Workplace Privacy: Not Just a Problem for Erin Andrews

Insights
9.01.09

(Labor Letter, September 2009)

With the disclosure of personal information now rampant on social networking sites like Facebook and Twitter, it sometimes seems like privacy is a relic of the past. Don't be fooled: privacy is a hot legal topic with serious implications for employers.

The Erin Andrews Saga
Sports fans may have heard of a recent incident in which ESPN reporter Erin Andrews was filmed nude in her hotel room through a peephole, by someone who posted the video on the Internet. ESPN's General Counsel quickly fired off an e-mail to the website demanding the immediate removal of the video and disclosure of its source. The video was removed shortly thereafter, but not before causing a media sensation.

The buzz continued for weeks, with Ms. Andrews later calling 911 to complain that she was being harassed by men who had knocked on her door and parked their car in front of her home in a gated community. Later news reports speculated that the Peeping Tom who videotaped Ms. Andrews may actually have been a co-worker, because the posted video appears to be a compilation of several different videos shot at different locations. Ms. Andrews and her attorneys have promised civil and criminal prosecution of the perpetrator.

To the casual observer, this incident may seem like just another incident of a TV personality being "overexposed" in the media, but to employment attorneys and Human Resources professionals, it's a sexual-harassment nightmare. As a sports reporter, when Ms. Andrews travels she's on the job, and ESPN, like all employers, has a duty to prevent and correct sexual harassment - whether by strangers or by co-workers. It was essential for ESPN to take immediate steps to stop the harassment and contain the damage as much as possible, both for the sake of Ms. Andrews and to limit the company's potential liability.

To Catch A Thief (Or A Voyeur)
But what about other situations? Is it ever okay for employers to secretly videotape their (clothed) employees? The California Supreme Court recently said yes. Although the California State Constitution has strong privacy protections applicable to public and private actors alike, the Court held that in some circumstances, the employer's business needs may trump an employee's right to privacy.

In *Hernandez v. Hillsides, Inc.*, two female employees of a 24-hour residential facility for abused and neglected children sued their employer for invasion of privacy after discovering a small video camera and motion detector hidden in their shared office. When the women discovered the video equipment, a red light on the motion detector flashed and the electrical cord attached to the camera was hot to the touch. The women's office had blinds that could be closed and a door that locked, and one of the women regularly changed into her gym clothes in the office after work to go running.

The employer placed the video equipment in the women's office without notifying them because someone had repeatedly used a computer in that office to access pornographic websites late at night. Although the employer did not suspect the female employees, several employees had keys to their office, and Hillside was concerned that one of its program directors - who are responsible for the abused children living at the facility - was involved. The employer did not tell the women of the surreptitious taping, for fear that gossip about the video equipment would alert the perpetrator.

The video camera was activated only at night, and only on three occasions during a three-week period. The camera was never turned on during the day when the women were working in their office.

When the women discovered the camera, the employer apologized, explained why he had not told them about it before, and showed them all of the video footage he had captured. Neither woman appeared on the videotape. (Neither did the perpetrator, so ultimately the secret sting operation was a bust.) Nevertheless, the employees sued Hillsides for invasion of privacy.

The trial court threw the women's lawsuit out without a trial, holding that the employer had not violated their right to privacy. An appeals court disagreed and reinstated the case, holding that the employer had intruded into a protected zone of privacy, and the intrusion was so unjustified and offensive that it constituted a violation of their privacy.

Not So Fast

But the California Supreme Court reversed the appellate court and dismissed the case. It held that the women had a "reasonable expectation of privacy" in their office - specifically, a reasonable expectation that their employer would not install video equipment capable of monitoring and recording their activities behind closed doors without their knowledge or consent. However, the court also found that the intrusion on their privacy was not so great as to be "highly offensive" to a reasonable person, because of the limited nature of the invasion and the employer's reason for doing it.

The Court gave great weight to the fact that the surveillance took place only for a limited period, Hillside took steps to avoid capturing the female employees on video during the daytime, and immediately showed them the video once the equipment was discovered. In addition, there was a legitimate reason for the videotaping: to protect the abused children who lived at the facility from possible further abuse. This reasoning is consistent with the balancing test often used in invasion-of-privacy cases in the state.

of-privacy cases in the state.

Despite dismissing the case, the Supreme Court expressly discouraged employers from engaging in surveillance, especially if the employees within camera range are not given adequate notice that they may be viewed and recorded. This disclaimer failed to soothe civil libertarians who complained that the decision will give employers permission to spy on employees so long as the employees didn't know about it.

For legal reasons, you should diminish your employees' expectations of privacy in their offices, desks, lockers, computers and e-mail accounts. Typically this will take the form of a written policy acknowledged by the employee (in an employee handbook or otherwise) in which you notify the employee in advance that these areas are not private, and that the company may search or monitor them under certain circumstances. And be mindful of special statutory protections: for example, some states expressly prohibit videotaping or monitoring of bathrooms, locker rooms and other changing areas.

Spying On Private Websites Can Be A Problem, Too

Invasions of employee privacy are not limited only to surreptitious videotaping - spying on private employee websites can be a problem, too.

In *Pietrylo v. Hillstone Restaurant Group*, a federal court in New Jersey recently allowed an invasion of privacy case to go to trial over claims arising from managers' viewing of a private employee MySpace page. Employees of the Houston's restaurant chain had set up a private, invitation-only site called "Spec-Tator" to gripe about their jobs at Houston's. The site was maintained on an employee's personal computer and accessed on employees' own time.

The initial posting on the "Spec-Tator" MySpace page stated that it was to allow employees to "vent about any BS we deal with [at] work without any outside eyes spying in on us. This group is entirely private, and can only be joined by invitation." The posting went on, "Let the s**t talking begin." Unsurprisingly, employees used the site to complain about their jobs, their supervisors, and so on.

Eventually, a non-management employee who had legitimate access showed the site to a manager. Another manager subsequently asked the employee for her password, which she provided, and other managers also viewed the site. Ultimately the employee who had created the site and another Houston's employee were fired.

They sued the restaurant for invasion of privacy, wrongful termination, violation of state and federal wiretapping statutes, violation of the federal Stored Communications Act, and the equivalent state act. The restaurant asked the court to dismiss the case without a trial, but the court refused to do so.

The court held that a trial was required to resolve the disputed fact of whether the employee who gave her password to management had been coerced into doing so. If she had, the restaurant was not an "authorized user" of the site and was potentially liable for violating the law and invading the other employees' privacy. The employees argued that management's request for her private password was inherently coercive under the circumstances of the case; the managers countered

password was inherently coercive under the circumstances of the case, the managers countered that they had merely asked the employee to provide her password without threats or coercion, and she had done so.

Ultimately the case comes down to the degree of pressure (if any) exerted on the cooperating employee by the employer. This is not a place you want to be in litigation.

Words To The Wise

What lessons, if any, can employers draw from these cautionary tales? First, recognize that employees may have privacy rights in and out of the workplace, and that failing to recognize and respect these rights can create or exacerbate legal problems. Second, issue written policies that place employees on notice that their right to privacy in the workplace is limited. Third, tread carefully when issues arise that implicate privacy concerns. Just because you have the capability to videotape or otherwise monitor employees without their knowledge doesn't mean it's the best way to solve a particular problem. Sometimes it even creates more problems.

This article was reprinted in the September 2009 Newsletter for the *Orange County Chapter of the Association of Legal Administrators*. It also appeared in the October 21, 2009 issue of *Workforce Management*.