Filed 8/3/09

IN THE SUPREME COURT OF CALIFORNIA

ABIGAIL HERNANDEZ et al.,	
Plaintiffs and Appellants,	S147552
v.	Ct.App. 2/3 B183713
HILLSIDES, INC. et al.,	Los Angeles County
Defendants and Respondents.	Super. Ct. No. GC032633

Defendants Hillsides, Inc., and Hillsides Children Center, Inc. (Hillsides) operated a private nonprofit residential facility for neglected and abused children, including the victims of sexual abuse. Plaintiffs Abigail Hernandez (Hernandez) and Maria-Jose Lopez (Lopez) were employed by Hillsides. They shared an enclosed office and performed clerical work during daytime business hours. Defendant John M. Hitchcock (Hitchcock), the director of the facility, learned that late at night, after plaintiffs had left the premises, an unknown person had repeatedly used a computer in plaintiffs' office to access the Internet and view pornographic Web sites. Such use conflicted with company policy and with Hillsides' aim of providing a safe haven for the children.

Concerned that the culprit might be a staff member who worked with the children, and without notifying plaintiffs, Hitchcock set up a hidden camera in their office. The camera could be made operable from a remote location, at any time of day or night, to permit either live viewing or videotaping of activities

around the targeted workstation. It is undisputed that the camera was not operated for either of these purposes during business hours, and, as a consequence, that plaintiffs' activities in the office were not viewed or recorded by means of the surveillance system. Hitchcock did not expect or intend to catch plaintiffs on tape.

Nonetheless, after discovering the hidden camera in their office, plaintiffs filed this tort action alleging, among other things, that defendants intruded into a protected place, interest, or matter, and violated their right to privacy under both the common law and the state Constitution. The trial court granted defendants' motion for summary judgment and dismissed the case. The Court of Appeal reversed, finding triable issues that plaintiffs had suffered (1) an intrusion into a protected zone of privacy that (2) was so unjustified and offensive as to constitute a privacy violation.

Defendants argue here, as below, that, absent evidence they targeted and either viewed or recorded plaintiffs as part of the surveillance scheme, there could be, as a matter of law, no actionable invasion of privacy on an intrusion theory. Hence, they insist, the Court of Appeal erred in reinstating that claim.

We agree with defendants that the trial court properly granted their motion for summary judgment. However, we reach this conclusion for reasons more varied and nuanced than those offered by defendants.

On the one hand, the Court of Appeal did not err in determining that a jury could find the requisite intrusion. While plaintiffs' privacy interests in a shared office at work were far from absolute, they had a reasonable expectation under widely held social norms that their employer would not install video equipment capable of monitoring and recording their activities — personal and work related — behind closed doors without their knowledge or consent.

On the other hand, the Court of Appeal erroneously found a triable issue as to whether such intrusion was highly offensive and sufficiently serious to

constitute a privacy violation. Any actual surveillance was drastically limited in nature and scope, exempting plaintiffs from its reach. Defendants also were motivated by strong countervailing concerns. We therefore will reverse the Court of Appeal's judgment insofar as it allowed the privacy claim to proceed to trial.

FACTS

In September 2003, plaintiffs Hernandez and Lopez filed this suit against defendants Hillsides and Hitchcock over the use of video surveillance equipment in plaintiffs' office. The complaint set forth three related causes of action in tort, and sought compensatory and punitive damages. The first cause of action alleged an invasion of privacy, alluding to principles and authorities under both the common law (see *Shulman v. Group W Productions, Inc*. (1998) 18 Cal.4th 200 (*Shulman*)) and the state Constitution (see Cal. Const., art 1, § 1; *Hill v. National Collegiate Athletic Assn*. (1994) 7 Cal.4th 1 (*Hill*)). The other two claims alleged intentional and negligent infliction of emotional distress.

In December 2004, after the parties engaged in discovery, defendants moved for summary judgment. The motion attached numerous supporting documents. They included the declarations of both defendant Hitchcock and Tom Foster (Foster), the computer specialist at Hillsides, and excerpts from the depositions of Hitchcock and plaintiffs Hernandez and Lopez. In opposing summary judgment, plaintiffs submitted additional excerpts from the same depositions, as well as declarations each of them had prepared. Based on these submissions, the following facts appear to be essentially undisputed.

Hillsides was established in 1913, and is affiliated with the Episcopal Church. First operated as an orphanage, Hillsides later became a residential treatment center for children, ranging in age from six to 18. At the time of the events herein, 66 boys and girls lived at its facility in Pasadena.

Typically, before entering Hillsides, the children had lived in foster homes and had been the victims of emotional, physical, and sexual abuse. Such abuse included exposure to and participation in pornography. Working in conjunction with child welfare authorities, Hillsides offered programs to assist residents with academic, psychological, and behavioral problems.

The campus consisted of 12 buildings — five that housed the children, and seven that were used for administrative, academic, and other purposes. The grounds were open to the public, but certain security measures were in place. For instance, Hillsides required employees to carry photo identification at work, and issued temporary badges to all visitors. Any visitor caught wandering on the grounds without a badge was directed or escorted to the receptionist at the main entrance of the facility. The residence halls were locked at all times. Other buildings were unlocked only during regular daytime business hours. Alarms sounded for any unauthorized entry.

In addition, security personnel, or "program directors," patrolled the premises. They worked every day, around the clock, with more of them on duty during the day than at night. The program directors also monitored televised images transmitted from four cameras stationed outside some of the buildings. These exterior cameras captured and recorded certain views of the parking lot, the administration building, and the main entrance of the facility, where visitors entered. No similar camera system was permanently installed inside any building.

Plaintiffs Hernandez and Lopez performed clerical work during daytime business hours at Hillsides. When they were hired in 1996 and 1999, respectively, they signed disclosure statements and underwent background screening procedures required by law of persons working at licensed child care facilities. This process included fingerprint and criminal record checks, and an agreement to report any child abuse witnessed or suspected while working at Hillsides.

Beginning in 2001, plaintiffs shared an office in the administrative building at Hillsides. Each woman had her own desk and computer workstation. The office had three windows on exterior walls. Blinds on the windows could be opened and closed. The office also had a door that could be closed and locked. A "doggie" door near the bottom of the office door was missing its flap, creating a small, low opening into the office. Several people, besides plaintiffs, had keys to their office: five administrators, including Hitchcock, and all of the program directors. Hernandez estimated that there were five program directors. Hitchcock counted eight of them.

According to plaintiffs, they occasionally used their office to change or adjust their clothing. Hernandez replaced her work clothes with athletic wear before leaving Hillsides to exercise at the end of the day. Two or three times, Lopez raised her shirt to show Hernandez her postpregnancy figure. Both women stated in their declarations that the blinds were drawn and the door was closed when this activity occurred. Hernandez also recalled the door being locked when she changed clothes.

On or before August 22, 2002, Hillsides circulated an "E-Mail, Voicemail and Computer Systems Policy." This document stated that it was intended to prevent employees from using Hillsides' electronic communications systems in a manner that defamed, harassed, or harmed others, or that subjected the company to "significant legal exposure." Illegal and inappropriate activity was prohibited, such as accessing sexually offensive Web sites or displaying, downloading, or distributing sexually explicit material. The policy further contemplated the use of electronic "[p]ersonal passwords." However, it warned employees that they had "no reasonable expectation of privacy in any . . . use of Company computers, network and system." Along the same lines, the policy advised that all data created, transmitted, downloaded, or stored on the system was Hillsides' property,

and that the company could "monitor and record employee activity on its computers, network . . . and e-mail systems," including "e-mail messages[,] . . . files stored or transmitted[,] and . . . web sites accessed."[1]

Plaintiffs acknowledged the existence of the foregoing policy in their depositions. Indeed, both testified that, as employees of Hillsides, they were not allowed to access pornographic Web sites from their computers at work. They indicated that such conduct would conflict with Hillsides' mission to provide a safe environment for the abused and vulnerable children in its care. Hernandez described such conduct as "wrong," "illegal," and "unethical." Lopez agreed with this assessment.

In order to ensure compliance with Hillsides' computer policy and restrictions, Foster, the computer specialist, could retrieve and print a list of all Internet Web sites accessed from every computer on the premises. The network server that recorded and stored such information could pinpoint exactly when and where such Web access had occurred. In July 2002, Foster determined that numerous pornographic Web sites had been viewed in the late-night and early-morning hours from at least two different computers. One of them was located in

---

1 On November 5, 2002, shortly *after* the events herein occurred, Hitchcock circulated a one-page memorandum reminding staff that they could not use Hillsides' computers or Internet services to view or access any sexually explicit or offensive material or Web site. The memorandum further stated that the network could be made to monitor Internet use, and that unspecified "surveillance devices" could be placed wherever inappropriate computer use occurred. Attached to the memorandum was a two-page document dated November 4, 2002, entitled "Communications Acceptable Use Policy." Like its predecessor, the new policy sought to address "possible legal issues" by providing that data stored on Hillsides' computers remained company property, that password protections were required, that Hillsides could monitor the computer network at any time, and that use of its equipment to view or access sexually explicit or offensive materials or Web sites was prohibited.

the computer laboratory, or classroom. The other one sat on the desk Lopez used in the office she shared with Hernandez.

The evidence indicated that Lopez's computer could have been accessed after hours by someone other than her, because she did not always log off before going home at night. Hitchcock explained in his deposition that employees were expected to turn off their computers when leaving work at the end of the day, that a personal password was required to log onto the computer again after it had been turned off, and that this policy was communicated orally to employees when their computers were first assigned. He admitted that he did not remind plaintiffs of this procedure before taking the surveillance steps at issue here. Nonetheless, Lopez noted in her declaration that "[o]nce [her] computer at Hillsides was turned off, it required the input of a secret password in order to be accessed again."

Foster told defendant Hitchcock about the inappropriate Internet use, and showed him printouts listing the pornographic Web sites that had been accessed. Given the odd hours at which such activity had occurred, Hitchcock surmised that the perpetrator was a program director or other staff person who had unfettered access to Hillsides in the middle of the night. Hitchcock did not blame any of the children, because they would have been under supervision and asleep in the residence halls at the time. Nor did he suspect plaintiffs. They typically were gone from the premises when the impermissible nighttime computer use occurred.

In light of these circumstances, Hitchcock decided to use video equipment Hillsides already had in its possession to record the perpetrator in the act of using the computers at night. He told other administrators about the problem and his surveillance plan. Hitchcock explained in both his deposition and declaration that

he sought to protect the children from any staff person who might expose them to pornography, emphasizing the harm they had endured before entering Hillsides.[2]

With Foster's assistance, Hitchcock initially installed the video equipment in the computer laboratory from which some of the pornographic Web sites had been accessed. However, because so many people used the laboratory for legitimate reasons during and after business hours, Hitchcock decided instead to conduct surveillance in the office that plaintiffs shared. He did not inform plaintiffs of this decision. He reasoned that the more people who knew and "gossiped" about the plan, the greater the chance the culprit would hear about it and never be identified or stopped.

Hence, at some point during the first week of October 2002, Hitchcock and Foster installed video recording equipment in plaintiffs' office and in a storage room nearby. First, in plaintiffs' office, they positioned a camera on the top shelf

---

[2] Plaintiffs claim defendants never established that an unidentified employee or other intruder accessed pornographic Web sites from Lopez's computer, thereby risking harm to Hillsides' residents or operations. Plaintiffs assume that declarations filed by Hitchcock and Foster containing such factual assertions are incompetent and inadmissible on numerous grounds, and that no other similar evidence exists. We reject the argument and its premise. Plaintiffs do not make clear through an analysis of the pleadings below, or specific record citations, whether the present evidentiary objections are the same as those made and overruled in the trial court. In the summary judgment context, we have declined similar requests to disregard evidence based on objections "in this court lack[ing] adequate argument and support." (*Lyle v. Warner Brothers Television Productions* (2006) 38 Cal.4th 264, 277, fn. 3.) In any event, the substance of the information contained in the challenged declarations appears in Hitchcock's deposition. As best we can determine from the record, plaintiffs never contested such deposition testimony in the trial court. Their failure to do so prevents them from complaining about the admission of the evidence in deposition form. (E.g., *Miller v. Department of Corrections* (2005) 36 Cal.4th 446, 452, fn. 3; see Code Civ. Proc., § 437c, subds. (b)(5) & (d) [evidentiary objections not made at summary judgment hearing are waived].)

of a bookcase, among some plants, where it apparently was obscured from view. They also tucked a motion detector into the lap of a stuffed animal or toy sitting on a lower shelf of the same bookcase. Second, these devices connected remotely to a television that Hitchcock and Foster moved into the storage room. A videocassette recorder was built into the unit. The television had a 19-inch monitor on which images could be viewed.

Hitchcock explained the system's operation in his deposition as follows: Through wireless technology, the camera broadcast images to the television monitor, and the motion detector operated the videocassette recorder. The recorder would "run as long as there [was] motion in that room to keep it activated." Once installed in plaintiffs' office, both the camera and the motion detector were always plugged into the electrical system, and therefore were capable of operating "all the time." However, in order for the camera to display an image on the monitor, and for the motion detector to trigger a recording of that image, a wireless "receptive device" in the storage room needed to be plugged into — i.e., "connected" and "engaged" to — the television set. Hitchcock further testified that if these wireless receptors were unplugged, disconnected, or disengaged, then the camera and motion detector were not "activated," and nothing was displayed or recorded on the television equipment.

Hitchcock was not the only person with access to the storage room and the video surveillance equipment inside. Plaintiffs each stated in their declarations that "several supervisory employees and program directors had keys and access to that storage room." Hitchcock stated in his deposition that he knew of only two employees with keys to the storage room, Susanne Crummey and Ramona McGee, and that the location was locked and "secure." Crummey and another administrator, Stacey Brake, were the only people other than Hitchcock and Foster

who knew that the video equipment in the storage room was specifically set up to monitor plaintiffs' office.

Hitchcock rarely activated the camera and motion detector in plaintiffs' office, and never did so while they were there. His deposition testimony addressed these circumstances as follows: On three occasions, Hitchcock connected the wireless receptors to the television in the storage room after plaintiffs left work for the day, and then disconnected the receptors the next morning, before plaintiffs returned to work. On one such morning, he also removed the camera from the office, and returned it later, when plaintiffs were gone for the night. In short, the camera and motion detector were always disabled during the workday, such that "there was no picture showing" and "no recording going on" while plaintiffs were in their office. Hitchcock further stated that between installation of the equipment in early October 2002, and his decision to remove it three weeks later, no one was videotaped or caught using the computer in plaintiffs' office. He assumed that the culprit had learned about the camera and stopped engaging in unauthorized activity.**3**

---

3 Plaintiffs insist here, as on appeal, that triable issues exist as to whether they were viewed or recorded because (1) the video surveillance equipment was "always on," (2) the television monitor in the storage room displayed a "continuous" live image of the interior of plaintiffs' office, and (3) "recording was possible" even when nothing triggered the motion detector. However, Hitchcock's deposition defeats these assertions, and plaintiffs presented no contrary evidence below. As we have seen, Hitchcock testified that no image was displayed or recorded on the television unless the remote controls in the storage room were connected, and that he connected them and activated the surveillance system only three times, at night, when plaintiffs were not at work. He also stated that no recording occurred unless movement was first sensed by the motion detector in its activated state, and that neither plaintiffs nor any third person appeared on the videotape. Indeed, the Court of Appeal reached a similar conclusion concerning the undisputed nature of Hitchcock's testimony about the "recording and/or

(footnote continued on next page)

Meanwhile, about 4:30 p.m. on Friday, October 25, 2002, plaintiffs discovered the video equipment in their office. A red light on the motion detector flashed at the time. The cord attached to the camera was plugged into the wall and was hot to the touch.

Shocked by the discovery, plaintiffs immediately reported it to two supervisors, Sylvia Levitan and Toni Aikins. Levitan called Hitchcock, who was at home. A program director helped remove the camera from plaintiffs' office and lock it in Levitan's office for safekeeping.

A short time later, Hitchcock called Hernandez in her office. He apologized for installing the camera, and said the surveillance was not aimed at plaintiffs, but at an intruder who had used Lopez's computer to access inappropriate Web sites. Hernandez expressed concern that she was videotaped while changing her clothes or that "personal stuff" in her office was somehow disturbed. Hitchcock replied by assuring Hernandez that "the only time we activated that camera and the video recorder was after you left at night and [we] deactivated the two devices before you came to work in the morning. [¶] . . . [A]t no time did [we] ever capture [you] or [Lopez] on the tape." During this conversation, Hitchcock asked to speak with Lopez, but learned she had left the office for the day. Hitchcock twice tried contacting Lopez over the next two days, which fell on a weekend, but did not reach her.

(footnote continued from previous page)

viewing" of plaintiffs. Plaintiffs did not seek rehearing or modification on this or any other factual point, and are barred from complaining about it now. (See Cal. Rules of Court, rule 8.500(c)(2) [Court of Appeal's statement of facts is accepted on review absent rehearing petition challenging alleged misstatements].)

Plaintiffs did not return to work until Wednesday, October 30, 2002. That morning, they met for 30 minutes with both defendant Hitchcock and Aikins, their supervisor. Hitchcock essentially repeated the substance of his prior conversation with Hernandez. He apologized and explained the reason for installing the camera in plaintiffs' office, and assured them that they were not the target of the surveillance and had not been videotaped.

During this meeting, Lopez asked to see the surveillance videotape. Hitchcock agreed. The group went to Hitchcock's office and watched the tape on his television set. According to the depositions of both plaintiffs, there was not much to see. No one appeared on the tape except for Hitchcock, who was briefly seen setting up the camera and moving around inside plaintiffs' office. The only other recorded images were of Lopez's empty desk and computer, the surrounding work area, some closets, and the entrance to the office. No sound accompanied the playing of the tape. Hitchcock never indicated to plaintiffs that any audio recording was made, or that the camera could record sound.[4]

Based on the foregoing facts, the trial court found no triable issue as to any cause of action stated in the complaint, granted summary judgment in defendants' favor, and dismissed the action. The court agreed with defendants that there had been no intrusion on plaintiffs' reasonable expectations of privacy. In this regard, the court emphasized the lack of evidence that plaintiffs "were secretly observed or recorded by way of a hidden camera located in their office. . . . [I]t is undisputed that the camera was only connected to a video monitor and to

---

[4] This court has reviewed a copy of the videotape provided by plaintiffs' counsel, which conforms to the parties' descriptions in the trial court. As to the camera, Lopez remarked in her deposition that, based on her own Internet research, Hitchcock's model had an audio recording feature. She did not otherwise describe the camera or explain her conclusion.

recording equipment on three occasions, all of which occurred after working hours when Plaintiffs were not present." Alternatively, the trial court concluded that any privacy expectations plaintiffs had in their joint office were "diminished," and were "overcome by Defendants' right to a safe environment for its children."

The Court of Appeal reversed as to the invasion-of-privacy count. Critical to the court's analysis on appeal was the placement in plaintiffs' office of a functioning hidden camera, capable of transmitting images that could be viewed or recorded by anyone who had access to the storage room and who activated the wireless remote controls. According to the appellate court, plaintiffs had a reasonable expectation to be free from this kind of intrusion in the workplace, notwithstanding evidence that they were never viewed or recorded and that they worked in a shared office to which others had access. For similar reasons, and even assuming defendants were merely trying to stop an intruder's inappropriate use of the computers at night, the Court of Appeal concluded that defendants' conduct was highly offensive. However, for reasons not challenged or relevant here, the Court of Appeal agreed with the trial court that plaintiffs had not presented triable claims for intentional and negligent infliction of emotional distress, and that such counts should be dismissed.

Defendants petitioned for review on the ground the Court of Appeal erred in not affirming the judgment in its entirety and reversing the trial court's dismissal of the invasion-of-privacy count. We granted review.[5]

---

[5] We note that the Employers Group and the California Employment Law Council have jointly filed a brief as amici curiae in support of defendant Hillsides.

DISCUSSION

A. Summary Judgment Rules

A grant of summary judgment is proper where it appears no triable issues of material fact exist, and judgment is warranted as a matter of law. (Code of Civ. Proc., § 437c, subd. (c); *Miller v. Department of Corrections, supra,* 36 Cal.4th 446, 460.) As the moving party, the defendant must show that the plaintiff "has not established, and cannot reasonably expect to establish, a prima facie case" on one or more elements of the cause of action. (*Saelzler v. Advanced Group 400* (2001) 25 Cal.4th 763, 768; accord, *Wilson v. 21st Century Ins. Co*. (2007) 42 Cal.4th 713, 720.) The reviewing court independently examines the record and considers all of the evidence set forth in the moving and opposing papers except that as to which objections have been made and sustained. (*Lyle v. Warner Brothers Television Productions, supra*, 38 Cal.4th 264, 274; *Guz v. Bechtel National, Inc*. (2000) 24 Cal.4th 317, 334; see *id*. at p. 335, fn. 7.)

B. General Privacy Principles

Defendants (joined by their amici curiae) argue here, as below, that they did nothing wrong in attempting to videotape a nighttime intruder using the computer in plaintiffs' office, because no private information about plaintiffs was obtained. Defendants insist that plaintiffs, not being the intended targets of the surveillance plan, were never viewed or recorded, and thereby suffered no serious or actionable intrusion into their private domain. Plaintiffs disagree and urge us to adopt the Court of Appeal's approach in the present case. They insist that defendants were able to view and record plaintiffs at will, without their knowledge or consent, and unjustifiably deprived them of the privacy they reasonably expected to have while working behind closed doors in their shared office.

The foregoing arguments have been framed throughout this action in terms of both the common law and the state Constitution. These two sources of privacy

protection "are not unrelated" under California law. (*Shulman, supra*, 18 Cal.4th 200, 227; accord, *Hill, supra*, 7 Cal.4th 1, 27; but see *Katzberg v. Regents of University of California* (2002) 29 Cal.4th 300, 313, fn. 13 [suggesting it is an open question whether the state constitutional privacy provision, which is otherwise self-executing and serves as the basis for injunctive relief, can also provide direct and sole support for a damages claim].) Such privacy principles provide the framework for our analysis, as follows.

A privacy violation based on the common law tort of intrusion has two elements. First, the defendant must intentionally intrude into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy. Second, the intrusion must occur in a manner highly offensive to a reasonable person. (*Shulman, supra*, 18 Cal.4th 200, 231, approving and following Rest.2d Torts, § 652B; *Miller v. National Broadcasting Co*. (1986) 187 Cal.App.3d 1463, 1482 (*Miller*); accord, *Taus v. Loftus* (2007) 40 Cal.4th 683, 724-725, 731 (*Taus*).) These limitations on the right to privacy are not insignificant. (*Miller, supra*, at p. 1482.) Nonetheless, the cause of action recognizes a measure of personal control over the individual's autonomy, dignity, and serenity. (*Shulman, supra*, at p. 231.) The gravamen is the mental anguish sustained when both conditions of liability exist. (*Miller, supra*, pp. 1484-1485.)

As to the first element of the common law tort, the defendant must have "penetrated some zone of physical or sensory privacy . . . or obtained unwanted access to data" by electronic or other covert means, in violation of the law or social norms. (*Shulman, supra*, 18 Cal.4th 200, 232; see *id*. at pp. 230-231.) In either instance, the expectation of privacy must be "objectively reasonable." (*Id*. at p. 232.) In *Sanders v. American Broadcasting Companies* (1999) 20 Cal.4th 907 (*Sanders*), a leading case on workplace privacy that we discuss further below, this court linked the reasonableness of privacy expectations to such factors as (1)

the identity of the intruder, (2) the extent to which other persons had access to the subject place, and could see or hear the plaintiff, and (3) the means by which the intrusion occurred. (*Id*. at p. 923; see *Shulman, supra*, 18 Cal.4th 200, 233-235.)

The second common law element essentially involves a "policy" determination as to whether the alleged intrusion is "highly offensive" under the particular circumstances. (*Taus, supra*, 40 Cal.4th 683, 737.) Relevant factors include the degree and setting of the intrusion, and the intruder's motives and objectives. (*Shulman, supra*, 18 Cal.4th 200, 236; *Miller, supra*, 187 Cal.App.3d 1463, 1483-1484.) Even in cases involving the use of photographic and electronic recording devices, which can raise difficult questions about covert surveillance, "California tort law provides no bright line on ['offensiveness']; each case must be taken on its facts." (*Shulman, supra*, at p. 237.)

The right to privacy in the California Constitution sets standards similar to the common law tort of intrusion. (*Hill, supra*, 7 Cal.4th 1, 27.)[6] Under this provision, which creates at least a limited right of action against both private and government entities (*id*. at p. 20), the plaintiff must meet several requirements.

First, he must possess a legally protected privacy interest. (*Hill, supra*, 7 Cal.4th 1, 35.) These interests include "conducting personal activities without observation, intrusion, or interference" (*ibid*.), as determined by "established social norms" derived from such sources as the "common law" and "statutory enactment." (*Id*. at p. 36.) Second, the plaintiff's expectations of privacy must be reasonable. This element rests on an examination of "customs, practices, and

---

6 Article I, section 1 of the California Constitution states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

physical settings surrounding particular activities" (*ibid*.), as well as the opportunity to be notified in advance and consent to the intrusion. (*Id*. at pp. 36-37.) Third, the plaintiff must show that the intrusion is so serious in "nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms." (*Id*. at p. 37; accord, *Sheehan v. San Francisco 49ers, Ltd.* (2009) 45 Cal.4th 992, 998 (*Sheehan*); *Pioneer Electronics* (*USA*), *Inc. v. Superior Court* (2007) 40 Cal.4th 360, 370-371 (*Pioneer*).)

Hill and its progeny further provide that no constitutional violation occurs, i.e., a "defense" exists, if the intrusion on privacy is justified by one or more competing interests. (*Hill, supra*, 7 Cal.4th 1, 38.) For purposes of this balancing function — and except in the rare case in which a "fundamental" right of personal autonomy is involved — the defendant need not present a " 'compelling' " countervailing interest; only "general balancing tests are employed." (*Id*. at p. 34.) To the extent the plaintiff raises the issue in response to a claim or defense of competing interests, the defendant may show that less intrusive alternative means were not reasonably available. (*Id*. at p. 38.) A relevant inquiry in this regard is whether the intrusion was limited, such that no confidential information was gathered or disclosed. (*Ibid*.; accord, *Sheehan, supra*, 45 Cal.4th 992, 998-999; *Pioneer, supra*, 40 Cal.4th 360, 371.)

In light of the foregoing, we will assess the parties' claims and the undisputed evidence under the rubric of both the common law and constitutional tests for establishing a privacy violation. Borrowing certain shorthand language from *Hill, supra,* 7 Cal.4th 1, which distilled the largely parallel elements of these two causes of action, we consider (1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification and other relevant interests. (*Id*. at pp. 27, 34.)

C. Intrusion upon Reasonable Privacy Expectations

For reasons we now explain, we cannot conclude as a matter of law that the Court of Appeal erred in finding a prima facie case on the threshold question whether defendants' video surveillance measures intruded upon plaintiffs' reasonable expectations of privacy. Plaintiffs plausibly maintain that defendants cannot prevail on this element of the cause of action simply because they "never intended to view or record" plaintiffs, or because defendants did not "capture [plaintiffs'] images at all." Other significant factors not considered by defendants point favorably in plaintiffs' direction on this issue.

Our analysis starts from the premise that, while privacy expectations may be significantly diminished in the workplace, they are not lacking altogether. In *Sanders, supra,* 20 Cal.4th 907, a reporter working undercover for a national broadcasting company obtained employment alongside the plaintiff as a telepsychic, giving "readings" to customers over the phone. The reporter then secretly videotaped and recorded interactions with the plaintiff and other psychics using a small camera hidden in her hat and a microphone attached to her brassiere. The taping occurred in a large room containing 100 cubicles that were open on one side and on top, and from which coworkers could be seen and heard nearby. Visitors could not enter this area without permission from the front desk. Ultimately, the plaintiff sued the reporter and the broadcasting company for violating his privacy after one of his secretly taped conversations aired on television. A jury verdict in the plaintiff's favor was reversed on appeal. The appellate court concluded that the plaintiff could not reasonably expect that actions and statements witnessed by coworkers would remain private and not be disclosed to third parties. (*Id.* at pp. 911-913 & fn. 1.)

Relying on the elements of the intrusion tort set forth in *Shulman, supra,* 18 Cal.4th 200, we disagreed with the Court of Appeal in *Sanders,* and reversed the

judgment. This court emphasized that privacy expectations can be reasonable even if they are not absolute. "[P]rivacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law." (*Sanders, supra,* 20 Cal.4th 907, 916.)

In adopting this refined approach, *Sanders* highlighted various factors which, either singly or in combination, affect societal expectations of privacy. One factor was the identity of the intruder. (*Sanders, supra,* 20 Cal.4th 907, 918, 923.) We noted that the plaintiff in that case, and other employees, were deliberately misled into believing that the defendant reporter was a colleague, and had no reason to suspect she worked undercover to secretly tape their interactions for use in a national television program. (*Id*. at p. 921.)

Also relevant in *Sanders, supra,* 20 Cal.4th 907, was the nature of the intrusion (*id*. at p. 918), meaning, *both* the extent to which the subject interaction could be "seen and overheard" *and* the "means of intrusion." (*Id*. at p. 923.) These factors weighed heavily in the plaintiff's favor: "[T]he possibility of being overheard by coworkers does not, as a matter of law, render unreasonable an employee's expectation that his or her interactions within a nonpublic workplace will not be videotaped in secret by a journalist." (*Ibid*.) We distinguished the situation in which "the workplace is regularly open to entry or observation by the public or press," or the subject interaction occurred between either the proprietor or employee of a business and a "customer" who walks in from the street. (*Ibid*.)

The present case, of course, does not involve an imposter or "stranger to the workplace" who surreptitiously recorded and videotaped conversations that were later published without the speaker's consent. (*Sanders, supra,* 20 Cal.4th 907, 918.) Nor does it involve commercial interactions between the representatives of

a business and its customers or other members of the public. Rather, defendants represent a private *employer* accused of installing electronic equipment that gave it the capacity to secretly watch and record employee activities behind closed doors in an office to which the general public had limited access. As we discuss later with respect to the "offensiveness" element of plaintiffs' claim, an employer may have sound reasons for monitoring the workplace, and an intrusion upon the employee's reasonable privacy expectations may not be egregious or actionable under the particular circumstances. However, on the threshold question whether such expectations were infringed, decisional law suggests that is the case here.

Consistent with *Sanders, supra*, 20 Cal.4th 907, 922, which asks whether the employee could be "overheard or observed" by others when the tortious act allegedly occurred, courts have examined the physical layout of the area intruded upon, its relationship to the workplace as a whole, and the nature of the activities commonly performed in such places. At one end of the spectrum are settings in which work or business is conducted in an open and accessible space, within the sight and hearing not only of coworkers and supervisors, but also of customers, visitors, and the general public. (See *Wilkins v. National Broadcasting Co*. (1999) 71 Cal.App.4th 1066, 1072-1073, 1078 [holding for purpose of common law intrusion tort that businessmen lacked privacy in lunch meeting secretly videotaped on crowded outdoor patio of public restaurant]; see also *Acosta v. Scott Labor LLC* (N.D.Ill. 2005) 377 F.Supp.2d 647, 649, 652 [similar conclusion as to employer secretly videotaped by disgruntled employee in common, open, and exposed area of workplace]; *Melder v. Sears, Roebuck and Co*. (La.Ct.App. 1999) 731 So.2d 991, 994, 1001 [similar conclusion as to department store employee captured on video cameras used to monitor customers as they shopped].)

At the other end of the spectrum are areas in the workplace subject to restricted access and limited view, and reserved exclusively for performing bodily

functions or other inherently personal acts. (See *Trujillo v. City of Ontario* (C.D.Cal. 2006) 428 F.Supp.2d 1094, 1099-1100, 1103, 1119-1122 (*Trujillo*) [recognizing that employees have common law and constitutional privacy interests while using locker room in basement of police station, and can reasonably expect that employer will not intrude by secretly videotaping them as they undress]; see also *Doe by Doe v. B.P.S. Guard Services, Inc*. (8th Cir. 1991) 945 F.2d 1422, 1424, 1427 (*Doe*) [similar conclusion as to models who were secretly viewed and videotaped while changing clothes behind curtained area at fashion show]; *Liberti v. Walt Disney World Co*. (M.D.Fla. 1995) 912 F.Supp. 1494, 1499, 1506 (*Liberti*) [similar conclusion as to dancers who were secretly viewed and videotaped while changing clothes and using restroom in dressing room at work].)

The present scenario falls between these extremes. (Cf. *Sacramento County Deputy Sheriffs' Assn. v. County of Sacramento* (1996) 51 Cal.App.4th 1468, 1482, 1487 [rejecting common law intrusion claim of jail employee secretly videotaped while handling inmate property based on accessibility of his office to others and heightened security concerns inherent in custodial setting]; see also *Marrs v. Marriott Corp*. (D.Md. 1992) 830 F.Supp. 274, 283 [similar conclusion as to security guard secretly videotaped while breaking into colleague's locked desk in open office used as common area by entire staff].)

Plaintiffs plausibly claim that Hillsides provided an enclosed office with a door that could be shut and locked, and window blinds that could be drawn, to allow the occupants to obtain some measure of refuge, to focus on their work, and to escape visual and aural interruptions from other sources, including their employer. Such a protective setting generates legitimate expectations that not all activities performed behind closed doors would be clerical and work related. As suggested by the evidence here, employees who share an office, and who have four walls that shield them from outside view (albeit, with a broken "doggie" flap

on the door), may perform grooming or hygiene activities, or conduct personal conversations, during the workday. Privacy is not wholly lacking because the occupants of an office can see one another, or because colleagues, supervisors, visitors, and security and maintenance personnel have varying degrees of access. (See *Sanders, supra*, 20 Cal.4th 907, 917 [" 'visibility to some people does not strip [away] the right to remain secluded from others' "]; *id.* at pp. 918-919 [" 'business office need not be sealed to offer its occupant a reasonable degree of privacy' "].)

Regarding another relevant factor in *Sanders, supra*, 20 Cal.4th 907, 923, the "means of intrusion," employees who retreat into a shared or solo office, and who perform work and personal activities in relative seclusion there, would not reasonably expect to be the subject of televised spying and secret filming by their employer. As noted, in assessing social norms in this regard, we may look at both the "common law" and "statutory enactment." (*Hill, supra*, 7 Cal.4th 1, 36.)

Courts have acknowledged the intrusive effect for tort purposes of hidden cameras and video recorders in settings that otherwise seem private. It has been said that the "unblinking lens" can be more penetrating than the naked eye with respect to "duration, proximity, focus, and vantage point." (*Cowles v. State* (Alaska 2001) 23 P.3d 1168, 1182 (dis. opn. of Fabe, J.).) Such monitoring and recording denies the actor a key feature of privacy — the right to control the dissemination of his image and actions. (See *Shulman, supra*, 18 Cal.4th 200, 235.) We have made clear that the " 'mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone.' " (*Sanders, supra*, 20 Cal.4th 907, 916.)

Not surprisingly, we discern a similar legislative policy against covert monitoring and recording that intrudes — or threatens to intrude — upon visual privacy. Some statutes criminalize the use of camcorders, motion picture cameras,

or photographic cameras to violate reasonable expectations of privacy in specified areas in which persons commonly undress or perform other intimate acts. Liability exists, under certain circumstances, where the lens allows the intruder to "look[ ]" into or "view[ ]" the protected area. (Pen. Code, § 647, subd. (j)(1).)[7] Of course, the intruder also cannot "secretly videotape, film, photograph, or record" anyone in that private place where various conditions exist. (*Id.*, subd. (j)(3)(A); see *Trujillo, supra,* 428 F.Supp.2d 1094, 1119 [statute intended to protect visual privacy of persons in various states of undress].)

Other statutes authorize civil damages for certain invasions of privacy that involve either a physical trespass or other offensive conduct for the purpose of capturing a picture of someone engaged in personal or familial activities. The focus of such provisions is on the "intent to capture" a "visual image" (Civ. Code,

---

[7] Penal Code section 647 imposes misdemeanor liability for disorderly conduct. Its diverse provisions include subdivision (j)(1), which applies to "[a]ny person who looks through a hole or opening, into, or otherwise views, by means of any instrumentality, including, but not limited to, a periscope, telescope, binoculars, camera, motion picture camera, or camcorder, the interior of a bedroom, bathroom, changing room, fitting room, dressing room, or tanning booth, or the interior of any other area in which the occupant has a reasonable expectation of privacy, with the intent to invade the privacy of a person or persons inside."

Subdivision (j)(3)(A) of Penal Code section 647 applies to "[a]ny person who uses a concealed camcorder, motion picture camera, or photographic camera of any type, to secretly videotape, film, photograph, or record by electronic means, another, identifiable person who may be in a state of full or partial undress, for the purpose of viewing the body of, or the undergarments worn by, that other person, without the consent or knowledge of that other person, in the interior of a bedroom, bathroom, changing room, fitting room, dressing room, or tanning booth, or the interior of any other area in which that other person has a reasonable expectation of privacy, with the intent to invade the privacy of that other person."

§ 1708.8, subd. (a)), or on the "attempt" to do so. (*Id*., subd. (b).)[8] Failure to capture or record the subject image is no defense to a statutory violation in this context. (*Id*., subd. (j); see *Richardson-Tunnell v. Schools Ins. Program for Employees* (*SIPE*) (2007) 157 Cal.App.4th 1056, 1063 [statute protects against aggressive, paparazzi-like, behavior of tabloid journalists].)

As emphasized by defendants, the evidence shows that Hitchcock never viewed or recorded plaintiffs inside their office by means of the equipment he installed both there and in the storage room. He also did not intend or attempt to do so, and took steps to avoid capturing them on camera and videotape. While such factors bear on the offensiveness of the challenged conduct, as discussed below, we reject the defense suggestion that they preclude us from finding the

---

8 Civil Code section 1708.8 authorizes compensatory and punitive damages and injunctive relief for acts constituting a physical or constructive invasion of privacy. Subdivision (a) states: "A person is liable for physical invasion of privacy when the defendant knowingly enters onto the land of another person without permission or otherwise committed a trespass in order to physically invade the privacy of the plaintiff with the intent to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity and the physical invasion occurs in a manner that is offensive to a reasonable person."

Subdivision (b) of Civil Code section 1708.8 states: "A person is liable for constructive invasion of privacy when the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used."

Subdivision (j) of Civil Code section 1708.8 states: "It is not a defense to a violation of this section that no image, recording, or physical impression was captured or sold."

requisite intrusion in the first place. (See *Shulman, supra*, 18 Cal.4th 200, 232 [requiring *either* a physical or sensory penetration into a private place or matter, *or* the gaining of unwanted access to private information].)

In particular, Hitchcock hid the video equipment in plaintiffs' office from view in an apparent attempt to prevent anyone from discovering, avoiding, or dismantling it. He used a camera and motion detector small enough to tuck inside and around decorative items perched on different bookshelves, both high and low. Plaintiffs presumably would have been caught in the camera's sights if they had returned to work after hours, or if Hitchcock had been mistaken about them having left the office when he activated the system. Additionally, except for the one day in which Hitchcock removed the camera from plaintiffs' office, the means to activate the monitoring and recording functions were available around the clock, for three weeks, to anyone who had access to the storage room. Assuming the storage room was locked, as many as eight to 11 employees had keys under plaintiffs' version of the facts (depending upon the total number of program directors at Hillsides).

In a related vein, plaintiffs cannot plausibly be found to have received warning that they would be subjected to the risk of such surveillance, or to have agreed to it in advance. We have said that notice of and consent to an impending intrusion can "inhibit reasonable expectations of privacy." (*Hill, supra*, 7 Cal.4th 1, 36; accord, *Sheehan, supra*, 45 Cal.4th 992, 1000-1001.) Such factors also can " ' "limit [an] intrusion upon personal dignity" ' " by providing an opportunity for persons to regulate their conduct while being monitored. (*Hill, supra*, at p. 36.) Here, however, the evidence shows that no one at Hillsides told plaintiffs that someone had used Lopez's computer to access pornographic Web sites. Nor were they told that Hitchcock planned to install surveillance equipment inside their office to catch the perpetrator on television and videotape.

Moreover, nothing in Hillsides' written computer policy mentioned or even alluded to the latter scenario. As noted earlier, the version in effect at the relevant time made clear that any monitoring and recording of employee activity, and any resulting diminution in reasonable privacy expectations, were limited to "use of Company computers" in the form of "e-mail" messages, electronic "files," and "web site" data. Foster performed this administrative function when he used the network server to produce the list of pornographic Web sites accessed in both the computer laboratory and Lopez's office, and showed such computer-generated data to Hitchcock. There is no evidence that employees like plaintiffs had any indication that Hillsides would take the next drastic step and use cameras and recording devices to view and videotape employees sitting at their desks and computer workstations, or moving around their offices within camera range.

In sum, the undisputed evidence seems clearly to support the first of two basic elements we have identified as necessary to establish a violation of privacy as alleged in plaintiffs' complaint. Defendants secretly installed a hidden video camera that was both operable and operating (electricity-wise), and that could be made to monitor and record activities inside plaintiffs' office, at will, by anyone who plugged in the receptors, and who had access to the remote location in which both the receptors and recording equipment were located. The workplace policy, that by means within the computer system itself, plaintiffs would be monitored about the pattern and use of Web sites visited, to prevent abuse of Hillsides' computer system, is distinguishable from and does not necessarily create a social norm that in order to advance that same interest, a camera would be placed inside their office, and would be aimed toward a computer workstation to capture all

human activity occurring there. Plaintiffs had no reasonable expectation that their employer would intrude so tangibly into their semi-private office.[9]

D. Offensiveness/Seriousness of the Privacy Intrusion

Plaintiffs must show more than an intrusion upon reasonable privacy expectations. Actionable invasions of privacy also must be "highly offensive" to a reasonable person (*Shulman, supra*, 18 Cal.4th 200, 231; see *id*. at p. 236), and "sufficiently serious" and unwarranted as to constitute an "egregious breach of the social norms." (*Hill, supra*, 7 Cal.4th 1, 37.) Defendants claim that, in finding a triable issue in this regard, the Court of Appeal focused too narrowly on the mere

---

9 In our analysis, we have sidestepped cases involving claims that searches by governmental agents and employers for evidence of misconduct or criminality in the workplace violate an employee's reasonable expectations of privacy under the Fourth Amendment of the federal Constitution. (See *O'Connor v. Ortega* (1987) 480 U.S. 709, 714-719 (plur. opn. of O'Connor, J.); *id*. at pp. 730-731 (conc. opn. of Scalia, J.); *id*. at pp. 732 (dis. opn. of Blackmun, J.); *Mancusi v. DeForte* (1968) 392 U.S. 364, 369.) Recognizing the special concerns involved in defining a private citizen's protection against governmental intrusion, and the government's unique interest in investigating and suppressing criminal activity, we have said that employee expectations of privacy against government searches are "not directly applicable" in the privacy tort context. (*Sanders, supra*, 20 Cal.4th 907, 919, fn. 3.) Here, as elsewhere, we do not suggest that the same standards necessarily apply in both settings. (*Ibid*.) We note, however, that where a governmental search intrudes upon an enclosed office or other protected workplace, and where covert video surveillance is involved, limited but reasonable expectations of privacy may exist under the Fourth Amendment. (Compare *U.S. v. Taketa* (9th Cir. 1991) 923 F.2d 665, 674-678 [disapproving admission of warrantless secret videotape made in shared office of airport]; and *State v. Bonnell* (Hawaii 1993) 856 P.2d 1265, 1275-1277 [upholding suppression of warrantless secret videotape made in employee break room of post office], with *Vega-Rodriguez v. Puerto Rico Telephone Co*. (1st Cir. 1997) 110 F.3d 174, 178-182 [allowing visible videotaping in open and undivided communications center of phone company]; and *Nelson v. Salem State College* (Mass. 2006) 845 N.E.2d 338, 346-347 [allowing secret videotaping in open area of business development office accessible to general public].)

presence of a functioning camera in plaintiffs' office during the workday, and on the inchoate risk that someone would sneak into the locked storage room and activate the monitoring and recording devices. Defendants imply that under a broader view of the relevant circumstances, no reasonable jury could find in plaintiffs' favor and impose liability on this evidentiary record. We agree.

For guidance, we note that this court has previously characterized the "offensiveness" element as an indispensible part of the privacy analysis. It reflects the reality that "[n]o community could function if every intrusion into the realm of private action" gave rise to a viable claim. (*Hill, supra*, 7 Cal.4th 1, 37.) Hence, no cause of action will lie for accidental, misguided, or excusable acts of overstepping upon legitimate privacy rights. (*Miller, supra*, 187 Cal.App.3d 1463, 1483-1484.) In light of such pragmatic policy concerns (see *Taus, supra*, 40 Cal.4th 683, 737), a court determining whether this requirement has been met as a matter of law examines all of the surrounding circumstances, including the "degree and setting" of the intrusion and "the intruder's 'motives and objectives.' " (*Shulman, supra*, 18 Cal.3d 200, 236, quoting and following *Miller, supra*, 187 Cal.App.3d at pp. 1483-1484.) Courts also may be asked to decide whether the plaintiff, in attempting to defeat a claim of competing interests, has shown that the defendant could have minimized the privacy intrusion through other reasonably available, less intrusive means. (*Hill, supra*, 7 Cal.4th at p. 38.)

1. Degree and Setting of Intrusion. This set of factors logically encompasses the place, time, and scope of defendants' video surveillance efforts. In this case, they weigh heavily against a finding that the intrusion upon plaintiffs' privacy interests was highly offensive or sufficiently serious to warrant liability.

In context, defendants took a measured approach in choosing the location to videotape the person who was misusing the computer system. Evidently, plaintiffs' office was *not* the preferred spot. Hitchcock initially tried to capture the

culprit in the computer laboratory. Based on the consistently high level of human traffic he described there, the laboratory apparently was far more accessible and less secluded than plaintiffs' office. The surveillance equipment was moved to the latter location only after Hitchcock determined it was too difficult to pinpoint who was using computers inappropriately in the open, more public laboratory setting.

Defendants' surveillance efforts also were largely confined to the area in which the unauthorized computer activity had occurred. Once the camera was placed in plaintiffs' office, it was aimed towards Lopez's desk and computer workstation. There is no evidence that Hitchcock intended or attempted to include Hernandez's desk in camera range. We can reasonably infer he avoided doing so, because no improper computer use had been detected there.

Likewise, access to the storage room and knowledge of the surveillance equipment inside were limited. A total of two people other than Hitchcock and Foster (Susanne Crummey and Stacey Brake) knew that the television/recorder was set up to monitor plaintiffs' office. Only one of them (Crummey) had a key to the lock on the storage room door. The spot was relatively remote and secure.

Timing considerations favor defendants as well. After being moved to plaintiffs' office and the storage room, the surveillance equipment was operational during a fairly limited window of time. Hitchcock decided to remove the equipment (and plaintiffs coincidentally discovered it) a mere 21 days later, during which time no one had accessed Lopez's computer for pornographic purposes. We can infer from the undisputed evidence that Hitchcock kept abreast of his own monitoring activities, and did not expose plaintiffs to the risk of covert visual monitoring or video recording any longer than was necessary to determine that his plan would not work, and that the culprit probably had been scared away.

Defendants' actual surveillance activities also were quite limited in scope. On the one hand, the camera and motion detector in plaintiffs' office were always

plugged into the electrical circuit and capable of operating the entire time they were in place. On the other hand, Hitchcock took the critical step of connecting the wireless receptors and activating the system only three times. At most, he was responsible for monitoring and recording inside of plaintiffs' office an average of only once a week for three weeks. Such measures were hardly excessive or egregious. (Cf. *Wolfson v. Lewis* (E.D.Pa. 1996) 924 F.Supp. 1413, 1420 [electronic surveillance that is persistent and pervasive may constitute a tortious intrusion on privacy even when conducted in a public or semi-public place].)

Moreover, on each of these three occasions, Hitchcock connected the wireless devices and allowed the system to remotely monitor and record events inside plaintiffs' office only after their shifts ended, and after they normally left Hillsides' property. He never activated the system during regular business hours when plaintiffs were scheduled to work. The evidence shows they were not secretly viewed or taped while engaged in personal or clerical activities.

On the latter point, we agree with defendants that their successful effort to avoid capturing plaintiffs on camera is inconsistent with an egregious breach of social norms. For example, in a case closely on point, one court has held that even where an employer placed a camera in an area reserved for the most personal functions at work, such that heightened privacy expectations applied, the lack of any viewing or recording defeated the employee's invasion of privacy claim. (E.g., *Meche v. Wal-Mart, Stores, Inc*. (La.Ct.App. 1997) 692 So.2d 544, 547 [camera concealed in ceiling of restroom to prevent theft].) This circumstance also distinguishes plaintiffs' case from those we have discussed above, in which covert visual monitoring and video recording in an employment setting supported a viable intrusion claim. (E.g., *Doe, supra*, 945 F.2d 1422, 1424, 1427 [models' changing area]; *Trujillo, supra*, 428 F.Supp.2d 1094, 1100, 1119-1122 [police locker room]; *Liberti, supra*, 912 F.Supp. 1494, 1499 [dancers' dressing room].)

2. Defendants' motives, justifications, and related issues. This case does not involve surveillance measures conducted for socially repugnant or unprotected reasons. (See, e.g., *Shulman, supra*, 18 Cal.4th 200, 237 [harassment, blackmail, or prurient curiosity].) Nor, contrary to what plaintiffs imply, does the record reveal the absence of any reasonable justification or beneficial motivation. The undisputed evidence is that defendants installed video surveillance equipment in plaintiffs' office, and activated it three times after they left work, in order to confirm a strong suspicion — triggered by publicized network tracking measures — that an unknown staff person was engaged in unauthorized and inappropriate computer use at night. Given the apparent risks under existing law of doing nothing to avert the problem, and the limited range of available solutions, defendants' conduct was not highly offensive for purposes of establishing a tortious intrusion into private matters. Our reasoning is as follows.

For legitimate business reasons, employers commonly link their network servers to the Internet, and provide employees with computers that have direct access to the network and the Internet. (*Delfino v. Agilent Technologies, Inc*. (2006) 145 Cal.App.4th 790, 805-806 (*Delfino*) [noting trend over previous decade].) As this phenomenon has grown, employers have adopted formal policies regulating the scope of appropriate computer and Internet use. Such policies contemplate reasonable monitoring efforts by employers, and authorize employee discipline for noncompliance. (E.g., *Delfino, supra*, at p. 800, fn. 13 [authorizing discharge for transmitting any threatening, sexually explicit, or harassing item on company computers]; *TBG Ins. Services Corp. v. Superior Court* (2002) 96 Cal.App.4th 443, 446 (*TBG*) [similar policy as to derogatory, defamatory, or obscene material, coupled with notice that company would monitor employee computer use]; *id*. at p. 451 [discussing American Management Association report stating that most large firms regulate and monitor employee

Internet use]; cf. Chin et al., Cal. Practice Guide: Employment Litigation (The Rutter Group 2007) ¶ 5:782.5 et seq. [exploring limits on computer monitoring in workplace].)

Despite efforts to control the problem, the potential for abuse of computer systems and Internet access in the workplace is wide-ranging. (See, e.g., *Intel Corp. v. Hamidi* (2003) 30 Cal.4th 1342, 1347 [holding that employee did not commit tort of trespass to chattels by sending mass emails on employer's electronic system, but otherwise declining to exempt Internet messages from general rules of tort liability]; *TBG*, *supra*, 96 Cal.App.4th 443, 446-447 [employee terminated after repeatedly accessing pornographic Web sites on computer at work].) The consequences to employers may be serious. (E.g., *Delfino*, *supra*, 145 Cal.App.4th 790, 795-796, 800 [third parties sued employer on various counts after receiving vile threats that employee sent over Internet from work computer]; *Monge v. Superior Court* (1986) 176 Cal.App.3d 503, 506-507, 509 [employee stated claims for discrimination, harassment, and punitive damages against employer who failed to investigate her complaints about receiving sexually offensive message from supervisors on her work computer].)

Here, Hitchcock learned that the computer in plaintiffs' office was being used to access the Internet late at night, long after their shifts ended, by someone not authorized to use that equipment or office. Data recorded and stored inside the computer system itself convinced Hitchcock and the computer specialist, Foster, that the unauthorized user was viewing sexually explicit Web sites. Given the hour at which this unauthorized Internet activity occurred, Hitchcock strongly suspected that the responsible party was a program director or other staff person with keys and access to the administration building, which was otherwise locked at that hour.

Such use of Hillsides' computer equipment by an employee violated written workplace policies circulated both before and after the challenged surveillance activities occurred. As those policies warned, and case law confirms, the offending conduct posed a risk that the perpetrator might expose Hillsides to legal liability from various quarters. At the very least, parties on both sides confirmed that accessing pornography on company computers was inconsistent with Hillsides' goal to provide a wholesome environment for the abused children in its care, and to avoid any exposure that might aggravate their vulnerable state.

We also note that Hitchcock's repeated assurances that he installed the surveillance equipment solely to serve the foregoing purposes and not to invade plaintiffs' privacy are corroborated by his actions afterwards. When confronted by plaintiffs about the camera in their office, he explained its presence, and tried to assuage their concerns about being suspected of wrongdoing and secretly videotaped. To this end, he showed them the actual surveillance tape on demand and without delay. Against this backdrop, a reasonable jury could find it difficult to conclude that defendants' conduct was utterly unjustified and highly offensive.

Plaintiffs argue that even assuming defendants acted to prevent a rogue employee from accessing pornography on Hillsides' computers, and to minimize a genuine risk of liability and harm, no claim or defense of justification has been established as a matter of law. Plaintiffs insist triable issues exist as to whether defendants could have employed means less offensive than installing the camera in their office and connecting it to the monitor and recorder nearby. Examples include better enforcement of Hillsides' log-off/password-protection policy, installation of software filtering programs,[10] closer nighttime monitoring of the

---

10 Plaintiffs fault defendants for not using "Net Nanny," a software program that apparently limits access to the Internet. Hitchcock testified that Hillsides

(footnote continued on next page)

camera outside the administration building, increased security patrols at night, and receipt of plaintiffs' informed consent to video surveillance.

Contrary to what plaintiffs imply, it appears defendants are not required to prove that there were no less intrusive means of accomplishing the legitimate objectives we have identified above in order to defeat the instant privacy claim. In the past, we have specifically declined to "impos[e] on a private organization, acting in a situation involving decreased expectations of privacy, the burden of justifying its conduct as the 'least offensive alternative' possible under the circumstances." (*Hill, supra*, 7 Cal.4th 1, 50 [invoking language and history of state constitutional privacy provision and relevant case authority]; accord, *Sheehan, supra*, 45 Cal.4th 992, 1002.)

The argument lacks merit in any event. First, the alternatives that plaintiffs propose would not necessarily have achieved at least one of defendants' aims — determining whether a program director was accessing pornographic Web sites in plaintiffs' office. Rather, it is the same suspect group of program directors on whom plaintiffs would have had defendants more heavily rely to monitor exterior cameras and perform office patrols. Obtaining plaintiffs' consent also might have risked disclosing the surveillance plan to other employees, including the program directors. With respect to stricter regulation of employee computer use (software filters and log-off enforcement), such steps might have stopped the improper use

---

(footnote continued from previous page)

installed "Net Nanny" after the relevant events occurred, and that it was being used in June 2004, when Hitchcock was deposed. However, it is not clear from his testimony, or from plaintiffs' briefs, when such software first became available or how it worked. Hitchcock explained that, before Hillsides installed "Net Nanny," no child could operate a computer without direct adult supervision.

of Lopez's computer. However, they would not have helped defendants identify the employee who performed such activity and who posed a risk of liability and harm in the workplace. (See *Hill, supra*, 7 Cal.4th 1, 50 [rejecting proposed alternatives as "different in kind and character" than challenged acts].)

Second, for reasons suggested above, this is not a case in which "sensitive information [was] gathered and feasible safeguards [were] slipshod or nonexistent." (*Hill, supra*, 7 Cal.4th 1, 38.) Rather, privacy concerns are alleviated because the intrusion was "limited" and no information about plaintiffs was accessed, gathered, or disclosed. (*Ibid*.) As we have seen, defendants did not suspect plaintiffs of using their computers improperly, and sought to ensure that they were not present when any monitoring or recording in their office occurred. The video equipment was rarely activated and then only at night, when plaintiffs were gone. There was no covert surveillance of them behind closed doors.

CONCLUSION

We appreciate plaintiffs' dismay over the discovery of video equipment — small, blinking, and hot to the touch — that their employer had hidden among their personal effects in an office that was reasonably secluded from public access and view. Nothing we say here is meant to encourage such surveillance measures, particularly in the absence of adequate notice to persons within camera range that their actions may be viewed and taped.

Nevertheless, considering all the relevant circumstances, plaintiffs have not established, and cannot reasonably expect to establish, that the particular conduct of defendants that is challenged in this case was highly offensive and constituted an egregious violation of prevailing social norms. We reach this conclusion from the standpoint of a reasonable person based on defendants' vigorous efforts to avoid intruding on plaintiffs' visual privacy altogether. Activation of the surveillance system was narrowly tailored in place, time, and scope, and was prompted by legitimate business concerns. Plaintiffs were not at risk of being monitored or recorded during regular work hours and were never actually caught on camera or videotape.

We therefore reverse the judgment of the Court of Appeal insofar as it reversed and vacated the trial court's order granting defendants' motion for summary judgment on all counts alleged in the complaint.

BAXTER, J.

WE CONCUR:

GEORGE, C. J.
KENNARD, J.
WERDEGAR, J.
CHIN, J.
MORENO, J.
CORRIGAN, J.

See next page for addresses and telephone numbers for counsel who argued in Supreme Court.

Name of Opinion Hernandez v. Hillsides, Inc.

Unpublished Opinion
Original Appeal
Original Proceeding
Review Granted XXX 142 Cal.App.4th 1377
Rehearing Granted

Opinion No. S147552
Date Filed: August 3, 2009

Court: Superior
County: Los Angeles
Judge: C. Edward Simpson

Attorneys for Appellant:

Eisenberg & Associates, Arnold Kessler and Mark S. Eisenberg for Plaintiffs and Appellants.

Attorneys for Respondent:

Seyfarth Shaw, Laura Wilson Shelby, Holger G. Besch, Candice Zee and Amy C. Chang for Defendants and Respondents.

Paul, Hastings, Janofsky & Walker, Paul W. Cane, Jr., and Teresa J. Hutson for Employers Group and California Employment Law Council as Amici Curiae on behalf of Defendants and Respondents.

Counsel who argued in Supreme Court (not intended for publication with opinion):

Mark S. Eisenberg
Eisenberg & Associates
12121 Wilshire Boulevard, Suite 600
Los Angeles, CA 90025
(310) 444-1100

Holger G. Besch
Seyfarth Shaw
2029 Century Park East, 33d Floor
Los Angeles, CA 90067-3063
(310) 277-7200

Paul W. Cane, Jr.
Paul, Hastings, Janofsky & Walker
55 Second Street, Twenty-Fourth Floor
San Francisco, CA 94105
(415) 856-7000