Care Agency, Inc., No. A-3506-08T1 (N.J. Super. Ct. App. Div. June 26, 2009).

⁵ Nelson v. NASA, 530 F.3d 865 (9th Cir. 2008).

⁶ Nelson v. NASA, No. 07-56424, 2009 U.S. App. EXIS 12073 (9th Cir. June 4, 2009)(dissent from order denying rehearing en banc).

- Be sure to have uncoerced access to personal social sites before accessing and relying on information found there
- Notify employees who are subject to surveillance or electronic monitoring to lower their expectations of privacy
- Conduct surveillance or electronic monitoring only when the employer has a legitimate purpose for obtaining the information
- Limit screening of applicants to information that is directly related to their ability to perform the duties of the position being filled