

the outward appearance of any person, irrespective of sex, with regard to bodily condition or characteristics, manner or style of dress, and manner or style of personal grooming, including, but not limited to, hair style and beards. It shall not relate, however, to the requirement of * * * prescribed standards * * * when uniformly applied to a class of employees for a reasonable business purpose.
* * *

D.C.Code § 2-1402.02(22). Has the employer violated the statute? See *Atlantic Richfield Co. v. District of Columbia Comm'n on Human Rights*, 515 A.2d 1095 (D.C.1986) (held: yes). Is a statutory approach to personal appearance discrimination practical? What problems do you envision? In *Kennedy v. District of Columbia*, 654 A.2d 847 (D.C.1994), the court held that the fire department violated the Human Rights Act by discharging a firefighter with a beard and handlebar mustache. The fire department failed to prove its purported safety reason for the regulation.

B. PRIVACY

Hernandez v. Hillsides, Inc.

211 P.3d 1063 (Cal. 2009).

■ BAXTER, CIRCUIT JUDGE:

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.

* * *

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.

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 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.

* * *

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.

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.

* * *

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. These limitations on the right to privacy are not insignificant. Nonetheless, the cause of action recognizes a measure of personal control over the individual's autonomy, dignity, and serenity. The gravamen is the mental anguish sustained when both conditions of liability exist.

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. In either instance, the expectation of privacy must be "objectively reasonable." 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.

The second common law element essentially involves a “policy” determination as to whether the alleged intrusion is “highly offensive” under the particular circumstances. Relevant factors include the degree and setting of the intrusion, and the intruder’s motives and objectives. 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.”

* * *

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. 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*, 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.

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.

The present scenario falls between these extremes.

Plaintiffs plausibly claim that Hillside 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.

Regarding another relevant factor in *Sanders*, 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.”

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.” Such monitoring and recording denies the actor a key feature of privacy—the right to control the dissemination of his image and actions. 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.’”

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. Of course, the intruder also cannot “secretly videotape, film, photograph, or record” anyone in that private place where various conditions exist.

* * *

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 requisite intrusion in the first place.

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 Hillside).

* * *

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.

Plaintiffs must show more than an intrusion upon reasonable privacy expectations. Actionable invasions of privacy also must be "highly offensive" to a reasonable person and "sufficiently serious" and unwarranted as to constitute an "egregious breach of the social norms." Defendants claim that, in finding a triable issue in this regard, the Court of Appeal focused too narrowly on the mere 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.

* * *

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.

NOTES AND QUESTIONS

1. What facts are most helpful to the defendant's case? No doubt, the employees were hurt, insulted, angry, and embarrassed, but the court is clear that for either common law or state constitutional invasion of privacy based on intrusion, there must be substantial evidence of objective, unreasonable conduct on the part of the defendant.
2. Surveillance of workers on the job is increasing in an effort to improve efficiency and reduce theft. Does the use of TV cameras, microphones, metal detectors, mirrors, one-way mirrors, or other devices invade any legitimate interests of employees? Does the reasonableness of such measures depend on the employer's justifications, the consent of the workers, or some other factors? See [Thomas v. General Elec. Co.](#), 207 F.Supp. 792 (W.D.Ky.1962) (holding that employer's photographing employee to increase efficiency of his operations and promote safety of employees did not violate employee's right to privacy); [Sacramento County Deputy Sheriffs' Ass'n v. Sacramento County](#), 59 Cal.Rptr.2d 834 (Ct.App.1996) (placement of video camera in county jail's release office did not violate deputy sheriff's Fourth Amendment rights). See also [Cowles v. Alaska](#), 23 P.3d 1168 (Alaska 2001), cert. denied, 534 U.S. 1131 (2002) (placing video camera without sound in ceiling above a desk visible to the public to determine reason for cash shortages did not violate Alaska Constitution).

City of Ontario v. Quon

560 U.S. 746 (2010).

■ JUSTICE KENNEDY delivered the opinion of the Court.

This case involves the assertion by a government employer of the right, in circumstances to be described, to read text messages sent and received on a pager the employer owned and issued to an employee. The employee contends that the privacy of the messages is protected by the ban on “unreasonable searches and seizures” found in the Fourth Amendment to the United States Constitution, made applicable to the States by the Due Process Clause of the Fourteenth Amendment. Though the case touches issues of far reaching significance, the Court concludes it can be resolved by settled principles determining when a search is reasonable.

The City of Ontario (City) is a political subdivision of the State of California. The case arose out of incidents in 2001 and 2002 when respondent Jeff Quon was employed by the Ontario Police Department (OPD). He was a police sergeant and member of OPD's Special Weapons and Tactics (SWAT) Team.

* * *

In October 2001, the City acquired 20 alphanumeric pagers capable of sending and receiving text messages. Arch Wireless Operating Company provided wireless service for the pagers. Under the City's service contract with Arch Wireless, each pager was allotted a limited number of characters sent or received each month. Usage in excess of that amount would result in an additional fee. The City issued pagers to Quon and other SWAT Team members in order to help the SWAT Team mobilize and respond to emergency situations.

Before acquiring the pagers, the City announced a "Computer Usage, Internet and E-Mail Policy" (Computer Policy) that applied to all employees. Among other provisions, it specified that the City "reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." In March 2000, Quon signed a statement acknowledging that he had read and understood the Computer Policy.

The Computer Policy did not apply, on its face, to text messaging. Text messages share similarities with e-mails, but the two differ in an important way. In this case, for instance, an e-mail sent on a City computer was transmitted through the City's own data servers, but a text message sent on one of the City's pagers was transmitted using wireless radio frequencies from an individual pager to a receiving station owned by Arch Wireless. It was routed through Arch Wireless' computer network, where it remained until the recipient's pager or cellular telephone was ready to receive the message, at which point Arch Wireless transmitted the message from the transmitting station nearest to the recipient. After delivery, Arch Wireless retained a copy on its computer servers. The message did not pass through computers owned by the City.

Although the Computer Policy did not cover text messages by its explicit terms, the City made clear to employees, including Quon, that the City would treat text messages the same way as it treated e-mails. At an April 18, 2002, staff meeting at which Quon was present, Lieutenant Steven Duke, the OPD officer responsible for the City's contract with Arch Wireless, told officers that messages sent on the pagers "are considered e-mail messages. This means that [text] messages would fall under the City's policy as public information and [would be] eligible for auditing." Duke's comments were put in writing in a memorandum sent on April 29, 2002, by Chief Scharf to Quon and other City personnel.

Within the first or second billing cycle after the pagers were distributed, Quon exceeded his monthly text message character allotment. Duke told Quon about the overage, and reminded him that messages sent on the pagers were "considered e-mail and could be audited." Duke said, however, that "it was not his intent to audit [an] employee's text messages to see if the overage [was] due to work related transmissions." Duke suggested that Quon could reimburse the City for the overage fee rather than have Duke audit the messages. Quon wrote a check to the City for the overage. Duke offered the same arrangement to other employees who incurred overage fees.

Over the next few months, Quon exceeded his character limit three or four times. Each time he reimbursed the City. Quon and another officer again incurred overage fees for their pager usage in August 2002. At a meeting in October, Duke told Scharf that he had become "tired of being a bill collector." Scharf decided to determine whether the existing character limit was too low—that is, whether officers such as Quon were having to pay fees for sending work-related messages—or if the overages were for personal messages. Scharf told Duke to request transcripts of text messages sent in August and September by Quon and the other employee who had exceeded the character allowance.

At Duke's request, an administrative assistant employed by OPD contacted Arch Wireless. After verifying that the City was the subscriber on the accounts, Arch Wireless provided the desired transcripts. Duke reviewed the transcripts and discovered that many of the messages sent and received on Quon's pager were not work related, and some were sexually explicit. Duke reported his findings to Scharf, who, along with Quon's immediate supervisor, reviewed the transcripts himself. After his review, Scharf referred the matter to OPD's internal affairs division for an investigation into whether Quon was violating OPD rules by pursuing personal matters while on duty.

The officer in charge of the internal affairs review was Sergeant Patrick McMahon. Before conducting a review, McMahon used Quon's work schedule to redact the transcripts in order to eliminate any messages Quon sent while off duty. He then reviewed the content of the messages Quon sent during work hours. McMahon's report noted that Quon sent or received 456 messages during work hours in the month of August 2002, of which no more than 57 were work related; he sent as many as 80 messages during a single day at work; and on an average workday, Quon sent or received 28 messages, of which only 3 were related to police business. The report concluded that Quon had violated OPD rules. Quon was allegedly disciplined.

Raising claims under Rev. Stat. § 1979, 42 U.S.C. § 1983; 18 U.S.C. § 2701 et seq., popularly known as the Stored Communications Act (SCA); and California law, Quon filed suit against petitioners in the United States District Court for the Central District of California. * * * Among the allegations in the complaint was that petitioners violated respondents' Fourth Amendment rights and the SCA by obtaining and reviewing the transcript of Jeff Quon's pager messages and that Arch Wireless had violated the SCA by turning over the transcript to the City.

* * *

The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated. . . ." It is well settled that the Fourth Amendment's protection extends beyond the sphere of criminal investigations. [Camara v. Municipal Court of City and County of San Francisco](#), 387 U.S. 523, 530 (1967). "The Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government," without regard to whether the government actor is investigating crime or performing another function. [Skinner v. Railway Labor Executives' Assn.](#), 489 U.S. 602, 613–614 (1989). The Fourth Amendment applies as well when the Government acts in its capacity as an employer. [Treasury Employees v. Von Raab](#), 489 U.S. 656, 665 (1989).

The Court discussed this principle in [O'Connor \[v. Ortega\]](#), 480 U.S. 709 (1987). There a physician employed by a state hospital alleged that hospital officials investigating workplace misconduct had violated his Fourth Amendment rights by searching his office and seizing personal items from his desk and filing cabinet. All Members of the Court agreed with the general principle that "[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer." A majority of the Court further agreed that

“‘special needs, beyond the normal need for law enforcement,’” make the warrant and probable-cause requirement impracticable for government employers.

* * *

Later, in the *Von Raab* decision, the Court explained that “operational realities” could diminish an employee’s privacy expectations, and that this diminution could be taken into consideration when assessing the reasonableness of a workplace search. In the two decades since *O’Connor*, however, the threshold test for determining the scope of an employee’s Fourth Amendment rights has not been clarified further. Here, though they disagree on whether Quon had a reasonable expectation of privacy, both petitioners and respondents start from the premise that the *O’Connor* plurality controls. It is not necessary to resolve whether that premise is correct. The case can be decided by determining that the search was reasonable even assuming Quon had a reasonable expectation of privacy.

* * *

The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. * * * It is not so clear that courts at present are on so sure a ground. Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.

Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. As one *amici* brief notes, many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency. Another *amicus* points out that the law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications. At present, it is uncertain how workplace norms, and the law’s treatment of them, will evolve.

Even if the Court were certain that the *O’Connor* plurality’s approach were the right one, the Court would have difficulty predicting how employees’ privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable. Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of