

Workplace Privacy in California: Employee Interests, Employer Rights

BY PAUL W. CANE AND GINA GUARIENTI COOK

California employers sometimes feel lost in a sea of employee “rights,” with the employer’s interests held secondary (if recognized at all). The California Supreme Court’s unanimous decision in *Hernandez v. HillSides, Inc.* (Aug. 4), a case regarding workplace privacy and video surveillance, provides some comfort.¹

In *HillSides*, the Supreme Court ruled in favor of an employer whose employees had sued for invasion of privacy after the employer secretly installed a concealed video camera in the employees’ office. The decision recognizes that employers can conduct surreptitious workplace surveillance as long as they have a legitimate business reason for doing so and properly tailor the methods and scope of the surveillance.

The Facts

Defendant HillSides, a private residential facility for neglected and abused children – including victims of sexual abuse – learned that someone was accessing pornographic websites from particular computers at the facility late at night. This use violated HillSides’ policies and conflicted with its aim of providing a safe haven for the children who resided there. One of the computers from which the websites were accessed was located in an enclosed office shared by two clerical employees, Abigail Hernandez and Maria-Jose Lopez.

To identify the culprit, HillSides installed a hidden, remote-operated camera in Hernandez’s and Lopez’s office without notifying them. Although HillSides did not believe that Hernandez and Lopez were the perpetrators, they did not inform Hernandez and Lopez of the surveillance. HillSides reasoned that the more people who knew and perhaps gossiped about the plan, the greater the chance the culprit would learn about it and avoid detection.

The camera was aimed at one of the computers at issue. The camera could be made operable from a remote location at any time of the day or night and could be used for either live viewing or recording. However, the camera was not operated for either purpose during business hours; the camera was “on” but not transmitting images. Thus, neither Hernandez nor Lopez was ever viewed or recorded by the camera.

Hernandez and Lopez discovered the camera when they noticed its red light blinking. They sued for invasion of privacy, noting that the office had a door that could be closed and locked, and that the office had blinds on the windows that could be closed. Hernandez and Lopez testified that they

occasionally used their office to change or adjust their clothing. Even though several office administrators had keys to the office, and the office had a “doggy” door through which someone potentially could have peered, Hernandez and Lopez contended that they still had a reasonable expectation of privacy there.

A trial court had granted summary judgment in favor of Hillside, but a panel of the court of appeal reversed, holding that a potential privacy intrusion had occurred, and that it was up to a jury to decide whether Hillside's interest in catching the wrongdoer trumped the plaintiffs' privacy interest.

The Decision

The Supreme Court reversed the court of appeal and ordered summary judgment for Hillside. The Supreme Court agreed that a potential privacy intrusion had occurred, because the camera had been placed where the plaintiffs had a reasonable expectation of privacy. However, Hillside prevailed as a matter of law because the Court held that, under the circumstances, the intrusion would not be highly offensive to a reasonable person.

Employees' Expectation of Privacy at Work

Even though the office at issue was shared, several administrators had a key to the office, and the “doggy” door made it possible for people to look into the office, the Court concluded that the plaintiffs had a reasonable expectation of privacy in their office. The office was not accessible to the general public, the employees could lock the office and close the blinds, and the employees treated the office as a private place when they changed clothes there. In addition, no Hillside policy informed employees that they might be subject to surveillance. Although Hillside's computer policy noted that internet activity might be monitored, no policy mentioned video surveillance.

Offensiveness of the Employer's Conduct

In the end, however, the employer prevailed because, the expectation of privacy notwithstanding, the Court concluded that the employer had not acted in a manner that would be considered “highly offensive to a reasonable person.” Key to the Court's conclusion was the fact that the surveillance was limited in time, place, and scope and the fact that the intrusion itself was limited:

- The surveillance was conducted only at night, after the plaintiffs had gone home for the day;
- The defendant took a measured approach in choosing the location to videotape – *i.e.*, it placed the surveillance equipment in the plaintiffs' office only after trying without success to monitor other, more-public areas with computers that the culprit may have used;
- The camera pointed at the specific computer in question rather than capturing the entire office;
- After discovering that no one had viewed pornographic websites from the plaintiffs' office in the 21 days that the camera was there, the camera was removed;
- The camera never recorded the plaintiffs, even though it was in the office while they worked;
- The employer had implemented safeguards to limit access to the surveillance equipment and the surveillance footage; and

- The employer had a manifestly legitimate business purpose for the surveillance: protecting the children who lived at the facility.

Employee-rights lawyers may attempt to suggest that the case's teaching is limited to its unusual factual context. That suggestion misreads the case. The Court went out of its way to generalize about employer monitoring of employees' computer and internet usage. Specifically, the Court recognized that the potential for computer abuse in the workplace is wide-ranging, that the consequences for employers can be serious, and that employers commonly regulate and monitor their employees' computer and internet use to make sure that it is appropriate. This broad recognition of the validity of workplace computer-monitoring policies should provide comfort to employers who must monitor employee activity in more-traditional workplaces. (Out of an abundance of caution, employers who want to monitor workplace computer use should require employees to acknowledge their understanding that computer use is for business purposes, and that the employer reserves the right to monitor workplace computer use.)

Employers also should be pleased that the Court rejected one of the most potentially dangerous arguments asserted by the plaintiffs: that, in order to defeat an invasion-of-privacy claim, employers who conduct workplace surveillance must engage in the least-intrusive means of accomplishing their legitimate objectives. In *Hillsides*, the Court refused to second-guess the employer's conduct based on alternatives that might have been as effective and less intrusive. In the real world, most any course of conduct can be second-guessed with the benefit of hindsight, and the Court declined to engage in that kind of second-guessing.

Affirmation of the Summary Judgment Decision

The procedural posture of this case also provides comfort to employers. The Supreme Court reinstated the trial court's decision to grant summary judgment in favor of the employer. Often courts announce "balancing-of-interests" and other legal tests that leave the balancing or application to the jury. (That, indeed, is what the court of appeal had done, earlier on in the case.) That approach creates legal uncertainty and imposes huge litigation costs. The parties do not know the legal answer until after a jury rules at trial. By affirming the summary judgment here, the Court in *Hillsides* provided employers with a useful precedent to use in seeking dismissals of cases short of trial.

Practical Advice for Employers

- **Address surveillance in workplace monitoring, investigation, or privacy policies:** Just as employers use internet and computer-usage policies to inform employees that their computer and internet activity may be monitored, so should they consider policies addressing workplace surveillance. Such policies may play a critical role if an employer has to demonstrate that the employee wholly lacked an expectation of privacy.
- **Before installing surveillance equipment, consider whether the setting is "private":** Employers should recognize that some areas of the workplace (*e.g.*, private offices with doors) are more private than others (*e.g.*, common areas, or perhaps cubicles without privacy walls) and should attempt to conduct surveillance in less-private areas.
- **Tailor the scope, duration, and methods of surveillance:** When conducting surveillance, employers should pay careful attention to the scope, duration, and methods of surveillance. Although the Court in *Hillsides* rejected the plaintiffs' argument that their claims would have succeeded if they were able to show that there was a less-intrusive alternative that the

employer could have adopted, employers should consider just such alternatives in order to best protect themselves.

- **Avoid audiotaping:** Although *Hillsides* establishes principles that are generally helpful for employers, employers should remember that the surveillance at issue did not involve an audio component. If it had, Penal Code sections 631 and 632, which prohibit wiretapping and eavesdropping, might have been implicated. When conducting workplace investigations, employers should remain cognizant of the obligations imposed by these Penal Code sections related to audiotaping.



If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Los Angeles

Heather A. Morgan
213-683-6188
heathermorgan@paulhastings.com

Orange County

Stephen L. Berry
714-668-6246
stephenberry@paulhastings.com

Palo Alto

Maureen E. O'Neill
650-320-1811
maureenoneill@paulhastings.com

San Diego

Mary C. Dollarhide
858-458-3019
marydollarhide@paulhastings.com

San Francisco

Paul W. Cane Jr.
415-856-7014
paulcane@paulhastings.com

¹ One of the authors, Paul, Hastings partner Paul Cane (San Francisco office), briefed and orally argued the case for *amici curiae* Employers Group and the California Employment Law Council. Co-author Gina Cook practices in Paul, Hastings' Los Angeles office.