EMPLOYEE CIVIL RIGHTS ISSUES IN TOUGH ECONOMIC TIMES

Presentation by Patricia T. Castle & Carol Grogan
August 7, 2009

I. INTRODUCTION

The increasing numbers of nonreelections, layoffs, reductions in force, and other methods being used by public agencies to deal with the current economy can lead to an increase in complaints by employees alleging that their civil rights have been violated by their employer.

Some of the complaints may have merit; some will not. Regardless of the merit of the complaint, responding to complaints filed with regulatory agencies such as the Department of Fair Employment and Housing (DFEH) and the Equal Employment Opportunity Commission (EEOC) can be expensive, time-consuming, and divisive in the work place.

These materials discuss proactive steps a District can take to help reduce the potential for such claims. A primary key is to foster recognition of the issues by the administrators who make employment decisions.

HYPOTHETICAL NO. 1

ADVERSE EMPLOYMENT ACTION BASED ON PROTECTED CLASS OR PROTECTED ACTIVITY

Jane Doe is hired as a first year, probationary teacher, in August. She learns in early December that she is pregnant, with serious complications. She takes a pregnancy disability leave of absence from early December until February 15, and those are her only absences from work.

A few days after she returns to work on February 16, Jane is notified that she is being nonreelected.

Jane files a discrimination complaint with the California DFEH alleging that she was discriminated and retaliated against for taking a protected disability leave of absence.

Evidence Helpful to District:

Documents indicating the employment action was not based on Jane's pregnancy, such as Board resolutions showing others were nonreelected, laid off, programs eliminated.

I. Outline of Presentation

Employee discrimination complaints may increase in poor economic times because the law protects complainants against adverse employment action based on the employee's protected activity, or the employee's membership in a protected class.

A. Examples of Protected Class:

Disability
Pregnancy
Sexual harassment
Age
Race, ethnicity, or national origin
Registered Domestic Partner

B. Examples of Protected Activity:

Exercise of protected leave rights, like:

Pregnancy Disability Leave,
FMLA/CFRA,
Kin Care Leave,
Military Leave;
Engaging in activity protected by the First Amendment, (religion, speech, press, assembly, petition);
Engaging in protected union activity;

Whistle-blowing, like

Filing a discrimination complaint (Labor Code section 98.6);
Disclosing information to a government agency or a law enforcement agency with reasonable cause to believe the information discloses a violation of statute or noncompliance with a regulation (Labor Code section 1102.5);
Filing any complaint or testifying in any matter related to occupational safety (Labor Code section 6399.7).

HYPOTHETICAL No. 2

VIDEO SURVEILLANCE

Your computer technician tells you that he believes someone is accessing pornographic web sites at night from a computer in an office shared by two employees. You place a motion-activated video surveillance system in the employees' office without informing them. One day, one of the employees notices a little light blinking whenever she moves, and calls you. You explain what you were doing, and that you only taped activities in the office at night. You tell her that all the tapes showed was the empty office at night. In fact, you tell her, you were going to remove the camera that very weekend.

Have your actions exposed the district to an invasion of privacy claim?

I. Outline of Presentation.

School districts must carefully avoid any activity that unlawfully intrudes on employees' rights, including their privacy interests.

A. Audio and video recording.

California's Invasion of Privacy Act (Penal Code section 632) requires the consent of all parties before private conversations, including phone conversations, can be recorded. A district should obtain the consent of employees before making any audio recording, including any video recording that includes audio recording. The district should inform employees of any video or audio recording devices in work areas where the employees may have a reasonable expectation of privacy.

B. Video surveillance as an invasion of privacy.

Although Penal Code section 632 requires consent for any audio recording or eavesdropping, it does not require consent for video recordings which do not have an audio component. However, video recordings without an audio component may give rise to legal actions based upon theories such as invasion of privacy.

In *Trujillo v. City of Ontario* (C.D. Cal. 2006) 428 F. Supp. 2d 1094, 1103-1107, *aff'd, Bernhard v. City of Ont.,* 270 Fed. Appx. 518 (unpublished), in response to complaints of theft, the city police department installed a video surveillance camera in the men's locker room. The employees were not told of the camera. The court noted that video surveillance constitutes a particularly intrusive search and held the plaintiff officers had a reasonable expectation of privacy to be free from covert video surveillance.

Also, California Labor Code section 435 provides in part:

No employer may cause an audio or video recording to be made of an employee in a restroom, locker room, or room designated by an employer for changing clothes, unless authorized by court order.

C. California Supreme Court to review *Hernandez v. Hillsides, Inc.* (2006) 142 Cal. App. 4th 1377.

The California Supreme Court has granted review of *Hernandez v. Hillsides, Inc*. to address the question of whether two employees can state a cause of action for invasion of privacy when a hidden camera was placed in their private office, even when the evidence showed that no one ever watched the feed broadcast by the camera. *Hernandez v. Hillsides, Inc*. 48 Cal. Rptr. 3d 780, *review granted*, (2007) 53 Cal. Rptr. 3d 801, 150 P.3d 692 .

The trial court found that the plaintiff employees had no cause of action because there was no evidence they were ever viewed or recorded. The Court of Appeal reversed, finding that the plaintiff employees could state an invasion of privacy claim even if they had not actually been viewed or recorded. The Court of Appeal reasoned that the intrusion occurred when privacy was invaded in an offensive manner without consent, not when information gained from the intrusion was disclosed. The California Supreme Court accepted the case for review and heard oral argument in June 2009. The Court is expected to issue a decision this year.

II. MATERIALS IN WORKBOOK.

A. Penal Code section 632

B. Labor Code section 435

C. *Hernandez v. Hillsides, Inc*. 48 Cal. Rptr. 3d 780, *review granted*, (2007) 53 Cal. Rptr. 3d 801, 150 P.3d 692.

Penal Code § 632. Eavesdropping on confidential communication; Punishment

(a) Every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500), or imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment. If the person has previously been convicted of a violation of this section or Section 631, 632.5, 632.6, 632.7, or 636, the person shall be punished by a fine not exceeding ten thousand dollars ($10,000), by imprisonment in the county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.

(b) The term "person" includes an individual, business association, partnership, corporation, limited liability company, or other legal entity, and an individual acting or purporting to act for or on behalf of any government or subdivision thereof, whether federal, state, or local, but excludes an individual known by all parties to a confidential communication to be overhearing or recording the communication.

(c) The term "confidential communication" includes any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.

(d) Except as proof in an action or prosecution for violation of this section, no evidence obtained as a result of eavesdropping upon or recording a confidential communication in violation of this section shall be admissible in any judicial, administrative, legislative, or other proceeding.

(e) This section does not apply (1) to any public utility engaged in the business of providing communications services and facilities, or to the officers, employees or agents thereof, where the acts otherwise prohibited by this section are for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility, or (2) to the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility, or (3) to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

(f) This section does not apply to the use of hearing aids and similar devices, by persons afflicted with impaired hearing, for the purpose of overcoming the impairment to permit the hearing of sounds ordinarily audible to the human ear.

Labor Code § 435. Recording employees

(a) No employer may cause an audio or video recording to be made of an employee in a restroom, locker room, or room designated by an employer for changing clothes, unless authorized by court order.

(b) No recording made in violation of this section may be used by an employer for any purpose. This section applies to a private or public employer, except the federal government.

(c) A violation of this section constitutes an infraction.

DEPUBLISHED
AWAITING REVIEW

ABIGAIL HERNANDEZ et al., Plaintiffs and Appellants, v. HILLSIDES, INC., et al., Defendants and Respondents.

142 Cal. App. 4th 1377; 48 Cal. Rptr. 3d 780
September 14, 2006, Filed

NOTICE:

NOT CITABLE--SUPERSEDED BY GRANT OF REVIEW

DISPOSITION: Judgment is reversed and remanded with directions.

SUMMARY:

CALIFORNIA OFFICIAL REPORTS SUMMARY

The trial court granted summary judgment to employers on causes of action brought by employees for invasion of privacy, intentional infliction of emotional distress, and negligent infliction of emotional distress. The employers, suspecting that someone had been accessing pornographic Web sites at night from some of the office computers, placed a motion-activated video surveillance system in the employees' office without informing the employees. (Superior Court of Los Angeles County, No. GC032633, C. Edward Simpson, Judge.)

The Court of Appeal reversed and remanded with directions to vacate the order granting the motion for summary judgment, to enter a new and different order denying the motion for summary judgment and granting summary adjudication of the causes of action for intentional infliction of emotional distress and negligent infliction of emotional distress, and to conduct further proceedings. The court held that the tort of invasion of privacy based on an intrusion did not require proof that private information had been disclosed to a third party. Intrusion occurred when privacy was invaded in an offensive manner without consent, not when information gained from the intrusion was disclosed. Thus, the mere placement of the surveillance equipment in the office was sufficient to invade the employees' privacy. Moreover, the employers did not establish that the employees did not have a reasonable expectation of privacy in their office. Factual issues remained as to the offensiveness of the employers' conduct and the reasonableness of their claim that the surveillance was justified. The employers were entitled to judgment on the claim for intentional infliction of emotional distress because their conduct was not extreme and outrageous, as well as on the claim for negligent infliction of emotional distress because no breach of duty was alleged. (Opinion by Croskey, Acting P. J., with Kitching and Aldrich, JJ., concurring.) [*1378]

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

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

JUDGES: Croskey, Acting P. J., with Kitching and Aldrich, JJ., concurring.

OPINION BY: CROSKEY

OPINION

[**782] **CROSKEY, Acting P. J.**--Abigail Hernandez and Maria Jose-Lopez (plaintiffs) appeal from the trial court's grant of summary judgment in favor of Hillsides, Inc., Hillsides Children's Center, Inc., and John M. Hitchcock (defendants). Plaintiffs had sued for damages after they had discovered that their employer, a residential facility for abused children, had placed a video camera in the office which they shared. The trial court held that plaintiffs could not prevail on their causes of action for invasion of privacy, intentional infliction of emotional distress, and negligent infliction of emotional distress because plaintiffs: (1) were not recorded or viewed by the surveillance equipment defendants placed in their office; and (2) had a diminished expectation of privacy [***2] that was overcome by defendants' need to protect the children residing at their facility.

We hold that a plaintiff need not establish that he or she was actually viewed or recorded in order to succeed on a cause of action for invasion of privacy. Additionally, defendants failed to conclusively establish that plaintiffs had a diminished expectation of privacy, or that their actions were sufficiently justified by the need to protect the children residing at their [*1381] facility. We therefore reverse. Plaintiffs, however, cannot state a cause of action for intentional infliction of emotional distress, and their cause of action for negligent infliction

of emotional distress is legally insufficient and factually superfluous, so summary adjudication should be granted in favor of defendants on those two causes of action.

FACTS AND PROCEDURAL BACKGROUND[1]

1 The facts we recite are set forth in the papers filed by the parties in support of and in opposition to defendants' motion for summary judgment.

Defendants [***3] run a residential facility for approximately 66 abused and neglected children between the ages of six and 18. Defendant John Hitchcock (Hitchcock) is the director of the facility. Plaintiffs were employed in clerical positions in the office building on defendants' campus. [**783] They shared an office with a locking door and a window with shades that could be drawn for privacy. [2] The door to plaintiffs' office contained a "doggie door" which was missing the swinging flap. On several occasions plaintiff Hernandez used her office to change clothes before leaving for the gym. Plaintiff Jose-Lopez occasionally used the office to show Hernandez how her figure was recovering after recently giving birth by raising her shirt to expose her breasts and stomach. Defendants had no knowledge that plaintiffs were using the office for such purposes, but such facts would support a conclusion that plaintiffs had an expectation of privacy while in their office.

2 Plaintiffs assert the shades are always drawn, but what is important for the purposes of this opinion is that plaintiffs' office can be sufficiently concealed from view.

[***4] 1. *Defendants Install Motion-activated Camera in Plaintiffs' Office*

Around July 2002, defendants' computer technician, Tom Foster, informed defendants that he believed someone was accessing pornographic Web sites at night from some of defendants' computers, including the one in plaintiffs' office. Defendants and various department heads and administrative staff members decided to conduct surveillance in areas where the illicit computer access had taken place. [3] Plaintiffs were not advised of this decision because they were considered to be part of a group of employees that "gossiped" and might inadvertently tip off the unknown person(s) defendants were trying to catch.

3 Defendants had purchased the surveillance equipment in February 2002 for the purpose of preventing thefts in the administration building.

Hitchcock installed a motion-activated video surveillance system in the computer lab where some of the illicit Web access had occurred. The surveillance system was moved to plaintiffs' shared office [***5] in October 2002. The camera and motion detector were placed on a shelf in plaintiffs' office [*1382] and set up to broadcast images to a TV monitor and video recorder located in a storage room across the hall. Only four people were aware that the surveillance equipment had been placed in plaintiffs' office. Plaintiffs were not among those who had such knowledge.

In his deposition, Hitchcock stated that the surveillance camera and motion detector operated "all the time," but that the system had only been "active" three times. The first time, Hitchcock had placed the camera and motion detector in plaintiffs' office after they had left for the day and removed it before they arrived the next morning. Thereafter, Hitchcock had left the camera and motion detector functioning in plaintiffs' office but only twice had "connected" the wireless receptor to the TV monitor and recorder in the storage room. His practice was to connect the receptor before leaving at night and, in order to prevent the camera from transmitting to the TV monitor during the day, disconnect it before plaintiffs arrived for work the following morning. Defendants did not provide any evidence, however, regarding which three dates [***6] the surveillance system had been activated.

At approximately 4:30 in the afternoon on Friday, October 25, 2002, plaintiffs noticed a red light on a shelf in their office blinking when there was movement in front of it. They looked more closely and discovered a camera. They followed the cord attached to the camera and discovered that it was plugged in and that the plug was hot to the touch. Plaintiffs notified their supervisor, who called Hitchcock at his home to report the discovery. Hitchcock, who had not been to the facility that [**784] day, called Hernandez in her office to explain the surveillance and assure her that the camera had not been installed to observe plaintiffs.

Plaintiffs were extremely upset by their discovery and did not return to work until Wednesday, October 30, 2005. When they returned, plaintiffs asked to view the surveillance tape. Plaintiffs were shown a tape containing scenes of their empty office, Hitchcock adjusting the camera, and about five minutes of static. In his deposition, Hitchcock stated that he had been planning to remove the camera the very weekend plaintiffs found it, because there had been no pornographic Web sites accessed from the computer in plaintiffs' [***7] office in the three-week period during which he had been periodically "recording" their office.

2. *Subsequent Lawsuit and Motion for Summary Judgment*

On September 12, 2003, plaintiffs filed suit against defendants for invasion of privacy, intentional infliction of emotional distress, and negligent infliction of emotional distress arising from their discovery of the surveillance equipment in their office. Defendants filed a motion for summary judgment on December 15, 2004, and raised three principal contentions.

[*1383] a. *Publication*

Defendants first argued that plaintiffs' cause of action for invasion of privacy must fail because plaintiffs had not been recorded or viewed by the camera installed in their office, and thus, as a matter of law, plaintiffs' privacy could not have been invaded. [4] Defendants asserted that the camera was only "active" three times, and only in the evening hours. Defendants relied on the videotape shown to plaintiffs and Hitchcock's deposition as proof plaintiffs were never viewed or recorded by the surveillance system. Defendants, however, did not provide declarations or depositions from any of the department heads involved in the decision to [***8] conduct video surveillance of plaintiffs' office or from any of the persons who had access to the storage room and who could have activated the surveillance system while plaintiffs were in their office.

> 4 Similarly, defendants argued that because plaintiffs were never viewed or recorded by the surveillance equipment placed in their office, defendants' conduct was not sufficiently outrageous to support a cause of action for intentional infliction of emotional distress.

In response, plaintiffs argued that Hitchcock's deposition stated that the camera was always on and the videotape showed an empty room, indicating that there did not need to be motion to activate the video recorder. Plaintiffs argued Hitchcock's statements that the camera was always on, but that they had never been recorded or viewed, were contradictory. [5] Additionally, plaintiffs noted that Hitchcock was not at Hillsides on the day plaintiffs found the camera, so he could not [**785] have "deactivated" it that morning, and that defendants did not provide [***9] the specific dates on which the surveillance system was "active."

> 5 Plaintiffs misunderstand Hitchcock's deposition testimony, which is not inconsistent with regard to the operation of the camera and the recording equipment. Hitchcock has consistently testified that the camera is "on" when it is plugged in, but would only transmit images for recording and/or viewing on the TV monitor if the "receptors" in the storage room were connected to the TV monitor and recorder. Hitchcock's testimony was that, in order to prevent the camera from transmitting or recording during the day, he would "disconnect" the camera receptors from the TV monitor and recorder in the storage room. Thus, the camera was technically "on" because it was plugged in to the wall in plaintiffs' office, but if the receptors were disconnected, as Hitchcock testified, there would be no way for any image of plaintiffs' office to appear on the TV monitor.

b. *Expectation of Privacy*

Defendants next argued that even if plaintiffs had been viewed [***10] or recorded, they had a diminished expectation of privacy in their jointly occupied office. Defendants argued plaintiffs could not have reasonably expected privacy in their office because: (1) a person could climb over a railing outside plaintiffs' window and peek in; (2) the "doggie door" allowed anyone to bend down and [*1384] see in the office; and (3) at least 11 people had keys to their office. Defendants also argued that four surveillance cameras throughout the campus and plaintiffs' signatures on computer monitoring policies indicated that they knew they could be "monitored" at any time while on the campus.

Plaintiffs countered that the windows in their office were always closed, and anyone with a need to come into the office while it was occupied would knock on the door for admittance, not lean down and peek in. Regardless of windows and doggie doors, plaintiffs argued, employees may have a reasonably objective expectation of privacy even when their workspace is an open cubicle in a room with dozens of other employees, making it all the more reasonable that an employee in an office with a lockable door would expect to enjoy privacy when the door was closed. Finally, plaintiffs [***11] noted that any policy regarding computer monitoring involved monitoring the computer system itself, not the office in which the computer was being used.

c. *Justification of Surveillance*

Lastly, defendants argued that even if plaintiffs possessed a minimal expectation of privacy, it was overcome by defendants' need to catch the person believed to be accessing pornographic Web sites at night, in order to protect the children on the campus from potential abuse or exposure to that activity.

Plaintiffs responded that while defendants asserted

the surveillance was in response to "pornographic" Web sites that had been accessed from facility computers, they failed to provide the titles of the Web sites, did not describe what sort of Web sites were "pornographic," and had not provided the Web logs that justified their decision to conduct a surveillance of plaintiffs' office. Plaintiffs further pointed out that defendants were aware of the "illicit" Web access for three months before taking any action to conduct surveillance in plaintiffs' office. Finally, plaintiffs argued that there were less intrusive means for determining the culprit than placing a secret surveillance camera in their [***12] office.

3. *Resolution of Motion and Appeal*

On March 1, 2006, the trial court granted the motion for summary judgment. Judgment was entered in favor of defendants. Plaintiffs filed a timely notice of appeal.

ISSUES ON APPEAL

The arguments made by the parties present four issues: (1) is publication a necessary element of plaintiffs' cause of action for invasion of privacy and, if [*1385] so, did defendants defeat it? (2) were plaintiffs' expectations of privacy reasonable? (3) did defendants conclusively establish that the surveillance was, under the circumstances, justified? and (4) did defendants defeat plaintiffs' causes of action for the infliction of emotional distress?

DISCUSSION

1. *Standard of Review*

" 'A defendant is entitled to summary judgment if the record establishes as a [**786] matter of law that none of the plaintiff's asserted causes of action can prevail.' (*Molko v. Holy Spirit Assn.* (1988) 46 Cal.3d 1092, 1107 [252 Cal. Rptr. 122].) The pleadings define the issues to be considered on a motion for summary judgment. (*Sadlier v. Superior Court* (1986) 184 Cal. App. 3d 1050, 1055 [29 Cal. Rptr. 374].) As [***13] to each claim as framed by the complaint, the defendant must present facts to negate an essential element or to establish a defense. Only then will the burden shift to the plaintiff to demonstrate the existence of a triable, material issue of fact. (*AARTS Productions, Inc. v. Crocker National Bank* (1986) 179 Cal. App. 3d 1061, 1064-1065 [225 Cal. Rptr. 203].)" (*Ferrari v. Grand Canyon Dories* (1995) 32 Cal.App.4th 248, 252 [38 Cal. Rptr. 2d 65].) "There is a triable issue of material fact if, and only if, the evidence would allow a reasonable trier of fact to find the underlying fact in favor of the party opposing the motion in accordance with the applicable standard of proof." (*Aguilar v. Atlantic Richfield Co.* (2001) 25 Cal.4th 826, 850 [107 Cal. Rptr. 2d 841, 24 P.3d 493].) We review orders granting or denying a summary judgment motion de novo. (*FSR Brokerage, Inc. v. Superior Court* (1995) 35 Cal.App.4th 69, 72 [41 Cal. Rptr. 2d 404].) We exercise "an independent assessment of the correctness of the trial court's ruling, applying the same legal standard as the trial court in determining whether there are any genuine issues of material fact or whether the moving party is entitled to judgment as [***14] a matter of law." (*Iverson v. Muroc Unified School Dist.* (1995) 32 Cal.App.4th 218, 222 [38 Cal. Rptr. 2d 35].)

2. *Invasion of Privacy Principles*

(1) In 1960, Prosser identified four basic privacy interests: (1) intrusion upon seclusion or solitude, or private affairs; (2) public disclosure of embarrassing private facts; (3) publicity which places the plaintiff in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness. (*Miller v. National Broadcasting Co., Inc.* (1986) 187 Cal. App. 3d 1463, 1482 [232 Cal. Rptr. 668].) The case before us involves the right to be secure from intrusion.

[*1386] **(2)** California courts have adopted Prosser's analysis and the Restatement formulation of intrusion: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." (Rest.2d Torts, § 652B; see also *Miller v. National Broadcasting Co., Inc., supra,* 187 Cal. App. 3d at p. 1482.) Intrusion into private places, [***15] conversations, and matters is the privacy tort that best captures the common understanding of an "invasion of privacy" and "is most clearly seen as an affront to individual dignity." (*Shulman v. Group W Productions, Inc.* (1998) 18 Cal.4th 200, 231 [74 Cal. Rptr. 2d 843, 955 P.2d 469] (*Shulman*).) The *Shulman* court noted that intrusion cases are inherently fact specific and, as a result, there are no bright line rules identifying the outer boundaries of intrusion. (*Id.* at p. 237.)

Thus, as applicable to the case before us, the tort of invasion of privacy, or intrusion, has two main elements: (1) intrusion into a private place, conversation, or matter; and (2) in a manner highly offensive to a reasonable person. (*Shulman, supra,* 18 Cal.4th at p. 231.) Tortious intrusion includes unconsented-to physical intrusion into private places, as well as "unwarranted sensory intrusions such as eavesdropping, wiretapping, and visual or photographic spying." (*Shulman, supra,* [**787] 18 Cal.4th at pp. 230-231, citing Rest.2d Torts, § 652B,

com. b & illus., pp. 378-379; see also *Wilkins v. National Broadcasting Co.* (1999) 71 Cal.App.4th 1066, 1075 [84 Cal. Rptr. 2d 329].) [***16]

3. *Publication Is Not an Element of Invasion of Privacy*

Defendants argue that plaintiffs could not raise a triable issue of fact as to whether they were recorded or viewed by the equipment defendants placed in their office because the videotape plaintiffs were shown included only footage of their empty office and Hitchcock. Whether plaintiffs were viewed or recorded, however, Hitchcock admittedly had entered plaintiffs' office and secretly placed a functioning camera which was capable of transmitting images from plaintiffs' office to a remote location where such images could be viewed or recorded at will by the activation of a remote receiver.

(3) The tort of invasion of privacy based on an intrusion does not require plaintiffs to prove that private information about them has been disclosed to a third party. (*Miller v. National Broadcasting Co., Inc., supra,* 187 Cal.App.3d at p. 1484.) A plaintiff is harmed when his or her privacy is invaded in an offensive manner without consent, not when information gained from the intrusion is disclosed or published. The Restatement Second of Torts explains: "[I]nvasion of privacy covered by this Section [intrusion] ... consists [*1387] solely of an intentional [***17] interference with [plaintiff's] interest in solitude or seclusion, either as to his [or her] person or as to his [or her] private affairs or concerns, of a kind that would be highly offensive to a reasonable [person]." (Rest.2d Torts, § 652B, com. a, p. 378.) The Restatement continues: "The invasion ... may be by some other form of investigation or examination into [plaintiff's] private concerns ... . The *intrusion itself* makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined." (*Id.,* com. b, pp. 378-379, italics added.) Thus, if unconsented-to disclosure, publication, or viewing of information about the plaintiff is harmful, then the action taken to obtain that private information must itself also be harmful.

Intrusion involves a plaintiff's peace of mind and right to be left alone. The focus is on whether the defendants penetrated "some zone of physical or sensory privacy surrounding, *or obtained unwanted access* to data about, the plaintiff," not whether the data was ever obtained or disclosed. (*Shulman, supra,* 18 Cal 4th at p. 232 [***18] , italics added; see also *Huntingdon Life Sciences, Inc. v. Stop Huntingdon Animal Cruelty USA, Inc.* (2005) 129 Cal.App.4th 1228, 1259 [29 Cal. Rptr. 3d 521].) Under *Shulman* and section 652B of the Restatement Second of Torts, gaining *access* to information about the plaintiffs that they reasonably believed would remain private is an intrusion into their seclusion. [6] The extent to which images [**788] of the plaintiffs were "captured" or "observed" by the defendants or third parties as a result of the defendants' intrusion may have an impact on the amount of damages the plaintiffs may recover, but it does not impact the defendants' liability for the intrusion.

> 6 Judicial Council of California Civil Jury Instructions (2004-2005) CACI No. 1800 also reflects this interpretation of intrusion. Notably, this approved jury instruction does *not* require that the jury find the plaintiffs were captured or observed by the intrusion, merely that the intrusion occurred:
>
> To establish a claim of intrusion *plaintiffs* must prove all of the following:
>
> "1. That [plaintiffs] had a reasonable expectation of privacy in [*insert facts regarding the place, conversation, or other circumstance*];
>
> "2. That [defendants] intentionally intruded in [*insert facts regarding the place, conversation, or other circumstance*];
>
> "3. That [defendants'] intrusion would be highly offensive to a reasonable person;
>
> "4. That [plaintiffs] were harmed; and
>
> "5. That [defendants'] conduct was a substantial factor in causing [plaintiffs'] harm."

[***19] The Legislature, in providing a statutory remedy for the offensive conduct of the so-called "paparazzi" or other persons engaged in similar invasive conduct, has recognized and relied upon this same analysis. Civil Code section 1708.8, subdivision (b), imposes liability for a "constructive invasion of privacy." That subdivision subjects a person to liability when that person "attempts to capture, in a manner that is offensive to a reasonable person, any [*1388] type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal ... 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." While this statute by its terms does not apply to the circumstances of this case, we note that subdivision (j) of section 1708.8 expressly states, "[i]t is not a defense to a violation of this section that no image,

recording, or [***20] physical impression was captured ... ." [7] Thus, it is the *intrusion* into plaintiffs' seclusion itself that is the actionable wrong.

> 7 Similarly, Penal Code section 632, which prohibits recording confidential communications, is violated the moment the recording is made without consent, regardless of whether it is subsequently disclosed. (*Marich v. MGM/UA Telecommunications, Inc.* (2003) 113 Cal.App.4th 415, 425 [7 Cal. Rptr. 3d 60].)

Several courts in other jurisdictions have considered whether an intrusion *alone* is actionable, and have reached the same result. In a Michigan Appellate Court case, the plaintiff and her daughter sued the owner of a roller skating rink, after the two had used the ladies' room in the rink and discovered "that the defendant had installed see-through panels in the ceiling of the restroom which permitted surreptitious observation from above the interior, including the separately partitioned stalls." (*Harkey v. Abate* (1984) 131 Mich.Ct.App. 177 [346 N.W.2d 74, 75].) [***21] The court held, over a dissent, that the plaintiff could recover despite having no proof that she and her daughter were viewed. "The type of invasion of privacy asserted by plaintiff does not depend upon any publicity given to the person whose interest is invaded, but consists solely of an intentional interference with his or her interest in solitude or seclusion of a kind that would be highly offensive to a reasonable person. [Citation.] Clearly, plaintiff and her daughter in this case had a right to privacy in the public restroom in question. *In our opinion, the installation of the hidden viewing devices alone constitutes an interference with that privacy which a reasonable person would find highly offensive*. And though the absence of proof that the devices were utilized is relevant to the question of damages, it is not fatal to plaintiff's case." (*Id*. at p. 76, italics added.)

In *Carter v. Innisfree Hotel, Inc.* (Ala. 1995) 661 So. 2d 1174, the plaintiff husband and wife discovered that a mirror in their hotel room had been scratched on the back in order to enable someone to view their room from an [*1389] adjacent room. While it was a disputed issue of fact [***22] as to whether someone had *actually* viewed the plaintiffs in their hotel room, the Alabama Supreme Court concluded that proof that the plaintiffs had been viewed was not a prerequisite [**789] for recovery. "There can be no doubt that the possible intrusion of foreign eyes into the private seclusion of a customer's hotel room is an invasion of that customer's privacy." (*Id*. at p. 1179.) [8]

> 8 In *New Summit Associates v. Nistle* (1987) 73 Md.Ct.Spec.App. 351 [533 A.2d 1350], plaintiff found scratches on the back of the bathroom mirror in her apartment, which allowed her bathroom to be viewed by someone in the neighboring vacant apartment, which was undergoing renovations. The court concluded the plaintiff "was not required to prove that a *particular* individual *actually observed* her while she used the facilities in her bathroom. The intentional act that exposed that private place intruded upon [plaintiff's] seclusion." (*Id*. at p. 1354.) However, the court held that the plaintiff could not recover from the landlord and management company defendants, as there was no proof either of them (or their agents) had committed the intrusion. (*Ibid*.)

[***23] Finally, in *Hamberger v. Eastman* (1964) 106 N.H. 107 [206 A.2d 239], the plaintiffs rented a house adjacent to the house of their landlord. They discovered the defendant had installed in their bedroom a listening and recording device, which was connected by wires to the defendant's house. The defendant argued there could be no cause of action as the plaintiffs did not allege that anyone listened to any sounds from their bedroom. The New Hampshire Supreme Court disagreed, holding that "actual or potential" publicity with respect to private matters constitutes a compensable injury. (*Id*. at p. 242.)

(4) Thus, we conclude that the mere placement of the surveillance equipment on the shelf in plaintiffs' office itself invaded their privacy because it allowed defendants, or anyone with access to the storage room, to "activate" the surveillance system at any time during the day without plaintiffs' knowledge, thus at least presenting the possibility of unwanted access to private data about plaintiffs. (*Shulman, supra,* 18 Cal.4th at p. 232.) Plaintiffs need not show more in order to establish their cause of action. [9]

> 9 In any event, even if publication were an element of the intrusion cause of action, defendants failed to defeat it. Defendants offer only Hitchcock's deposition testimony as evidence that plaintiffs were never viewed, despite the fact that Hitchcock himself stated that three other people knew where the surveillance system was located, where it was broadcasting, and were able to access the locked storage room. Moreover, while defendants argue that the system was only set up to record three times, they offer no dates or estimates as to when those incidents

occurred. Hitchcock stated that he would activate the system at night and deactivate it in the morning, yet he was not at Hillsides on the day that the system was found and thus could not have deactivated it that morning. Therefore, even if publication or "viewing" were an element of invasion of privacy, there would remain a triable issue of fact as to what dates and what times of the day the surveillance system was recording and/or broadcasting and whether or not anyone besides Hitchcock had used the storage room during the three weeks he had used it as the "control room" for the surveillance.

[*1390] [***24] 4. *Defendants Did Not Establish that Plaintiffs Did Not Have a Reasonable Expectation of Privacy in Their Office*

(5) As a matter of law, a claim of intrusion cannot fail merely because the events or conversations which the defendant intruded upon were not completely private from all other eyes and ears. (*Sanders v. American Broadcasting Companies* (1999) 20 Cal.4th 907, 911 [85 Cal. Rptr. 2d 909, 978 P.2d 67].) Privacy is not a binary, all-or-nothing characteristic; it has degrees and nuances. (*Id.* at p. 916.) An expectation of privacy in a given setting is not unreasonable just because the privacy expected is not complete or absolute. (*Ibid.*) "[I]n the workplace, as elsewhere, the reasonableness of a person's expectation of [**790] visual and aural privacy depends not only on who might have been able to observe the subject interaction, but on the identity of the claimed intruder and the means of intrusion." (*Id.* at p. 923.)

While plaintiffs did not enjoy complete and absolute privacy in their office, it was reasonable for them to expect images of them in their office with the door closed would not be transmitted to another portion of the building. Hitchcock was [***25] not leaning down and peeking through the doggie door or peering through the window in the office, but he was, in effect, secretly hidden in the office with plaintiffs via the installed surveillance equipment which had the ability to transmit plaintiffs' images onto the monitor in the storage closet across the hall. The fact that plaintiffs were employees and that a passerby in the hallway could have attempted to look in the office via the doggie door does not, as a matter of law, deny them protection against the unwanted intrusion represented by defendants' secret installation of a hidden camera.

5. *Factual Issues Remain As To the "Offensiveness" of Defendants' Conduct and Their Claimed Justification*

a. *The "Offensiveness" Issue*

(6) If a defendant has intruded on a plaintiff's objectively reasonable privacy, the plaintiff must next establish the intrusion was "highly offensive" in order to recover. Offensiveness inquires as to " 'the degree of intrusion, the context, the conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.' " (*Wilkins v. National Broadcasting Co., supra,* 71 Cal.App.4th at pp. 1075-1076, [***26] quoting *Miller v. National Broadcasting Co., Inc., supra,* 187 Cal. App. 3d at pp. 1483-1484.) Whether or not something is offensive also depends on the particular method [*1391] of intrusion used. (*Shulman, supra,* 18 Cal.4th at pp. 236-237.) Difficult cases involve photographic and electronic recording equipment because of the potential for use in ways that severely threaten personal privacy. (*Shulman, supra,* at p. 237.) There is no bright line rule on this question, and every case must be determined on its facts. (*Ibid.*)

A reasonable jury could conclude that the intrusion into plaintiffs' office in this case is highly offensive. Defendants placed a motion-activated camera in a private office shared by plaintiffs, and left it functioning for *no legitimate reason* while plaintiffs were present. Nor did defendants alert plaintiffs to the presence of the camera, so they could modify their behavior to protect their own privacy. Under these circumstances, defendants have not established as a matter of law that their conduct was not highly offensive. Thus, a triable issue of fact exists which must be resolved upon remand.

b. *The Justification* [***27] *Issue*

Defendants argue that their surveillance was necessary and justified to catch whoever was accessing illicit pornographic Web sites in the early hours of the morning, in violation of Hillsides' computer usage policies. The only evidence, however, offered by defendants to show their need to engage in this surveillance is the declaration of Tom Foster, the computer technician, and the deposition of Hitchcock. While Foster stated that in July 2002 the Web logs he maintained for Hillsides in their mainframe computer indicated [**791] that illicit pornographic Web sites had been accessed, he offered no description of the type of sites accessed, how frequently, or their Web addresses. Hitchcock has consistently stated that the Web logs reflected Web sites that justified surveillance of plaintiffs' office, but has never provided the logs, the titles of the Web sites, or any description of the Web sites more elaborate than "immoral," "illicit," and "pornographic."

While it is possible that these Web sites are so alarming and potentially threatening to the well-being of children at Hillsides that surveillance would be justified, defendants simply do not offer anything more than conclusory statements [***28] that they had information that the Web sites were pornographic and being accessed from a computer in plaintiffs' office. Why defendants failed to produce this presumably compelling evidence in support of their motion for summary judgment was not explained.

Even assuming, arguendo, that defendants were justified in their actions, it is undisputed that the offensive Web sites were only being accessed at night. Hitchcock admitted the camera did not need to be in the office during the hours that plaintiffs were working and that he had no suspicions as to [*1392] plaintiffs' activities. In fact, the first occasion Hitchcock used the surveillance system in plaintiffs' office, he placed the camera and motion detector in the office after hours and removed it prior to plaintiffs' arrival the next morning. Defendants offer no explanation as to why the second and third occasions required leaving the camera and motion detector in plaintiffs' office during the day for three weeks when any of the four people with knowledge of the surveillance system could have activated the system without plaintiffs' knowledge. Thus, defendants have failed to conclusively establish their surveillance was justified under [***29] the circumstances. This is another issue that must be resolved by a trier of fact.

6. *Intentional Infliction of Emotional Distress and Negligent Infliction of Emotional Distress*

(7) Invasion of a person's peace of mind is an independent wrong that, in and of itself, gives rise to liability. (*Shulman, supra,* 18 Cal.4th at p. 232.) Intentional infliction of emotional distress requires " ' " 'extreme and outrageous conduct by the defendant with the intention of causing, or reckless disregard [for] the probability of causing, emotional distress' " ' " (*Wilkins v. National Broadcasting Co., supra,* 71 Cal.App.4th at p. 1087.) The conduct must be "so extreme and outrageous 'as to exceed all bounds of that usually tolerated in a civilized society.' " (*Ibid.*) Given that the placement of the camera was not intended to spy on plaintiffs and, in fact, was only intended to be activated when they were not in the office, we find, as a matter of law, that defendants' conduct does not rise to the level of "extreme and outrageous." Thus, plaintiffs cannot prevail on their cause of action for intentional infliction of emotional distress. Summary resolution [***30] of this cause of action in favor of defendants is appropriate.

(8) As to plaintiffs' cause of action for negligent infliction of emotional distress, "[t]he negligent causing of emotional distress is not an independent tort but the tort of negligence, involving the usual duty and causation issues." (6 Witkin, Summary of Cal. Law (10th ed. 2005) Torts, § 1004, p. 270.) Plaintiffs' complaint alleges no duty breached, but only alleges that defendants' intentional act of placing the camera in their office caused them emotional distress. Emotional distress damages may be recoverable as part of the [**792] general damages if plaintiffs prevail on their invasion of privacy cause of action. (CACI No. 1820.) As such, plaintiffs' purported cause of action for "negligent infliction of emotional distress" is both legally without merit and factually superfluous. Summary resolution of this cause of action is thus also appropriate.

[*1393] ***DISPOSITION***

The judgment is reversed. The matter is remanded with directions to vacate the order granting the motion for summary judgment and enter a new and different order denying the motion for summary judgment and granting summary adjudication [***31] of plaintiffs' causes of action for intentional infliction of emotional distress and negligent infliction of emotional distress. The trial court shall then conduct such further proceedings as are appropriate in a manner not inconsistent with the views expressed herein. Plaintiffs shall recover their costs on appeal.

Kitching, J., and Aldrich, J., concurred.

HYPOTHETICAL No. 3

LEGAL OFF-DUTY CONDUCT

An establishment that features exotic dancers is located within your district. Almost daily, shortly after the end of the school day, the car of a district teacher is seen parked outside the establishment. Many parents in the community have approached you asking that something be done about the teacher's conduct.

What should you do?

I. Outline of Presentation.

A. Constitutional rights and private activities.

Any attempt by a public employer to control or monitor off-duty conduct could result in the employee alleging a violation of various Constitutional rights, including the right of privacy.

The California Constitution, article I, section 1, explicitly recognizes a right of privacy. The United States Constitution has been held to contain an implicit right of privacy. A person does not surrender his or her right to privacy by virtue of becoming a public employee. (*Long Beach City Employees Ass'n v. City of Long Beach* (1986) 41 Cal.3d 937, 951.)

The California Constitution, Article I, Section 1, provides:

> 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.

B. The legal burden.

The courts have extended broad protections to public employees based upon unnamed constitutionally protected rights.

A public employer may not deny employment or discipline an employee due to private activities unless the employer can show:

1. Those activities will have an adverse impact on the employee's job performance; and

2. The discrimination against the employee for the exercise of constitutional rights is justified by a compelling public interest.

Bogacki v. Board of Supervisory (1971) 5 Cal. 3d 771, 778.

C. Examples of Constitutionally-protected areas:

The following are areas found to be protected, absent a compelling public interest:

Wearing a beard. *Finot v. Pasadena City Bd. Of Education* (1967) 250 Cal.App. 2d 189, 198.

Sexual orientation. *Gay Law Students Assn. V. Pacific Tel. & Tel. Co.* (1979) 24 Cal.3d 458, 474-475.

Personal activities without a compelling job-related justification. *Thorne v. City of El Segundo* (9th Cir. 1983) 726 F.2d 459, 470.

HYPOTHETICAL NO. 4

ELECTRONIC COMMUNICATIONS & EMPLOYEE PRIVACY

When he was hired five years ago, a classified employee in the Heavenly Unified School District was given a copy of, and signed for, a district policy which prohibited the personal use of district computers and stated that district employees should have no expectation of privacy when using district computers. Last year, the district acquired pagers with texting capability and one of them was assigned to the employee. The district did not update its policy to include pagers or texting. In announcing the pager program, the employee's supervisor told employees receiving pagers that the district would not audit pager use so long as the employee paid for any usage that resulted in an "overage" charge. On several occasions, the employee paid for overages.

Recently, to determine the effectiveness of the pager program, the Business Office audited the usage of all pagers assigned to employees. The audit discovered that the employee sent and received many, highly sexually explicit, personal messages.

After a hearing in which the text messages were introduced as evidence over the objection of the employee's lawyer, the district's board of trustees terminated the employee. The employee sued, alleging that the district had violated his Fourth Amendment and California Constitutional rights against unreasonable search and seizure by accessing, divulging and reviewing the contents of his personal text messages.

The appellate court held that the district violated the employee's Fourth Amendment rights. The Court said the employee had a reasonable expectation of privacy in his pager messages because pagers were not listed on the AUP and the supervisor told the employee his pager usage would not be audited. (See *Quon v. Arch Wireless Operating Incorporated Company, et al [2008] 529 F3d. 892.)*

I. Outline of Presentation

Public employees have much greater electronic communications and privacy rights than do private employees.

A. To some extent, most private and public employers monitor, record or review employee communications on the job.

Nearly a decade ago, more than 75 percent of the major private firms in the United States were already monitoring, recording, and reviewing employee communications and activities on the job, including their telephone calls, e-mails, Internet connections, and computer files. (*TBG Insurance Services Corp. v. Superior Court [Los Angeles]* [2002] 96

Cal.App.4th 443, 451.) That percentage likely is higher now, considering the proliferation of and advances in technology over the past eight years, as well as the emerging need for employers to protect themselves, their employees, customers and others, in a variety of situations, including:

- E mails containing malware or links to malicious websites.
- Theft of confidential, personal information by hackers.
- Loss of productivity caused by web-surfing and other abuses.
- The use of employer electronic devices to commit a crime.
- Federal funding statutes that require recipient public agencies to monitor and filter Internet connections to prevent access to websites with pornography or material offensive to minors.
- The legal duty of employers to prevent, investigate and correct unlawful discrimination and harassment, which may involve inspection of e-mail content, Internet connections, text messaging, telephone traffic and other electronic evidence.

B. However, public employees have much greater privacy rights in their electronic communications than do private employees.

In contrast to private employees, public employees are protected by constitutional provisions that limit the conduct of their public employer in obtaining information about them, and in acting upon that information. These include:

1. A federal constitutional due process right to prior notice or prohibited conduct, as well as notice of disciplinary action and the right to be heard before discipline is imposed. In the absence of clear Acceptable Use Policy, a public employer may not be able to take disciplinary action based on an employee's use of electronic devices.

2. Public employees also have privacy rights protected by the First Amendment and the California constitution, as well as a Fourth Amendment right against unreasonable search and seizure by their public employer. A violation of these rights can lead to a money damages lawsuit, as well as an inability to use the information obtained against the employee.

3. Public employees also have First Amendment free speech rights that can be implicated in electronic communications, including the right to petition the government for redress of grievances.

4. All public employers should adopt an Acceptable Use Policy, (AUP), that defines the electronic devices subject to the policy, the level of employee privacy related to the use of those devices, the permissible and impermissible uses of those devices, and the consequences for impermissible uses.

5. Every employee and every supervisor should know and understand the employer's AUP.

6. The best practices for implementing an AUP are:

a. have a legitimate business reason for any examination;
b. limit the scope of the examination to the justification;
c. obtain prior approval as specified in the AUP, or from at least one level higher in the organization;
d. implement the AUP in a viewpoint-neutral manner;
e. obtain legal advice.

7. Examples of communication that may be protected, depending on the facts:

criticism of public officials or policies;
discrimination complaints;
whistle-blowing complaints;
religious speech (prayer meeting invitation);
political speech (board elections);
union speech.

8. However, as a matter of law, no employee can have a reasonable expectation of privacy in public records covered by the California Public Records Act.

Government Code sections 6252(e) and 6253(b) define "public records" as:

Any "writing" containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics, unless the writing is exempt from disclosure by express provisions of law.

9. Examples of records not exempt from disclosure under CPRA are:

a. An employee's gross salary (*International Federation of Professional and Technical Engineers v. Superior Court* (2007) 42 Cal.4th 319)

b. Records of substantial complaints of employee misconduct and related investigations (*Bakersfield City School District v. Superior Court* (2004) 118 Cal.App.4th 1041)

10. No AUP can prevent other types of disclosure of records required by law, such as:

Search warrants;
Subpoenas;
Discovery during litigation;
The Patriot Act.

_____ SCHOOL DISTRICT

EMPLOYEE ACCEPTABLE USE POLICY FOR DISTRICT COMPUTERS, ELECTRONIC DEVICES, NETWORK AND OTHER ELECTRONIC INFORMATION RESOURCES

School District recognizes that electronic information resources can enhance productivity, facilitate professional communication, and assist in providing quality educational programs. This policy applies to, and describes the responsibilities and obligations of, all District employees using the District's electronic information resources, including the District's computers, electronic devices, and network.

1. Description of the District's Electronic Information Resources. The District's electronic information resources covered by this policy include the District's computers, electronic devices, and network.

A. Definition of "District Computer":

The term "District computer" means any computer, including a laptop computer, that is owned, leased or rented by the District, purchased with funds from a grant approved by or awarded to the District, or borrowed by the District from another agency, company or entity, whether or not the computer is equipped with a modem or communication peripheral capable of digital connection.

B. Definition of "District Electronic Device":

The term "District electronic device" means any device other than a District computer that is capable of transmitting, receiving, or storing digital media and is owned, leased, or rented by the District, purchased with funds from a grant approved by or awarded to the District, or borrowed by the District from another agency, company or entity, whether or not the electronic device is portable and whether or not the electronic device is equipped with a modem or other communication peripheral capable of digital connection.

District electronic devices include but are not limited to:

- telephones;
- cellular telephones;
- radios;
- pagers;
- voice mail;
- e-mail;
- text messages;
- digital cameras;
- personal digital assistants such as Palm Pilots and Smart Phones;
- portable storage devices such as thumb drives and zip drives;
- portable media devices such as IPODs and MP3 players;
- optical storage media such as compact discs (CDs) and digital versatile discs (DVDs);
- printers and copiers;
- fax machines.

C. Definition of "District Electronic Network":

The term "District electronic network" means the District's Local Area, District-wide, and Internet systems, including software, e-mail and voice mail systems.

2. Ownership. The District's electronic information resources, including District laptop computers and portable electronic devices, are District property, provided to meet District needs. They do not belong to employees.

All District computers and electronic devices, including District laptop computers and portable electronic devices, are to be registered to the District, and not to the employee. All software on District computers and electronic devices, including District laptop computers and portable electronic devices, is to be registered to the District, and not to the employee, except as provided in Section 6.

No employee shall remove a District computer or electronic device from District property without the prior, express authorization of _____.

The use of District electronic information resources is a privilege which the District may revoke or restrict at any time without prior notice to the employee.

3. No Employee Privacy. Employees have no privacy whatsoever in their personal or work-related use of the District's computers, electronic devices, network, and other electronic information resources, or to any communications or other information in the District's electronic information resources or that may pass through District electronic information resources. The District retains the right, with or without cause, and with or without notice to the employee, to remotely monitor, physically inspect, or examine the District's computers, electronic devices, network, or other electronic information resources, and any communication or information stored on or passing through the District's electronic information resources, including but not limited to software, data and image files, Internet use, e-mails, text messages, and voice mail.

When an employee leaves the employment of the District, management shall be given access to, and the authority to dispose of, any and all of his or her computer files, e-mail, voice mail, text messages, and any other electronically stored information.

4. Personal Use. Employees shall use the District's computers, electronic devices, network, and other electronic information resources primarily for purposes related to their employment. District laptop computers and portable electronic devices shall be used solely by authorized employees, and not by family members or other unauthorized persons.

Where approved by _____ in advance, an employee may make minimal personal use of District electronic information resources as long as such use does not violate this policy, does not result in any additional fee or charge to the District, and does not interfere with the District's normal business practices or the performance of an employee's duties. As described in Section 3, employees have no privacy whatsoever in their personal use of the District's computers, electronic devices, and network, including but not limited to software, data and image files, Internet use, text messages, and e-mails.

5. Password Protection. To protect against unauthorized use, all District computers and electronic devices, including laptop computers, that are capable of being password protected, shall be password protected, even if a computer or electronic device is assigned to a single employee for his or her sole use. If password protection is not technically feasible, the employee to whom the computer or electronic device is assigned shall be responsible for physically protecting it against unauthorized use. A screen saver which is capable of being password protected shall be password protected.

Each employee shall be responsible for registering his or her password(s) with _____, whether the password protection is at the system level or program level. The District needs the ability to access its own equipment.

6. Software and Electronic Devices. Software, computers, and electronic devices must meet specific standards to protect the District's network and other electronic information resources. In addition, violations of software copyright law have the potential of costing the District millions of dollars.

Therefore, a technology administrator shall be designated at _____. Only the designated technology administrator at _____ shall be allowed to authorize: (1) the installation, maintenance, or removal of software on District computers and electronic devices; and (2) the connection of non-District electronic devices to District computers.

Unless directed to or authorized by _____, no employee shall install, maintain, or remove software on District computers and electronic devices. Unless directed to or authorized by _____, no employee shall connect an electronic device to District computers, whether hardwired or wireless.

_____ is authorized to approve employee requests for the installation of non-District software, subject to the following limitations:

A. Software not [reasonably] related to the mission of the District shall not be installed.

B. No software shall be installed without written proof of licensing, which shall be retained by _____. Multiple installations of the same license number will be assumed to violate copyright unless a multiple license provision can be demonstrated.

C. The employee shall surrender to the District all rights whatsoever he or she may have in the software, including but not limited to the following:

- The District has the right to remove the software at any time and for any reason without prior notice to the employee.
- The District has no obligation to return the software to the employee.
- If the employee is assigned to a different computer or electronic device, the District has no obligation to install the software on that equipment.

Employees who have been authorized to download and install software shall run the most up-to-date District approved anti-virus software on all files and programs downloaded, and shall adhere to copyrights, trademarks, licenses, and contractual agreements applicable to the software, including provisions prohibiting the duplication of material without proper authorization and the inclusion of copyright notices in any use of the material.

7. Filters and Other Internet Protection Measures. To ensure that the use of the District's network is consistent with the District's mission, the District uses content and bandwidth software to prevent access to pornographic and other websites that are inconsistent with the mission and values of the District. No employee shall bypass or evade, or attempt to bypass or evade, the District's filter system.

8. Other Unacceptable Uses. In addition to the previous requirements, employees using the District's computers, electronic devices or network shall be responsible for using them only in compliance with the following requirements.

A. An employee shall use only his or her assigned account or password to access District computers, electronic devices, and network. No employee shall permit the use of his or her assigned account or password, or use another person's assigned account or password, without the prior express, written consent of _____.

B. Employees are prohibited from using the District's computers, electronic devices, network and other electronic resources for knowingly transmitting, receiving, or storing any oral or written communication that is obscene, threatening or disruptive, or that reasonably could be construed as harassment or disparagement of others based on their race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, sex, age, or sexual orientation. This prohibition applies to written and oral communication of any kind, including music.

C. Employees are prohibited from using the District's computers, electronic devices and network for knowingly transmitting, receiving, or storing any visual image that depicts actual or simulated torture, bondage, or physical abuse of any human being or other creature, or that is sexually explicit.

(1) "Sexually explicit" includes, but is not limited to depictions of actual or simulated human sex acts, and the unclothed human genitalia, pubic area, anus, buttocks, and female breast that lack serious artistic, literary, scientific, or political value.

(2) This prohibition applies to visual depictions of any kind, including screen savers, drawings, cartoons and animations.

D. Employees shall not knowingly store or transmit copyrighted material on the District's computers, electronic devices, or network without the permission of the holder of the copyright. Employees shall download copyrighted material only in accordance with applicable copyright laws.

E. Employees are prohibited from knowingly using the District's computers, electronic devices, and network to intentionally access information intended to be private or restricted; change data created or owned by another user or any other agency, company or network; make any unauthorized changes to the appearance or operational characteristics of the District's system; load, upload, download or create a computer virus; alter the file of any other user or entity; or remove, change or add a password without the approval of _____.

F. Employees are prohibited from remotely accessing any District computer or server without prior express written approval of _____.

G. Employees are prohibited from uploading to a non-District server any file contained on a District computer or server; whether the file is work related or personal, unless the employee has been granted the prior express written approval of _____.

H. Any text transmission can only be used by authorized District blog messaging systems and/or device.

I. Employees also are prohibited from using the District's computers, electronic devices, and network for:

(1) personal financial gain;

(2) commercial advertising;

(3) political activity as defined in Education Code sections 7050-7058;

(4) religious advocacy;

(5) promoting charitable organizations;

(6) communicating in someone else's name;

(7) attempting to breach network security;

(8) creating, sending or receiving materials that are inconsistent with the mission and values of the District;

(9) mass distribution of e-mail to a school site without the prior approval of ____.

(10) mass distribution of e-mail to the District office without the approval of _____.

(11) accessing pornographic or other websites that are inconsistent with the mission and values of the District;

(12) any activity prohibited by law, Board policy or administrative regulations, or the rules of conduct described in the _____ Administrative Code.

9. Violation of This Policy. Technology employees shall promptly report violations of this policy to _____.

Employees who violate this policy are subject to discipline, up to and including termination, pursuant to the provisions of applicable laws governing employee discipline, and applicable District policies, procedures and collective bargaining agreements. The employee's use of the District's electronic information resources also may be restricted, suspended, or revoked.

JERILYN QUON; APRIL FLORIO; JEFF QUON; STEVE TRUJILLO, Plaintiffs-Appellants, v. ARCH WIRELESS OPERATING COMPANY, INCORPORATED, a Delaware corporation; CITY OF ONTARIO, a municipal corporation; LLOYD SCHARF, individually and as Chief of Ontario Police Department; ONTARIO POLICE DEPARTMENT; DEBBIE GLENN, individually and as a Sergeant of Ontario Police Department, Defendants-Appellees.

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

529 F.3d 892; 2008 U.S. App. LEXIS 12766; 91 Empl. Prac. Dec. (CCH) P43,233; 27 I.E.R. Cas. (BNA) 1377

February 6, 2008, Argued and Submitted, Pasadena, California
June 18, 2008, Filed

DISPOSITION: The judgment was affirmed in part, specifically, that defendant police chief was entitled to qualified immunity; but it was reversed in part, specifically, that the employees were entitled to judgment as a matter of law as to their SCA, Fourth Amendment, and state constitutional claims. Therefore, the case was remanded for further proceedings.

COUNSEL: Dieter C. Dammeier, Zahra Khoury, Lackie & Dammeier APC, Upland, California, for the plaintiffs-appellants.

Dimitrios C. Rinos, Rinos & Martin, LLP, Tustin, California; Kent L. Richland, Kent J. Bullard, Greines, Martin, Stein & Richland LLP, Los Angeles, California, for defendants-appellees City of Ontario, Ontario Police Department, and Lloyd Scharf.

Bruce E. Disenhouse, Kinkle, Rodiger and Spriggs, Riverside, California, for defendant-appellee Debbie Glenn.

John H. Horwitz, Schaffer, Lax, McNaughton & Chen, Los Angeles, California, for defendant-appellee Arch Wireless, Inc.

JUDGES: Before: Harry Pregerson and Kim McLane Wardlaw, Circuit Judges, and Ronald B. Leighton, * District Judge.

* The Honorable Ronald B. Leighton, United States District Judge for the Western District of Washington, sitting by designation.

OPINION BY: Kim McLane Wardlaw

OPINION

[*895] WARDLAW, Circuit Judge:

This case arises from the Ontario Police Department's review of text messages sent and received by Jeff Quon, a Sergeant and member of the City of Ontario's SWAT team. We must decide whether [**2] (1) Arch Wireless Operating Company Inc., the company with whom the City contracted for text messaging services, violated the Stored Communications Act, 18 U.S.C. §§ 2701-2711 (1986); and (2) whether the City, the Police Department, and Ontario Police Chief Lloyd Scharf violated Quon's rights and the rights of those with whom he "texted"--Sergeant Steve Trujillo, Dispatcher April Florio, and his wife Jerilyn Quon [1] -- under the Fourth Amendment to the United States Constitution and Article I, Section 1 of the California Constitution.

1 Doreen Klein, a plaintiff below, has not filed an appeal.

I. FACTUAL BACKGROUND

On October 24, 2001, Arch Wireless ("Arch Wireless") contracted to provide wireless text-messaging services for the City of Ontario. The City received twenty two-way alphanumeric pagers, which it distributed to its employees, including Ontario Police Department ("OPD" or "Department") Sergeants Quon and Trujillo, in late 2001 or early 2002.

According to Steven Niekamp, Director of

Information Technology for Arch Wireless:

> A text message originating from an Arch Wireless two-way alphanumeric text-messaging pager is sent to another two-way text-messaging pager as follows: The message [**3] leaves the originating pager via a radio frequency transmission. That transmission is received by any one of many receiving stations, which are owned by Arch Wireless. Depending on the location of the receiving station, the message is then entered into the Arch Wireless computer network either by wire transmission or via satellite by another radio frequency transmission. [*896] Once in the Arch Wireless computer network, the message is sent to the Arch Wireless computer server. Once in the server, a copy of the message is archived. The message is also stored in the server system, for a period of up to 72 hours, until the recipient pager is ready to receive delivery of the text message. The recipient pager is ready to receive delivery of a message when it is both activated and located in an Arch Wireless service area. Once the recipient pager is able to receive delivery of the text message, the Arch Wireless server retrieves the stored message and sends it, via wire or radio frequency transmission, to the transmitting station closest to the recipient pager. The transmitting stations are owed [sic] by Arch Wireless. The message is then sent from the transmitting station, via a radio frequency [**4] transmission, to the recipient pager where it can be read by the user of the recipient pager.

The City had no official policy directed to text-messaging by use of the pagers. However, the City did have a general "Computer Usage, Internet and E-mail Policy" (the "Policy") applicable to all employees. The Policy stated that "[t]he use of City-owned computers and all associated equipment, software, programs, networks, Internet, e-mail and other systems operating on these computers is limited to City of Ontario related business. The use of these tools for personal benefit is a significant violation of City of Ontario Policy." The Policy also provided:

> C. Access to all sites on the Internet is recorded and will be periodically reviewed by the City. The City of Ontario 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.
>
> D. Access to the Internet and the e-mail system is **not** confidential; and information produced either in hard copy or in electronic form is considered City property. As such, these systems should not be used for personal [**5] or confidential communications. Deletion of e-mail or other electronic information may not fully delete the information from the system.
>
> E. The use of inappropriate, derogatory, obscene, suggestive, defamatory, or harassing language in the e-mail system will not be tolerated.

In 2000, before the City acquired the pagers, both Quon and Trujillo had signed an "Employee Acknowledgment," which borrowed language from the general Policy, indicating that they had "read and fully understand the City of Ontario's Computer Usage, Internet and E-mail policy." The Employee Acknowledgment, among other things, states that "[t]he City of Ontario reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice," and that "[u]sers should have no expectation of privacy or confidentiality when using these resources." Two years later, on April 18, 2002, Quon attended a meeting during which Lieutenant Steve Duke, a Commander with the Ontario Police Department's Administration Bureau, informed all present that the pager messages "were [**6] considered e-mail, and that those messages would fall under the City's

policy as public information and eligible for auditing." Quon "vaguely recalled attending" this meeting, but did not recall Lieutenant Duke stating at the meeting that use of the pagers was governed by the City's Policy.

[*897] Although the City had no official policy expressly governing use of the pagers, the City did have an informal policy governing their use. Under the City's contract with Arch Wireless, each pager was allotted 25,000 characters, after which the City was required to pay overage charges. Lieutenant Duke "was in charge of the purchasing contract" and responsible for procuring payment for overages. He stated that "[t]he practice was, if there was overage, that the employee would pay for the overage that the City had. . . . [W]e would usually call the employee and say, 'Hey, look, you're over X amount of characters. It comes out to X amount of dollars. Can you write me a check for your overage[?]' "

The informal policy governing use of the pagers came to light during the Internal Affairs investigation, which took place after Lieutenant Duke grew weary of his role as bill collector. In a July 2, 2003 memorandum [**7] entitled "Internal Affairs Investigation of Jeffery Quon," (the "McMahon Memorandum") OPD Sergeant Patrick McMahon wrote that upon interviewing Lieutenant Duke, he learned that early on

> Lieutenant Duke went to Sergeant Quon and told him the City issued two-way pagers were considered e-mail and could be audited. He told Sergeant Quon it was not his intent to audit employee's [sic] text messages to see if the overage is due to work related transmissions. He advised Sergeant Quon he could reimburse the City for the overage so he would not have to audit the transmission and see how many messages were non-work related. Lieutenant Duke told Sergeant Quon he is doing this because if anybody wished to challenge their overage, he could audit the text transmissions to verify how many were non-work related. Lieutenant Duke added the text messages were considered public records and could be audited at any time.

For the most part, Lieutenant Duke agreed with McMahon's characterization of what he said during his interview. Later, however, during his deposition, Lieutenant Duke recalled the interaction as follows:

> I think what I told Quon was that he had to pay for his overage, that I did not want to [**8] determine if the overage was personal or business unless they wanted me to, because if they said, "It's all business, I'm not paying for it," then I would do an audit to confirm that. And I didn't want to get into the bill collecting thing, so he needed to pay for his personal messages so we didn't--pay for the overage so we didn't do the audit. And he needed to cut down on his transmissions.

According to the McMahon Memorandum, Quon remembered the interaction differently. When asked "if he ever recalled a discussion with Lieutenant Duke that if his textpager went over, his messages would be audited . . . Sergeant Quon said, 'No. In fact he [Lieutenant Duke] said the other, if you don't want us to read it, pay the overage fee.' "

Quon went over the monthly character limit "three or four times" and paid the City for the overages. Each time, "Lieutenant Duke would come and tell [him] that [he] owed X amount of dollars because [he] went over [his] allotted characters." Each of those times, Quon paid the City for the overages.

In August 2002, Quon and another officer again exceeded the 25,000 character limit. Lieutenant Duke then let it be known at a meeting that he was "tired of being a [**9] bill collector with guys going over the allotted amount of characters on their text pagers." In response, Chief Scharf ordered Lieutenant Duke to "request the transcripts of those pagers for auditing [*898] purposes." Chief Scharf asked Lieutenant Duke "to determine if the messages were exclusively work related, thereby requiring an increase in the number of characters officers were permitted, which had occurred in the past, or if they were using the pagers for personal matters. One of the officers whose transcripts [he] requested was plaintiff Jeff Quon."

City officials were not able to access the text

messages themselves. Instead, the City e-mailed Jackie Deavers, a major account support specialist for Arch Wireless, requesting the transcripts. According to Deavers,

> I checked the phone numbers on the transcripts against the e-mail that I had gotten, and I looked into the system to make sure they were actually pagers that belonged to the City of Ontario, and they were. So I took the transcripts and put them in a manila envelope [and brought them to the City].

Deavers stated that she did not determine whether private messages were being released, though she acknowledged that, upon reviewing [**10] approximately four lines of the transcript, she had realized that the messages were sexually explicit. She also stated that she would only deliver messages to the "contact" on the account, and that she would not deliver messages to the "user" unless he was also the contact on the account. In this case, the "contact" was the City.

After receiving the transcripts, Lieutenant Duke conducted an initial audit and reported the results to Chief Scharf. Subsequently, Chief Scharf and Quon's supervisor, Lieutenant Tony Del Rio, reviewed the transcripts themselves. Then, in October 2002, Chief Scharf referred the matter to internal affairs "to determine if someone was wasting . . . City time not doing work when they should be." Sergeant McMahon, who conducted this investigation on behalf of Internal Affairs, enlisted the help of Sergeant Glenn, also a member of Internal Affairs. Sergeant McMahon released the McMahon Memorandum on July 2, 2003. According to the Memorandum, the transcripts revealed that Quon "had exceeded his monthly allotted characters by 15,158 characters," and that many of these messages were personal in nature and were often sexually explicit. These messages were directed to [**11] and received from, among others, the other Appellants.

II. PROCEDURAL BACKGROUND

On May 6, 2003, Appellants filed a Second Amended Complaint in the District Court for the Central District of California alleging, *inter alia*, violations of the Stored Communications Act ("SCA") and the Fourth Amendment. After the district court dismissed one of Appellants' claims against Arch Wireless pursuant to Federal Rule of Civil Procedure 12(b)(6), all parties filed numerous rounds of summary judgment motions. On August 15, 2006, the district court denied Appellants' summary judgment motion in full, and granted in part and denied in part Appellees' summary judgment motions.

Appellants appeal the district court's holding that Arch Wireless did not violate the SCA, 18 U.S.C. §§ 2701-2711. [2] The district court found that Arch Wireless was a "remote computing service" under § 2702(a), and that it therefore committed no harm when it released the text-message transcripts to its "subscriber," the City.

> 2 Appellants fail to raise on appeal their claims against Arch Wireless for violations of California Penal Code section 629.86 and their state-law invasion of privacy claim under Article I, Section 1 of the California Constitution. [**12] Therefore, they have waived those claims. *See Blanford v. Sacramento County*, 406 F.3d 1110, 1114 n.8 (9th Cir. 2005).

[*899] Appellants also appeal the district court's resolution of their claims against the City, the Department, Scharf, and Glenn. [3] Appellants argue that the City, the Department, and Scharf violated Appellants' Fourth Amendment rights to be free from unreasonable search and seizure pursuant to 42 U.S.C. § 1983, and that the City, Department, Scharf, and Glenn violated Article I, Section 1 of the California Constitution, which protects a citizen's right to privacy. [4] The district court addressed only the Fourth Amendment claim. [5] Relying on *O'Connor v. Ortega*, 480 U.S. 709, 715, 725-26, 107 S. Ct. 1492, 94 L. Ed. 2d 714 (1987), the district court determined that to prove a Fourth Amendment violation, the plaintiff must show that he had a reasonable expectation of privacy in his text messages, and that the government's search or seizure was unreasonable under the circumstances. The district court held that, in light of Lieutenant Duke's informal policy that he would not audit a pager if the user paid the overage charges, Appellants had a reasonable expectation of privacy in their text messages as a matter of [**13] law. Regarding the reasonableness of the search, the district court found that whether Chief Scharf's

intent was to uncover misconduct or to determine the efficacy of the 25,000 character limit was a genuine issue of material fact. If it was the former, the search was unreasonable; if it was the latter, the search was reasonable. Concluding that Chief Scharf was not entitled to qualified immunity on the Fourth Amendment claim, and that the City and the Department were not entitled to statutory immunity on the California constitutional privacy claim, the district court held a jury trial on the single issue of Chief Scharf's intent. The jury found that Chief Scharf's intent was to determine the efficacy of the character limit. Therefore, all defendants were absolved of liability for the search.

> 3 Appellants fail to raise on appeal their claims against the City, the Department, Scharf, and Glenn for violations of the Stored Communications Act and California Penal Code section 629.86. Jerilyn Quon fails to address on appeal her claim for defamation and interference with prospective business advantage; nor does Florio address her claim that seizure of her personal pager and cell phone violated [**14] the Fourth Amendment. Therefore, Appellants have waived those claims. *See Blanford*, 406 F.3d at 1114.
>
> 4 "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." CAL. CONST. art. I, § 1.
>
> 5 The district court limited its discussion to the Fourth Amendment because "the arguments lodged by the governmental defendants against plaintiffs' invasion of privacy claim and state constitutional claim are the same as those pressed against plaintiffs' Fourth Amendment claim . . . ."

On December 7, 2006, Appellants filed a motion to amend or alter the judgment pursuant to Federal Rule of Civil Procedure 59(e), and a motion for new trial pursuant to Rule 59(a). The district court denied each of these motions. Appellants timely appeal.

III. JURISDICTION AND STANDARD OF REVIEW

The district court had jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1343. We have jurisdiction over final judgments of the district courts pursuant to 28 U.S.C. § 1291.

We review a district court's grant of summary judgment de novo. *Bagdadi v. Nazar*, 84 F.3d 1194, 1197 (9th Cir. 1996). [**15] In reviewing the grant of summary judgment, we "must determine, viewing the [*900] evidence in the light most favorable to the nonmoving party, whether genuine issues of material fact exist and whether the district court correctly applied the relevant substantive law." *Id.*

IV. DISCUSSION

A. Stored Communications Act

Congress passed the Stored Communications Act in 1986 as part of the Electronic Communications Privacy Act. The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209-13 (2004). Generally, the SCA prevents "providers" of communication services from divulging private communications to certain entities and/or individuals. *Id.* at 1213. Appellants challenge the district court's finding that Arch Wireless is a "remote computing service" ("RCS") as opposed to an "electronic communication service" ("ECS") under the SCA, §§ 2701-2711. The district court correctly concluded that if Arch Wireless is an ECS, it is liable as a matter of law, and that if it is an RCS, [**16] it is not liable. However, we disagree with the district court that Arch Wireless acted as an RCS for the City. Therefore, summary judgment in favor of Arch Wireless was error.

Section 2702 of the SCA governs liability for both ECS and RCS providers. 18 U.S.C. § 2702(a)(1)-(2). The nature of the services Arch Wireless offered to the City determines whether Arch Wireless is an ECS or an RCS. As the Niekamp Declaration makes clear, Arch Wireless provided to the City a service whereby it would facilitate communication between two pagers--"text messaging" over radio frequencies. As part of that service, Arch Wireless archived a copy of the message on its server. When Arch Wireless released to the City the transcripts of Appellants' messages, Arch Wireless potentially ran afoul of the SCA. This is because both an ECS and RCS can

release private information to, or with the lawful consent of, "an addressee or intended recipient of such communication," *id.* § 2702(b)(1), (b)(3), whereas only an RCS can release such information "with the lawful consent of . . . the subscriber." *Id.* § 2702(b)(3). It is undisputed that the City was not an "addressee or intended recipient," and that the City was [**17] a "subscriber."

The SCA defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15). The SCA prohibits an ECS from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service," unless, among other exceptions not relevant to this appeal, that person or entity is "an addressee or intended recipient of such communication." *Id.* § 2702(a)(1), (b)(1), (b)(3). "Electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17).

An RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711(2). Electronic communication system--which is simply the means by which an RCS provides computer storage or processing services and has no bearing on how we interpret the meaning of "RCS"--is defined as "any wire, radio, electromagnetic, [**18] photooptical or photoelectronic facilities [*901] for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id.* § 2510(14). The SCA prohibits an RCS from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service." Unlike an ECS, an RCS may release the contents of a communication with the lawful consent of a "subscriber." *Id.* § 2702(a)(2), (b)(3).

We turn to the plain language of the SCA, including its common-sense definitions, to properly categorize Arch Wireless. An ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). On its face, this describes the text-messaging pager services that Arch Wireless provided. Arch Wireless provided a "service" that enabled Quon and the other Appellants to "send or receive . . . electronic communications," i.e., text messages. Contrast that definition with that for an RCS, which "means the provision to the public of computer storage or processing services by means of an electronic [**19] communications system." *Id.* § 2711(2). Arch Wireless did not provide to the City "computer storage"; nor did it provide "processing services." By archiving the text messages on its server, Arch Wireless certainly was "storing" the messages. However, Congress contemplated this exact function could be performed by an ECS as well, stating that an ECS would provide (A) temporary storage incidental to the communication; and (B) storage for backup protection. *Id.* § 2510(17).

This reading of the SCA is supported by its legislative history. The Senate Report identifies two main services that providers performed in 1986: (1) data communication; and (2) data storage and processing. First, the report describes the means of communication of information:

> [W]e have large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing . . . . [M]any different companies, not just common carriers, offer a wide variety of telephone and other communications services.

S. REP. NO. 99-541, at 2-3 (1986). Second,

> [t]he Committee also recognizes that computers are used extensively today for the storage and processing of information. [**20] With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services. These services as well as

> the providers of electronic mail create electronic copies of private correspondence for later reference. This information is processed for the benefit of the user but often it is maintained for approximately 3 months to ensure system integrity.

Id. at 3. Under the heading "Remote Computer Services," the Report further clarifies that term refers to the processing or storage of data by an off-site third party:

> In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data inhouse on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today [*902] businesses of all sizes--hospitals, [**21] banks and many others--use remote computing services for computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer. Data is most often transmitted between these services and their customers by means of electronic communications.

Id. at 10-11.

In the Senate Report, Congress made clear what it meant by "storage and processing of information." It provided the following example of storage: "physicians and hospitals maintain medical files in offsite data banks." Congress appeared to view "storage" as a virtual filing cabinet, which is not the function Arch Wireless contracted to provide here. The Senate Report also provided an example of "processing of information": "businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services." In light of the Report's elaboration upon what Congress intended by the term "Remote Computer Services," it is clear that, before the advent of advanced computer processing programs [**22] such as Microsoft Excel, businesses had to farm out sophisticated processing to a service that would process the information. *See* Kerr, 72 GEO. WASH. L. REV. at 1213-14. Neither of these examples describes the service that Arch Wireless provided to the City.

Any lingering doubt that Arch Wireless is an ECS that retained messages in electronic storage is disposed of by *Theofel v. Farey-Jones*, 359 F.3d 1066, 1070 (9th Cir. 2004). In *Theofel*, we held that a provider of e-mail services, undisputedly an ECS, stored e-mails on its servers for backup protection. *Id.* at 1075. NetGate was the plaintiffs' Internet Service Provider ("ISP"). Pursuant to a subpoena, NetGate turned over plaintiffs' e-mail messages to the defendants. We concluded that plaintiffs' e-mail messages--which were stored on NetGate's server after delivery to the recipient--were "stored 'for purposes of backup protection' . . . . within the ordinary meaning of those terms." *Id.* (citation omitted).

The service provided by NetGate is closely analogous to Arch Wireless's storage of Appellants' messages. Much like Arch Wireless, NetGate served as a conduit for the transmission of electronic communications from one user to another, [**23] and stored those communications "as a 'backup' for the user." *Id.* Although it is not clear for whom Arch Wireless "archived" the text messages--presumably for the user or Arch Wireless itself--it is clear that the messages were archived for "backup protection," just as they were in *Theofel*. Accordingly, Arch Wireless is more appropriately categorized as an ECS than an RCS.

Arch Wireless contends that our analysis in *Theofel* of the definition of "backup protection" supports its position. There, we noted that "[w]here the underlying message has expired in the normal course, any copy is no longer performing any backup function. An ISP that kept permanent copies of temporary messages could not fairly be described as 'backing up' those messages." *Id.* at 1070. Thus, the argument goes, Arch Wireless's permanent retention of the Appellants' text messages could not have been for backup purposes; instead, it must have been for storage

purposes, which would require us to classify Arch Wireless as an RCS. This reading is not persuasive. First, there is no indication in the record that Arch Wireless retained a permanent copy of the text-messages [*903] or stored them for the benefit of the City; instead, [**24] the Niekamp Declaration simply states that copies of the messages are "archived" on Arch Wireless's server. More importantly, *Theofel's* holding--that the e-mail messages stored on NetGate's server after delivery were for "backup protection," and that NetGate was undisputedly an ECS--forecloses Arch Wireless's position.

We hold that Arch Wireless provided an "electronic communication service" to the City. The parties do not dispute that Arch Wireless acted "knowingly" when it released the transcripts to the City. When Arch Wireless knowingly turned over the text-messaging transcripts to the City, which was a "subscriber," not "an addressee or intended recipient of such communication," it violated the SCA, 18 U.S.C. § 2702(a)(1). Accordingly, judgment in Appellants' favor on their claims against Arch Wireless is appropriate as a matter of law, and we remand to the district court for proceedings consistent with this holding.

B. Fourth Amendment

Appellants assert that they are entitled to summary judgment on their Fourth Amendment claim against the City, the Department, and Scharf, and on their California constitutional privacy claim against the City, the Department, Scharf, and Glenn. Specifically, [**25] Appellants agree with the district court's conclusion that they had a reasonable expectation of privacy in the text messages. However, they argue that the issue regarding Chief Scharf's intent in authorizing the search never should have gone to trial because the search was unreasonable as a matter of law. We agree.

"The 'privacy' protected by [Article I, Section 1 of the California Constitution] is no broader in the area of search and seizure than the 'privacy' protected by the Fourth Amendment . . . ." *Hill v. Nat'l Collegiate Ath. Ass'n*, 7 Cal. 4th 1, 30 n.9, 26 Cal. Rptr. 2d 834, 865 P.2d 633 (1994). Accordingly, our analysis proceeds under the Fourth Amendment to the United States Constitution. The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. "[T]he touchstone of the Fourth Amendment is reasonableness." *United States v. Kriesel*, 508 F.3d 941, 947 (9th Cir. 2007) (citing *Samson v. California*, 547 U.S. 843, 126 S. Ct. 2193, 2201 n.4, 165 L. Ed. 2d 250 (2006)). Under the "general Fourth Amendment approach," we examine "the totality of the circumstances to determine whether a search is reasonable." *Id.* "The reasonableness [**26] of a search is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *United States v. Knights*, 534 U.S. 112, 118-19, 122 S. Ct. 587, 151 L. Ed. 2d 497 (2001) (internal quotation marks omitted).

"Searches and seizures by government employers or supervisors of the private property of their employees . . . are subject to the restraints of the Fourth Amendment." *O'Connor*, 480 U.S. at 715. In *O'Connor*, the Supreme Court reasoned that "[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer." *Id.* at 717. However, the Court also noted that "[t]he operational realities of the workplace . . . may make *some* employees' expectations of privacy unreasonable." *Id.* For example, "[p]ublic employees' expectations of privacy in their offices, desks, and file cabinets . . . may be reduced [*904] by virtue of actual office practices and procedures, or by legitimate regulation." *Id.* The Court recognized that, "[g]iven the great variety of work environments in the public sector, the question whether an employee has a reasonable [**27] expectation of privacy must be addressed on a case-by-case basis." *Id.* at 718.

Even assuming an employee has a reasonable expectation of privacy in the item seized or the area searched, he must also demonstrate that the search was unreasonable to prove a Fourth Amendment violation: "public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances." *Id.* at 725-26. Under this standard, we must evaluate whether the search was "justified at its inception," and whether it "was reasonably

related in scope to the circumstances which justified the interference in the first place." *Id.* at 726 (internal quotation marks omitted).

1. Reasonable Expectation of Privacy

The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question. The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little [**28] explored. Here, we must first answer the threshold question: Do users of text messaging services such as those provided by Arch Wireless have a reasonable expectation of privacy in their text messages stored on the service provider's network? We hold that they do.

In *Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967), the government placed an electronic listening device on a public telephone booth, which allowed the government to listen to the telephone user's conversation. *Id.* at 348. The Supreme Court held that listening to the conversation through the electronic device violated the user's reasonable expectation of privacy. *Id.* at 353. In so holding, the Court reasoned, "One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." *Id.* at 352. Therefore, "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably [**29] relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." *Id.* at 353.

On the other hand, the Court has also held that the government's use of a pen register--a device that records the phone numbers one dials--does not violate the Fourth Amendment. This is because people "realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Smith v. Maryland*, 442 U.S. 735, 742, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979). The Court distinguished *Katz* by noting that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications." *Id.* at 741.

[*905] This distinction also applies to written communications, such as letters. It is well-settled that, "since 1878, . . . the Fourth Amendment's protection against 'unreasonable searches and seizures' protects a citizen against the warrantless opening of sealed letters and packages addressed to him in order to examine the contents." *United States v. Choate*, 576 F.2d 165, 174 (9th Cir. 1978) (citing *Ex parte Jackson*, 96 U.S. 727, 24 L. Ed. 877 (1877)); *see also United States v. Jacobsen*, 466 U.S. 109, 114, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984) [**30] ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy."). However, as with the phone numbers they dial, individuals do not enjoy a reasonable expectation of privacy in what they write on the outside of an envelope. *See United States v. Hernandez*, 313 F.3d 1206, 1209-10 (9th Cir. 2002) ("Although a person has a legitimate interest that a mailed package will not be opened and searched en route, there can be no reasonable expectation that postal service employees will not handle the package or that they will not view its exterior" (citations omitted)).

Our Internet jurisprudence is instructive. In *United States v. Forrester*, we held that "e-mail . . . users have no expectation of privacy in the to/from addresses of their messages . . . because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Thus, we have extended the pen register and outside-of-envelope rationales to the "to/from" line of e-mails. But we have not ruled on whether [**31] persons have a reasonable expectation of privacy in the content of e-mails. Like the Supreme Court in *Smith*, in *Forrester* we explicitly noted that "e-mail to/from addresses . . . constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers." *Id.* Thus, we concluded that "[t]he privacy interests in these two forms of communication [letters and e-mails] are identical," and that, while "[t]he contents may deserve Fourth Amendment protection . . . the address and size of the package do not." *Id.* at 511.

We see no meaningful difference between the e-mails at issue in *Forrester* and the text messages at issue here. [6] Both are sent from user to user via a service provider that stores the messages on its servers. Similarly, as in *Forrester*, we also see no meaningful distinction between text messages and letters. As with letters and e-mails, it is not reasonable to expect privacy in the information used to "address" a text message, such as the dialing of a phone number to send a message. However, users do have a reasonable expectation of privacy in the content of their text messages vis-a-vis the service provider. [**32] *Cf. United States v. Finley*, 477 F.3d 250, 259 (5th Cir. 2007) (holding that defendant had a reasonable expectation of privacy in the text messages on his cell phone, and that he consequently had standing to challenge the search). That Arch Wireless may have been able to access the contents of the messages for its own purposes is irrelevant. *See United States v. Heckenkamp*, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (holding that a student did not lose his reasonable expectation of privacy in information stored on his computer, despite a university policy that it could access [*906] his computer in limited circumstances while connected to the university's network); *United States v. Ziegler*, 474 F.3d 1184, 1189-90 (9th Cir. 2007) (holding that an employee had a reasonable expectation of privacy in a computer in a locked office despite a company policy that computer usage would be monitored). For, just as in *Heckencamp*, where we found persuasive that there was "no policy allowing the university actively to monitor or audit [the student's] computer usage," 482 F.3d at 1147, Appellants did not expect that Arch Wireless would monitor their text messages, much less turn over the messages to third parties [**33] without Appellants' consent.

> 6 Because Jeff Quon's reasonable expectation of privacy hinges on the OPD's informal policy regarding his use of the OPD-issued pagers, *see infra* pages 7027-29, this conclusion affects only the rights of Trujillo, Florio, and Jerilyn Quon.

We do not endorse a monolithic view of text message users' reasonable expectation of privacy, as this is necessarily a context-sensitive inquiry. Absent an agreement to the contrary, Trujillo, Florio, and Jerilyn Quon had no reasonable expectation that Jeff Quon would maintain the private nature of their text messages, or vice versa. *See United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) ("[T]he maker of a telephone call has a reasonable expectation that police officials will not intercept and listen to the conversation; however, the conversation itself is held with the risk that one of the participants may reveal what is said to others." (citing *Hoffa v. United States*, 385 U.S. 293, 302, 87 S. Ct. 408, 17 L. Ed. 2d 374 (1966))). Had Jeff Quon voluntarily permitted the Department to review his text messages, the remaining Appellants would have no claims. Nevertheless, the OPD surreptitiously reviewed messages that all parties reasonably believed [**34] were free from third-party review. As a matter of law, Trujillo, Florio, and Jerilyn Quon had a reasonable expectation that the Department would not review their messages absent consent from either a sender or recipient of the text messages.

We now turn to Jeff Quon's reasonable expectation of privacy, which turns on the Department's policies regarding privacy in his text messages. We agree with the district court that the Department's informal policy that the text messages would not be audited if he paid the overages rendered Quon's expectation of privacy in those messages reasonable.

The Department's general "Computer Usage, Internet and E-mail Policy" stated both that the use of computers "for personal benefit is a significant violation of City of Ontario Policy" and that "[u]sers should have no expectation of privacy or confidentiality when using these resources." Quon signed this Policy and attended a meeting in which it was made clear that the Policy also applied to use of the pagers. If that were all, this case would be analogous to the cases relied upon by the Appellees. *See, e.g., Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) ("[Employer] had announced that it [**35] could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that [employee] might have had and so scotches his claim."); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1234-35 (D. Nev. 1996) (finding a diminished expectation of privacy under the Fourth Amendment where police department had issued a memorandum informing employees that messages sent on city-issued pagers would be "logged on the [department's] network" and that certain types of messages were "banned from the system," and

because any employee "with access to, and a working knowledge of, the Department's computer system" could see the messages); *see also O'Connor*, 480 U.S. at 719 (noting that expectation of privacy would not be reasonable if the employer "had established any reasonable regulation or policy discouraging employees. . . [*907] from storing personal papers and effects in their desks or file cabinets"); *Schowengerdt v. General Dynamics Corp.*, 823 F.2d 1328, 1335 (9th Cir. 1987) ("We conclude that [the employee] would enjoy a reasonable expectation of privacy in areas given over to his exclusive use, unless he was on notice from his employer that searches [**36] of the type to which he was subjected might occur from time to time for work-related purposes.").

As the district court made clear, however, such was not the "operational reality" at the Department. The district court reasoned:

> Lieutenant Duke made it clear to the staff, and to Quon in particular, that he would *not* audit their pagers so long as they agreed to pay for any overages. Given that Lieutenant Duke was the one in charge of administering the use of the city-owned pagers, his statements carry a great deal of weight. Indeed, before the events that transpired in this case the department did not audit any employee's use of the pager for the eight months the pagers had been in use.

Even more telling, Quon had exceeded the 25,000 character limit "three or four times," and had paid for the overages every time without anyone reviewing the text of the messages. This demonstrated that the OPD followed its "informal policy" and that Quon reasonably relied on it. Nevertheless, without warning, his text messages were audited by the Department. Under these circumstances, Quon had a reasonable expectation of privacy in the text messages archived on Arch Wireless's server.

Appellees argue that, [**37] because Lieutenant Duke was not a policymaker, his informal policy could not create an objectively reasonable expectation of privacy. Moreover, Lieutenant Duke's statements "were specific to his own bill-collecting practices" and were "limited to . . . an accounting audit. He did not address privacy rights." However, as the district court pointed out, "Lieutenant Duke was the one in charge of administering the use of the city-owned pagers, [and] his statements carry a great deal of weight." That Lieutenant Duke was not the official policymaker, or even the final policymaker, does not diminish the chain of command. He was in charge of the pagers, and it was reasonable for Quon to rely on the policy--formal or informal--that Lieutenant Duke established and enforced.

Appellees also point to the California Public Records Act ("CPRA") to argue that Quon had no reasonable expectation of privacy because, under that Act, "public records are open to inspection at all times . . . and every person has a right to inspect any public record." CAL GOV'T CODE § 6253. Assuming for purposes of this appeal that the text messages archived on Arch Wireless's server were public records as defined by the [**38] CPRA, [7] we are not persuaded by Appellees' argument. The CPRA does not diminish an employee's reasonable expectation of privacy. As the district court reasoned, "There is no evidence before the [c]ourt suggesting that CPRA requests to the department are so widespread or frequent as to constitute 'an open atmosphere so open to fellow employees or the public that no expectation of privacy is reasonable.' " (quoting *Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001) (internal quotation marks omitted)).

> 7 The Act defines "public records" as "any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics." CAL GOV'T CODE § 6252(e).

The Fourth Amendment utilizes a reasonableness standard. Although the fact [*908] that a hypothetical member of the public may request Quon's text messages might slightly diminish his expectation of privacy in the messages, it does not make his belief in the privacy of the text messages objectively unreasonable. *See Zaffuto v. City of Hammond*, 308 F.3d 485, 489 (5th Cir. 2002) ("[Defendant] also argues that the existence of Louisiana's public [**39] records law and a department policy that calls would be taped suggests that it would not be objectively reasonable for [plaintiff] to expect privacy in making a personal

phone call from work . . . . [The officers testified that] they understood the policy to mean that only calls coming into the communications room (where outside citizens would call) were being recorded, not calls from private offices. A reasonable juror could conclude, on this evidence, that [plaintiff] expected that his call to his wife would be private, and that that expectation was objectively reasonable."). Therefore, Appellees' CPRA argument is without merit.

2. Reasonableness of the Search

Given that Appellants had a reasonable expectation of privacy in their text messages, we now consider whether the search was reasonable. We hold that it was not.

The district court found a material dispute concerning the "actual *purpose* or *objective* Chief Scharf sought to achieve in having Lieutenant Duke perform the audit of Quon's pager." It reasoned that if Chief Scharf's purpose was to uncover misconduct, the search was unreasonable at its inception because "the officers' pagers were audited for the period when Lieutenant [**40] Duke's informal, but express policy of *not* auditing pagers unless overages went unpaid was in effect." The district court further reasoned, however, that if the purpose was to determine "the utility or efficacy of the existing monthly character limits," the search was reasonable because "the audit was done for the benefit of (not as a punishment against) the officers who had gone over the monthly character limits." Concluding that a genuine issue of material fact existed on this point, the district judge determined that this was a question for the jury. The jury found that Chief Scharf's purpose was to "determine the efficacy of the existing character limits to ensure that officers were not being required to pay for work-related expenses," rendering a verdict in favor of the City, the Department, Scharf, and Glenn.

Given that a jury has already found that Chief Scharf's purpose in auditing the text messages was to determine the efficacy of the 25,000 character limit, we must determine--keeping that purpose in mind--whether the search was nevertheless unconstitutional.

A search is reasonable "at its inception" if there are "reasonable grounds for suspecting . . . that the search is necessary [**41] for a noninvestigatory work-related purpose such as to retrieve a needed file." *O'Connor*, 480 U.S. at 726. Here, the purpose was to ensure that officers were not being required to pay for work-related expenses. This is a legitimate workrelated rationale, as the district court acknowledged.

However, the search was not reasonable in scope. As *O'Connor* makes clear, a search is reasonable in scope "when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct]." *Id.* (internal quotation marks omitted). Thus, "if less intrusive methods were feasible, or if the depth of the inquiry or extent of the seizure exceeded that necessary for the government's legitimate purposes . . . the search would be unreasonable . . . ." *Schowengerdt*, 823 F.2d at 1336. The district court determined that there were no [*909] less-intrusive means, reasoning that talking to the officers beforehand or looking only at the numbers dialed would not have allowed Chief Scharf to determine whether 25,000 characters were sufficient for work-related text messaging because that required examining the content of all the messages. Therefore, [**42] "the only way to accurately and definitively determine whether such hidden costs were being imposed by the monthly character limits that were in place was by looking at the actual text-messages used by the officers who exceeded the character limits."

We disagree. There were a host of simple ways to verify the efficacy of the 25,000 character limit (if that, indeed, was the intended purpose) without intruding on Appellants' Fourth Amendment rights. For example, the Department could have warned Quon that for the month of September he was forbidden from using his pager for personal communications, and that the contents of all of his messages would be reviewed to ensure the pager was used only for work-related purposes during that time frame. Alternatively, if the Department wanted to review past usage, it could have asked Quon to count the characters himself, or asked him to redact personal messages and grant permission to the Department to review the redacted transcript. Under this process, Quon would have an incentive to be truthful because he may have previously paid for work-related overages and presumably would want the limit increased to avoid paying for such overages in the future. [**43] These are just a few of the ways in which the Department could have

conducted a search that was reasonable in scope. Instead, the Department opted to review the contents of all the messages, work-related and personal, without the consent of Quon or the remaining Appellants. This was excessively intrusive in light of the noninvestigatory object of the search, and because Appellants had a reasonable expectation of privacy in those messages, the search violated their Fourth Amendment rights.

3. Qualified Immunity for Chief Scharf

Chief Scharf asserts that, even if we conclude that he violated Appellants' Fourth Amendment and California constitutional privacy rights, he is entitled to qualified immunity. We agree.

When determining whether qualified immunity applies, we engage in the following two-step inquiry. First, we ask, "[t]aken in the light most favorable to the party asserting the injury, do the facts alleged show the officer's conduct violated a constitutional right?" *Saucier v. Katz*, 533 U.S. 194, 201, 121 S. Ct. 2151, 150 L. Ed. 2d 272 (2001). If we answer this question in the affirmative, as we do here, we then proceed to determine "whether the right was clearly established." *Id.* "This inquiry . . . must be undertaken [**44] in light of the specific context of the case, not as a broad general proposition." *Id.* Specifically, "[t]he relevant, dispositive inquiry in determining whether a right is clearly established is whether it would be clear to a reasonable officer that his conduct was unlawful in the situation he confronted." *Id.* at 202.

Chief Scharf argues that, "[i]n 2002, there was no clearly established law from the Supreme Court or our Circuit governing the right of a government employer to review text messages on government-issued pagers in order to determine whether employees are engaging in excessive personal use of the pagers while on duty." Chief Scharf misconstrues *Saucier*. While there may be no case with a holding that aligns perfectly with the factual scenario presented here, it was clear at the time of [*910] the search that an employee is free from unreasonable search and seizure in the workplace. *See, e.g., O'Connor*, 480 U.S. at 715 (1987); *Schowengerdt*, 823 F.2d at 1335 (1987); *Ortega v. O'Connor*, 146 F.3d 1149, 1157 (9th Cir. 1998) ("[I]t was clearly established in 1981 that, in the absence of an accepted practice or regulation to the contrary, government employees . . . had a reasonable expectation [**45] of privacy in their private offices, desks, and file cabinets, thereby triggering the protections of the Fourth Amendment with regard to searches and seizures.").

Nevertheless, we ultimately agree with Chief Scharf because, at the time of the search, there was no clearly established law regarding whether users of text-messages that are archived, however temporarily, by the service provider have a reasonable expectation of privacy in those messages. Therefore, Chief Scharf is entitled to qualified immunity.

4. Statutory Immunity on the California Constitutional Claim

The City and the Department contend that they are shielded from liability on the California constitutional claim. We conclude that the district court correctly determined that the City and the Department are not protected by statutory immunity.

California Government Code section 821.6 provides that "[a] public employee is not liable for injury caused by his instituting or prosecuting any judicial or administrative proceeding within the scope of his employment, even if he acts maliciously and without probable cause." "The policy behind section 821.6 is to encourage fearless performance of official duties. State officers and [**46] employees are encouraged to investigate and prosecute matters within their purview without fear of reprisal from the person or entity harmed thereby." *Shoemaker v. Myers*, 2 Cal. App. 4th 1407, 1424, 4 Cal. Rptr. 2d 203 (1992) (citations omitted). Immunity "also extends to actions taken in preparation for formal proceedings. Because investigation is an essential step toward the institution of formal proceedings, it is also cloaked with immunity." *Amylou R. v. County of Riverside*, 28 Cal. App. 4th 1205, 1209-10, 34 Cal. Rptr. 2d 319 (1994) (internal quotation marks omitted).

Although Chief Scharf ordered an "investigation" in the ordinary sense of the word, the investigation never could have led to a "judicial or administrative proceeding" because Lieutenant Duke's informal policy permitted officers to use the pagers for personal purposes and to exceed the 25,000 character limit. Thus, Quon could have committed no misconduct, a prerequisite for a formal proceeding against him. As such, the City's and Department's conduct does not fall within California Government Code section 821.6, and

they are not entitled to statutory immunity.

V. CONCLUSION

As a matter of law, Arch Wireless is an "electronic communication service" that provided [**47] text messaging service via pagers to the Ontario Police Department. The search of Appellants' text messages violated their Fourth Amendment and California constitutional privacy rights because they had a reasonable expectation of privacy in the content of the text messages, and the search was unreasonable in scope. While Chief Scharf is shielded by qualified immunity, the City and the Department are not shielded by statutory immunity. In light of our conclusions of law, we affirm in part, reverse in part, and remand to the district court for further proceedings on Appellants' Stored Communications Act claim against Arch Wireless, and their claims against the City, the Department, [*911] and Glenn under the Fourth Amendment and California Constitution.

Because we hold that Appellants prevail as a matter of law on their claims against Arch Wireless, the City, the Department, and Glenn, we need not reach their appeal from the denial of their motions to alter or amend the judgment and for a new trial under Federal Rule of Civil Procedure 59. The parties shall bear their own costs of appeal.

AFFIRMED in part, REVERSED in part, and REMANDED for Further Proceedings.

DEPUBLISHED
AWAITING REVIEW

ABIGAIL HERNANDEZ et al., Plaintiffs and Appellants, v. HILLSIDES, INC., et al., Defendants and Respondents.

142 Cal. App. 4th 1377; 48 Cal. Rptr. 3d 780
September 14, 2006, Filed

NOTICE:

NOT CITABLE--SUPERSEDED BY GRANT OF REVIEW

DISPOSITION: Judgment is reversed and remanded with directions.

SUMMARY:

CALIFORNIA OFFICIAL REPORTS SUMMARY

The trial court granted summary judgment to employers on causes of action brought by employees for invasion of privacy, intentional infliction of emotional distress, and negligent infliction of emotional distress. The employers, suspecting that someone had been accessing pornographic Web sites at night from some of the office computers, placed a motion-activated video surveillance system in the employees' office without informing the employees. (Superior Court of Los Angeles County, No. GC032633, C. Edward Simpson, Judge.)

The Court of Appeal reversed and remanded with directions to vacate the order granting the motion for summary judgment, to enter a new and different order denying the motion for summary judgment and granting summary adjudication of the causes of action for intentional infliction of emotional distress and negligent infliction of emotional distress, and to conduct further proceedings. The court held that the tort of invasion of privacy based on an intrusion did not require proof that private information had been disclosed to a third party. Intrusion occurred when privacy was invaded in an offensive manner without consent, not when information gained from the intrusion was disclosed. Thus, the mere placement of the surveillance equipment in the office was sufficient to invade the employees' privacy. Moreover, the employers did not establish that the employees did not have a reasonable expectation of privacy in their office. Factual issues remained as to the offensiveness of the employers' conduct and the reasonableness of their claim that the surveillance was justified. The employers were entitled to judgment on the claim for intentional infliction of emotional distress because their conduct was not extreme and outrageous, as well as on the claim for negligent infliction of emotional distress because no breach of duty was alleged. (Opinion by Croskey, Acting P. J., with Kitching and Aldrich, JJ., concurring.) [*1378]

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

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

JUDGES: Croskey, Acting P. J., with Kitching and Aldrich, JJ., concurring.

OPINION BY: CROSKEY

OPINION

[**782] **CROSKEY, Acting P. J.**--Abigail Hernandez and Maria Jose-Lopez (plaintiffs) appeal from the trial court's grant of summary judgment in favor of Hillsides, Inc., Hillsides Children's Center, Inc., and John M. Hitchcock (defendants). Plaintiffs had sued for damages after they had discovered that their employer, a residential facility for abused children, had placed a video camera in the office which they shared. The trial court held that plaintiffs could not prevail on their causes of action for invasion of privacy, intentional infliction of emotional distress, and negligent infliction of emotional distress because plaintiffs: (1) were not recorded or viewed by the surveillance equipment defendants placed in their office; and (2) had a diminished expectation of privacy [***2] that was overcome by defendants' need to protect the children residing at their facility.

We hold that a plaintiff need not establish that he or she was actually viewed or recorded in order to succeed on a cause of action for invasion of privacy. Additionally, defendants failed to conclusively establish that plaintiffs

had a diminished expectation of privacy, or that their actions were sufficiently justified by the need to protect the children residing at their [*1381] facility. We therefore reverse. Plaintiffs, however, cannot state a cause of action for intentional infliction of emotional distress, and their cause of action for negligent infliction of emotional distress is legally insufficient and factually superfluous, so summary adjudication should be granted in favor of defendants on those two causes of action.

FACTS AND PROCEDURAL BACKGROUND[1]

1 The facts we recite are set forth in the papers filed by the parties in support of and in opposition to defendants' motion for summary judgment.

Defendants [***3] run a residential facility for approximately 66 abused and neglected children between the ages of six and 18. Defendant John Hitchcock (Hitchcock) is the director of the facility. Plaintiffs were employed in clerical positions in the office building on defendants' campus. [**783] They shared an office with a locking door and a window with shades that could be drawn for privacy. [2] The door to plaintiffs' office contained a "doggie door" which was missing the swinging flap. On several occasions plaintiff Hernandez used her office to change clothes before leaving for the gym. Plaintiff Jose-Lopez occasionally used the office to show Hernandez how her figure was recovering after recently giving birth by raising her shirt to expose her breasts and stomach. Defendants had no knowledge that plaintiffs were using the office for such purposes, but such facts would support a conclusion that plaintiffs had an expectation of privacy while in their office.

2 Plaintiffs assert the shades are always drawn, but what is important for the purposes of this opinion is that plaintiffs' office can be sufficiently concealed from view.

[***4] 1. *Defendants Install Motion-activated Camera in Plaintiffs' Office*

Around July 2002, defendants' computer technician, Tom Foster, informed defendants that he believed someone was accessing pornographic Web sites at night from some of defendants' computers, including the one in plaintiffs' office. Defendants and various department heads and administrative staff members decided to conduct surveillance in areas where the illicit computer access had taken place. [3] Plaintiffs were not advised of this decision because they were considered to be part of a group of employees that "gossiped" and might inadvertently tip off the unknown person(s) defendants were trying to catch.

3 Defendants had purchased the surveillance equipment in February 2002 for the purpose of preventing thefts in the administration building.

Hitchcock installed a motion-activated video surveillance system in the computer lab where some of the illicit Web access had occurred. The surveillance system was moved to plaintiffs' shared office [***5] in October 2002. The camera and motion detector were placed on a shelf in plaintiffs' office [*1382] and set up to broadcast images to a TV monitor and video recorder located in a storage room across the hall. Only four people were aware that the surveillance equipment had been placed in plaintiffs' office. Plaintiffs were not among those who had such knowledge.

In his deposition, Hitchcock stated that the surveillance camera and motion detector operated "all the time," but that the system had only been "active" three times. The first time, Hitchcock had placed the camera and motion detector in plaintiffs' office after they had left for the day and removed it before they arrived the next morning. Thereafter, Hitchcock had left the camera and motion detector functioning in plaintiffs' office but only twice had "connected" the wireless receptor to the TV monitor and recorder in the storage room. His practice was to connect the receptor before leaving at night and, in order to prevent the camera from transmitting to the TV monitor during the day, disconnect it before plaintiffs arrived for work the following morning. Defendants did not provide any evidence, however, regarding which three dates [***6] the surveillance system had been activated.

At approximately 4:30 in the afternoon on Friday, October 25, 2002, plaintiffs noticed a red light on a shelf in their office blinking when there was movement in front of it. They looked more closely and discovered a camera. They followed the cord attached to the camera and discovered that it was plugged in and that the plug was hot to the touch. Plaintiffs notified their supervisor, who called Hitchcock at his home to report the discovery. Hitchcock, who had not been to the facility that [**784] day, called Hernandez in her office to explain the surveillance and assure her that the camera had not been installed to observe plaintiffs.

Plaintiffs were extremely upset by their discovery

and did not return to work until Wednesday, October 30, 2005. When they returned, plaintiffs asked to view the surveillance tape. Plaintiffs were shown a tape containing scenes of their empty office, Hitchcock adjusting the camera, and about five minutes of static. In his deposition, Hitchcock stated that he had been planning to remove the camera the very weekend plaintiffs found it, because there had been no pornographic Web sites accessed from the computer in plaintiffs' [***7] office in the three-week period during which he had been periodically "recording" their office.

2. *Subsequent Lawsuit and Motion for Summary Judgment*

On September 12, 2003, plaintiffs filed suit against defendants for invasion of privacy, intentional infliction of emotional distress, and negligent infliction of emotional distress arising from their discovery of the surveillance equipment in their office. Defendants filed a motion for summary judgment on December 15, 2004, and raised three principal contentions.

[*1383] a. *Publication*

Defendants first argued that plaintiffs' cause of action for invasion of privacy must fail because plaintiffs had not been recorded or viewed by the camera installed in their office, and thus, as a matter of law, plaintiffs' privacy could not have been invaded. [4] Defendants asserted that the camera was only "active" three times, and only in the evening hours. Defendants relied on the videotape shown to plaintiffs and Hitchcock's deposition as proof plaintiffs were never viewed or recorded by the surveillance system. Defendants, however, did not provide declarations or depositions from any of the department heads involved in the decision to [***8] conduct video surveillance of plaintiffs' office or from any of the persons who had access to the storage room and who could have activated the surveillance system while plaintiffs were in their office.

> 4 Similarly, defendants argued that because plaintiffs were never viewed or recorded by the surveillance equipment placed in their office, defendants' conduct was not sufficiently outrageous to support a cause of action for intentional infliction of emotional distress.

In response, plaintiffs argued that Hitchcock's deposition stated that the camera was always on and the videotape showed an empty room, indicating that there did not need to be motion to activate the video recorder. Plaintiffs argued Hitchcock's statements that the camera was always on, but that they had never been recorded or viewed, were contradictory. [5] Additionally, plaintiffs noted that Hitchcock was not at Hillsides on the day plaintiffs found the camera, so he could not [**785] have "deactivated" it that morning, and that defendants did not provide [***9] the specific dates on which the surveillance system was "active."

> 5 Plaintiffs misunderstand Hitchcock's deposition testimony, which is not inconsistent with regard to the operation of the camera and the recording equipment. Hitchcock has consistently testified that the camera is "on" when it is plugged in, but would only transmit images for recording and/or viewing on the TV monitor if the "receptors" in the storage room were connected to the TV monitor and recorder. Hitchcock's testimony was that, in order to prevent the camera from transmitting or recording during the day, he would "disconnect" the camera receptors from the TV monitor and recorder in the storage room. Thus, the camera was technically "on" because it was plugged in to the wall in plaintiffs' office, but if the receptors were disconnected, as Hitchcock testified, there would be no way for any image of plaintiffs' office to appear on the TV monitor.

b. *Expectation of Privacy*

Defendants next argued that even if plaintiffs had been viewed [***10] or recorded, they had a diminished expectation of privacy in their jointly occupied office. Defendants argued plaintiffs could not have reasonably expected privacy in their office because: (1) a person could climb over a railing outside plaintiffs' window and peek in; (2) the "doggie door" allowed anyone to bend down and [*1384] see in the office; and (3) at least 11 people had keys to their office. Defendants also argued that four surveillance cameras throughout the campus and plaintiffs' signatures on computer monitoring policies indicated that they knew they could be "monitored" at any time while on the campus.

Plaintiffs countered that the windows in their office were always closed, and anyone with a need to come into the office while it was occupied would knock on the door for admittance, not lean down and peek in. Regardless of windows and doggie doors, plaintiffs argued, employees

may have a reasonably objective expectation of privacy even when their workspace is an open cubicle in a room with dozens of other employees, making it all the more reasonable that an employee in an office with a lockable door would expect to enjoy privacy when the door was closed. Finally, plaintiffs [***11] noted that any policy regarding computer monitoring involved monitoring the computer system itself, not the office in which the computer was being used.

c. *Justification of Surveillance*

Lastly, defendants argued that even if plaintiffs possessed a minimal expectation of privacy, it was overcome by defendants' need to catch the person believed to be accessing pornographic Web sites at night, in order to protect the children on the campus from potential abuse or exposure to that activity.

Plaintiffs responded that while defendants asserted the surveillance was in response to "pornographic" Web sites that had been accessed from facility computers, they failed to provide the titles of the Web sites, did not describe what sort of Web sites were "pornographic," and had not provided the Web logs that justified their decision to conduct a surveillance of plaintiffs' office. Plaintiffs further pointed out that defendants were aware of the "illicit" Web access for three months before taking any action to conduct surveillance in plaintiffs' office. Finally, plaintiffs argued that there were less intrusive means for determining the culprit than placing a secret surveillance camera in their [***12] office.

3. *Resolution of Motion and Appeal*

On March 1, 2006, the trial court granted the motion for summary judgment. Judgment was entered in favor of defendants. Plaintiffs filed a timely notice of appeal.

ISSUES ON APPEAL

The arguments made by the parties present four issues: (1) is publication a necessary element of plaintiffs' cause of action for invasion of privacy and, if [*1385] so, did defendants defeat it? (2) were plaintiffs' expectations of privacy reasonable? (3) did defendants conclusively establish that the surveillance was, under the circumstances, justified? and (4) did defendants defeat plaintiffs' causes of action for the infliction of emotional distress?

DISCUSSION

1. *Standard of Review*

" 'A defendant is entitled to summary judgment if the record establishes as a [**786] matter of law that none of the plaintiff's asserted causes of action can prevail.' (*Molko v. Holy Spirit Assn.* (1988) 46 Cal.3d 1092, 1107 [252 Cal. Rptr. 122].) The pleadings define the issues to be considered on a motion for summary judgment. (*Sadlier v. Superior Court* (1986) 184 Cal. App. 3d 1050, 1055 [29 Cal. Rptr. 374].) As [***13] to each claim as framed by the complaint, the defendant must present facts to negate an essential element or to establish a defense. Only then will the burden shift to the plaintiff to demonstrate the existence of a triable, material issue of fact. (*AARTS Productions, Inc. v. Crocker National Bank* (1986) 179 Cal. App. 3d 1061, 1064-1065 [225 Cal. Rptr. 203].)" (*Ferrari v. Grand Canyon Dories* (1995) 32 Cal.App.4th 248, 252 [38 Cal. Rptr. 2d 65].) "There is a triable issue of material fact if, and only if, the evidence would allow a reasonable trier of fact to find the underlying fact in favor of the party opposing the motion in accordance with the applicable standard of proof." (*Aguilar v. Atlantic Richfield Co.* (2001) 25 Cal.4th 826, 850 [107 Cal. Rptr. 2d 841, 24 P.3d 493].) We review orders granting or denying a summary judgment motion de novo. (*FSR Brokerage, Inc. v. Superior Court* (1995) 35 Cal.App.4th 69, 72 [41 Cal. Rptr. 2d 404].) We exercise "an independent assessment of the correctness of the trial court's ruling, applying the same legal standard as the trial court in determining whether there are any genuine issues of material fact or whether the moving party is entitled to judgment as [***14] a matter of law." (*Iverson v. Muroc Unified School Dist.* (1995) 32 Cal.App.4th 218, 222 [38 Cal. Rptr. 2d 35].)

2. *Invasion of Privacy Principles*

(1) In 1960, Prosser identified four basic privacy interests: (1) intrusion upon seclusion or solitude, or private affairs; (2) public disclosure of embarrassing private facts; (3) publicity which places the plaintiff in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness. (*Miller v. National Broadcasting Co., Inc.* (1986) 187 Cal. App. 3d 1463, 1482 [232 Cal. Rptr. 668].) The case before us involves the right to be secure from intrusion.

[*1386] **(2)** California courts have adopted Prosser's analysis and the Restatement formulation of intrusion: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or

his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." (Rest.2d Torts, § 652B; see also *Miller v. National Broadcasting Co., Inc., supra,* 187 Cal. App. 3d at p. 1482.) Intrusion into private places, [***15] conversations, and matters is the privacy tort that best captures the common understanding of an "invasion of privacy" and "is most clearly seen as an affront to individual dignity." (*Shulman v. Group W Productions, Inc.* (1998) 18 Cal.4th 200, 231 [74 Cal. Rptr. 2d 843, 955 P.2d 469] (*Shulman*).) The *Shulman* court noted that intrusion cases are inherently fact specific and, as a result, there are no bright line rules identifying the outer boundaries of intrusion. (*Id.* at p. 237.)

Thus, as applicable to the case before us, the tort of invasion of privacy, or intrusion, has two main elements: (1) intrusion into a private place, conversation, or matter; and (2) in a manner highly offensive to a reasonable person. (*Shulman, supra,* 18 Cal.4th at p. 231.) Tortious intrusion includes unconsented-to physical intrusion into private places, as well as "unwarranted sensory intrusions such as eavesdropping, wiretapping, and visual or photographic spying." (*Shulman, supra,* [**787] 18 Cal.4th at pp. 230-231, citing Rest.2d Torts, § 652B, com. b & illus., pp. 378-379; see also *Wilkins v. National Broadcasting Co.* (1999) 71 Cal.App.4th 1066, 1075 [84 Cal. Rptr. 2d 329].) [***16]

3. *Publication Is Not an Element of Invasion of Privacy*

Defendants argue that plaintiffs could not raise a triable issue of fact as to whether they were recorded or viewed by the equipment defendants placed in their office because the videotape plaintiffs were shown included only footage of their empty office and Hitchcock. Whether plaintiffs were viewed or recorded, however, Hitchcock admittedly had entered plaintiffs' office and secretly placed a functioning camera which was capable of transmitting images from plaintiffs' office to a remote location where such images could be viewed or recorded at will by the activation of a remote receiver.

(3) The tort of invasion of privacy based on an intrusion does not require plaintiffs to prove that private information about them has been disclosed to a third party. (*Miller v. National Broadcasting Co., Inc., supra,* 187 Cal.App.3d at p. 1484.) A plaintiff is harmed when his or her privacy is invaded in an offensive manner without consent, not when information gained from the intrusion is disclosed or published. The Restatement Second of Torts explains: "[I]nvasion of privacy covered by this Section [intrusion] ... consists [*1387] solely of an intentional [***17] interference with [plaintiff's] interest in solitude or seclusion, either as to his [or her] person or as to his [or her] private affairs or concerns, of a kind that would be highly offensive to a reasonable [person]." (Rest.2d Torts, § 652B, com. a, p. 378.) The Restatement continues: "The invasion ... may be by some other form of investigation or examination into [plaintiff's] private concerns ... . The *intrusion itself* makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined." (*Id.,* com. b, pp. 378-379, italics added.) Thus, if unconsented-to disclosure, publication, or viewing of information about the plaintiff is harmful, then the action taken to obtain that private information must itself also be harmful.

Intrusion involves a plaintiff's peace of mind and right to be left alone. The focus is on whether the defendants penetrated "some zone of physical or sensory privacy surrounding, *or obtained unwanted access* to data about, the plaintiff," not whether the data was ever obtained or disclosed. (*Shulman, supra,* 18 Cal 4th at p. 232 [***18] , italics added; see also *Huntingdon Life Sciences, Inc. v. Stop Huntingdon Animal Cruelty USA, Inc.* (2005) 129 Cal.App.4th 1228, 1259 [29 Cal. Rptr. 3d 521].) Under *Shulman* and section 652B of the Restatement Second of Torts, gaining *access* to information about the plaintiffs that they reasonably believed would remain private is an intrusion into their seclusion. [6] The extent to which images [**788] of the plaintiffs were "captured" or "observed" by the defendants or third parties as a result of the defendants' intrusion may have an impact on the amount of damages the plaintiffs may recover, but it does not impact the defendants' liability for the intrusion.

> 6 Judicial Council of California Civil Jury Instructions (2004-2005) CACI No. 1800 also reflects this interpretation of intrusion. Notably, this approved jury instruction does *not* require that the jury find the plaintiffs were captured or observed by the intrusion, merely that the intrusion occurred:
>
> To establish a claim of intrusion *plaintiffs* must prove all of the following:
>
> "1. That [plaintiffs] had a reasonable expectation of privacy in [*insert facts regarding the place, conversation, or other circumstance*];

"2. That [defendants] intentionally intruded in [*insert facts regarding the place, conversation, or other circumstance*];

"3. That [defendants'] intrusion would be highly offensive to a reasonable person;

"4. That [plaintiffs] were harmed; and

"5. That [defendants'] conduct was a substantial factor in causing [plaintiffs'] harm."

[***19] The Legislature, in providing a statutory remedy for the offensive conduct of the so-called "paparazzi" or other persons engaged in similar invasive conduct, has recognized and relied upon this same analysis. Civil Code section 1708.8, subdivision (b), imposes liability for a "constructive invasion of privacy." That subdivision subjects a person to liability when that person "attempts to capture, in a manner that is offensive to a reasonable person, any [*1388] type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal ... 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." While this statute by its terms does not apply to the circumstances of this case, we note that subdivision (j) of section 1708.8 expressly states, "[i]t is not a defense to a violation of this section that no image, recording, or [***20] physical impression was captured ... ." [7] Thus, it is the *intrusion* into plaintiffs' seclusion itself that is the actionable wrong.

7 Similarly, Penal Code section 632, which prohibits recording confidential communications, is violated the moment the recording is made without consent, regardless of whether it is subsequently disclosed. (*Marich v. MGM/UA Telecommunications, Inc.* (2003) 113 Cal.App.4th 415, 425 [7 Cal. Rptr. 3d 60].)

Several courts in other jurisdictions have considered whether an intrusion *alone* is actionable, and have reached the same result. In a Michigan Appellate Court case, the plaintiff and her daughter sued the owner of a roller skating rink, after the two had used the ladies' room in the rink and discovered "that the defendant had installed see-through panels in the ceiling of the restroom which permitted surreptitious observation from above the interior, including the separately partitioned stalls." (*Harkey v. Abate* (1984) 131 Mich.Ct.App. 177 [346 N.W.2d 74, 75].) [***21] The court held, over a dissent, that the plaintiff could recover despite having no proof that she and her daughter were viewed. "The type of invasion of privacy asserted by plaintiff does not depend upon any publicity given to the person whose interest is invaded, but consists solely of an intentional interference with his or her interest in solitude or seclusion of a kind that would be highly offensive to a reasonable person. [Citation.] Clearly, plaintiff and her daughter in this case had a right to privacy in the public restroom in question. *In our opinion, the installation of the hidden viewing devices alone constitutes an interference with that privacy which a reasonable person would find highly offensive*. And though the absence of proof that the devices were utilized is relevant to the question of damages, it is not fatal to plaintiff's case." (*Id*. at p. 76, italics added.)

In *Carter v. Innisfree Hotel, Inc.* (Ala. 1995) 661 So. 2d 1174, the plaintiff husband and wife discovered that a mirror in their hotel room had been scratched on the back in order to enable someone to view their room from an [*1389] adjacent room. While it was a disputed issue of fact [***22] as to whether someone had *actually* viewed the plaintiffs in their hotel room, the Alabama Supreme Court concluded that proof that the plaintiffs had been viewed was not a prerequisite [**789] for recovery. "There can be no doubt that the possible intrusion of foreign eyes into the private seclusion of a customer's hotel room is an invasion of that customer's privacy." (*Id*. at p. 1179.) [8]

8 In *New Summit Associates v. Nistle* (1987) 73 Md.Ct.Spec.App. 351 [533 A.2d 1350], plaintiff found scratches on the back of the bathroom mirror in her apartment, which allowed her bathroom to be viewed by someone in the neighboring vacant apartment, which was undergoing renovations. The court concluded the plaintiff "was not required to prove that a *particular* individual *actually observed* her while she used the facilities in her bathroom. The intentional act that exposed that private place intruded upon [plaintiff's] seclusion." (*Id*. at p. 1354.) However, the court held that the plaintiff could not recover from the landlord and management company defendants, as there was no proof either of them (or their agents) had

committed the intrusion. (*Ibid.*)

[***23] Finally, in *Hamberger v. Eastman* (1964) 106 N.H. 107 [206 A.2d 239], the plaintiffs rented a house adjacent to the house of their landlord. They discovered the defendant had installed in their bedroom a listening and recording device, which was connected by wires to the defendant's house. The defendant argued there could be no cause of action as the plaintiffs did not allege that anyone listened to any sounds from their bedroom. The New Hampshire Supreme Court disagreed, holding that "actual or potential" publicity with respect to private matters constitutes a compensable injury. (*Id*. at p. 242.)

(4) Thus, we conclude that the mere placement of the surveillance equipment on the shelf in plaintiffs' office itself invaded their privacy because it allowed defendants, or anyone with access to the storage room, to "activate" the surveillance system at any time during the day without plaintiffs' knowledge, thus at least presenting the possibility of unwanted access to private data about plaintiffs. (*Shulman, supra,* 18 Cal.4th at p. 232.) Plaintiffs need not show more in order to establish their cause of action. [9]

> 9 In any event, even if publication were an element of the intrusion cause of action, defendants failed to defeat it. Defendants offer only Hitchcock's deposition testimony as evidence that plaintiffs were never viewed, despite the fact that Hitchcock himself stated that three other people knew where the surveillance system was located, where it was broadcasting, and were able to access the locked storage room. Moreover, while defendants argue that the system was only set up to record three times, they offer no dates or estimates as to when those incidents occurred. Hitchcock stated that he would activate the system at night and deactivate it in the morning, yet he was not at Hillsides on the day that the system was found and thus could not have deactivated it that morning. Therefore, even if publication or "viewing" were an element of invasion of privacy, there would remain a triable issue of fact as to what dates and what times of the day the surveillance system was recording and/or broadcasting and whether or not anyone besides Hitchcock had used the storage room during the three weeks he had used it as the "control room" for the surveillance.

[*1390] [***24] 4. *Defendants Did Not Establish that Plaintiffs Did Not Have a Reasonable Expectation of Privacy in Their Office*

(5) As a matter of law, a claim of intrusion cannot fail merely because the events or conversations which the defendant intruded upon were not completely private from all other eyes and ears. (*Sanders v. American Broadcasting Companies* (1999) 20 Cal.4th 907, 911 [85 Cal. Rptr. 2d 909, 978 P.2d 67].) Privacy is not a binary, all-or-nothing characteristic; it has degrees and nuances. (*Id.* at p. 916.) An expectation of privacy in a given setting is not unreasonable just because the privacy expected is not complete or absolute. (*Ibid*.) "[I]n the workplace, as elsewhere, the reasonableness of a person's expectation of [**790] visual and aural privacy depends not only on who might have been able to observe the subject interaction, but on the identity of the claimed intruder and the means of intrusion." (*Id.* at p. 923.)

While plaintiffs did not enjoy complete and absolute privacy in their office, it was reasonable for them to expect images of them in their office with the door closed would not be transmitted to another portion of the building. Hitchcock was [***25] not leaning down and peeking through the doggie door or peering through the window in the office, but he was, in effect, secretly hidden in the office with plaintiffs via the installed surveillance equipment which had the ability to transmit plaintiffs' images onto the monitor in the storage closet across the hall. The fact that plaintiffs were employees and that a passerby in the hallway could have attempted to look in the office via the doggie door does not, as a matter of law, deny them protection against the unwanted intrusion represented by defendants' secret installation of a hidden camera.

5. *Factual Issues Remain As To the "Offensiveness" of Defendants' Conduct and Their Claimed Justification*

a. *The "Offensiveness" Issue*

(6) If a defendant has intruded on a plaintiff's objectively reasonable privacy, the plaintiff must next establish the intrusion was "highly offensive" in order to recover. Offensiveness inquires as to " 'the degree of intrusion, the context, the conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.' " (*Wilkins v. National Broadcasting Co., supra,* 71

Cal.App.4th at pp. 1075-1076, [***26] quoting *Miller v. National Broadcasting Co., Inc., supra,* 187 Cal. App. 3d at pp. 1483-1484.) Whether or not something is offensive also depends on the particular method [*1391] of intrusion used. (*Shulman, supra,* 18 Cal.4th at pp. 236-237.) Difficult cases involve photographic and electronic recording equipment because of the potential for use in ways that severely threaten personal privacy. (*Shulman, supra,* at p. 237.) There is no bright line rule on this question, and every case must be determined on its facts. (*Ibid.*)

A reasonable jury could conclude that the intrusion into plaintiffs' office in this case is highly offensive. Defendants placed a motion-activated camera in a private office shared by plaintiffs, and left it functioning for *no legitimate reason* while plaintiffs were present. Nor did defendants alert plaintiffs to the presence of the camera, so they could modify their behavior to protect their own privacy. Under these circumstances, defendants have not established as a matter of law that their conduct was not highly offensive. Thus, a triable issue of fact exists which must be resolved upon remand.

b. *The Justification* [***27] *Issue*

Defendants argue that their surveillance was necessary and justified to catch whoever was accessing illicit pornographic Web sites in the early hours of the morning, in violation of Hillsides' computer usage policies. The only evidence, however, offered by defendants to show their need to engage in this surveillance is the declaration of Tom Foster, the computer technician, and the deposition of Hitchcock. While Foster stated that in July 2002 the Web logs he maintained for Hillsides in their mainframe computer indicated [**791] that illicit pornographic Web sites had been accessed, he offered no description of the type of sites accessed, how frequently, or their Web addresses. Hitchcock has consistently stated that the Web logs reflected Web sites that justified surveillance of plaintiffs' office, but has never provided the logs, the titles of the Web sites, or any description of the Web sites more elaborate than "immoral," "illicit," and "pornographic." While it is possible that these Web sites are so alarming and potentially threatening to the well-being of children at Hillsides that surveillance would be justified, defendants simply do not offer anything more than conclusory statements [***28] that they had information that the Web sites were pornographic and being accessed from a computer in plaintiffs' office. Why defendants failed to produce this presumably compelling evidence in support of their motion for summary judgment was not explained.

Even assuming, arguendo, that defendants were justified in their actions, it is undisputed that the offensive Web sites were only being accessed at night. Hitchcock admitted the camera did not need to be in the office during the hours that plaintiffs were working and that he had no suspicions as to [*1392] plaintiffs' activities. In fact, the first occasion Hitchcock used the surveillance system in plaintiffs' office, he placed the camera and motion detector in the office after hours and removed it prior to plaintiffs' arrival the next morning. Defendants offer no explanation as to why the second and third occasions required leaving the camera and motion detector in plaintiffs' office during the day for three weeks when any of the four people with knowledge of the surveillance system could have activated the system without plaintiffs' knowledge. Thus, defendants have failed to conclusively establish their surveillance was justified under [***29] the circumstances. This is another issue that must be resolved by a trier of fact.

6. *Intentional Infliction of Emotional Distress and Negligent Infliction of Emotional Distress*

(7) Invasion of a person's peace of mind is an independent wrong that, in and of itself, gives rise to liability. (*Shulman, supra,* 18 Cal.4th at p. 232.) Intentional infliction of emotional distress requires " ' " 'extreme and outrageous conduct by the defendant with the intention of causing, or reckless disregard [for] the probability of causing, emotional distress' " ' " (*Wilkins v. National Broadcasting Co., supra,* 71 Cal.App.4th at p. 1087.) The conduct must be "so extreme and outrageous 'as to exceed all bounds of that usually tolerated in a civilized society.' " (*Ibid.*) Given that the placement of the camera was not intended to spy on plaintiffs and, in fact, was only intended to be activated when they were not in the office, we find, as a matter of law, that defendants' conduct does not rise to the level of "extreme and outrageous." Thus, plaintiffs cannot prevail on their cause of action for intentional infliction of emotional distress. Summary resolution [***30] of this cause of action in favor of defendants is appropriate.

(8) As to plaintiffs' cause of action for negligent infliction of emotional distress, "[t]he negligent causing of emotional distress is not an independent tort but the tort of negligence, involving the usual duty and causation issues." (6 Witkin, Summary of Cal. Law (10th ed. 2005)

Torts, § 1004, p. 270.) Plaintiffs' complaint alleges no duty breached, but only alleges that defendants' intentional act of placing the camera in their office caused them emotional distress. Emotional distress damages may be recoverable as part of the [**792] general damages if plaintiffs prevail on their invasion of privacy cause of action. (CACI No. 1820.) As such, plaintiffs' purported cause of action for "negligent infliction of emotional distress" is both legally without merit and factually superfluous. Summary resolution of this cause of action is thus also appropriate.

[*1393] ***DISPOSITION***

The judgment is reversed. The matter is remanded with directions to vacate the order granting the motion for summary judgment and enter a new and different order denying the motion for summary judgment and granting summary adjudication [***31] of plaintiffs' causes of action for intentional infliction of emotional distress and negligent infliction of emotional distress. The trial court shall then conduct such further proceedings as are appropriate in a manner not inconsistent with the views expressed herein. Plaintiffs shall recover their costs on appeal.

Kitching, J., and Aldrich, J., concurred.

JERRY ALLEN HOLLIDAY, Plaintiff and Appellant, v. CITY OF MODESTO et al., Defendants and Respondents

Court of Appeal of California, Fifth Appellate District
229 Cal. App. 3d 528; 280 Cal. Rptr. 206;

April 18, 1991

NOTICE: [***1] Opinion certified for partial publication - Pursuant to California Rules of Court, rule 976.1, this opinion is certified for publication with the exception of parts I, III, and IV.

DISPOSITION: The judgment is reversed with directions to enter a new judgment granting Holliday's petition for writ of mandate ordering respondent Garth Lipsky, as Modesto City Manager, to set aside those portions of his determination of January 21, 1988, finding that appellant disobeyed direct orders of his superior and imposing discipline on appellant; the order shall further direct respondent Lipsky to make a new determination imposing discipline for appellant's violation of Modesto Fire Department rule FR 213(f) which is fair, just, and reasonable but is at a level less than a two-rank demotion and does not include drug-testing orders. Costs to appellant.

SUMMARY:

CALIFORNIA OFFICIAL REPORTS SUMMARY

A city fire lieutenant, who had been cited for misdemeanor possession of marijuana while he was off duty, was ordered to be demoted two ranks and was required to submit to drug testing twice a year for two and one-half years. The discipline was based on his violation of various department rules. He filed a petition for a writ of mandate seeking relief from the order (Code Civ. Proc., § 1094.5); respondents answering were the fire chief, who had made the order, the city manager, who reimposed the chief's recommended discipline despite a hearing officer's finding that it was excessive, and the city. The trial court denied the petition, finding no abuse of discretion in the discipline imposed. (Superior Court of Stanislaus County, No. 231907, Edward M. Lacy, Jr., Judge.)

The Court of Appeal reversed with directions to grant the petition for writ of mandate, ordering the city manager to set aside portions of his order finding that the petitioner had disobeyed direct orders of his superior and imposing discipline on petitioner, and directing the city manager to make a new determination imposing discipline that did not include drug testing orders and was at a level less than a two-rank demotion. The court held that drug testing was a condition of employment and thus a subject for negotiation with the union within the requirements of the Meyers-Milias-Brown Act (Gov. Code, § 3500 et seq.), which governs the rights of public agency employees to organize and negotiate with their employers. (Opinion by Thaxter, J., with Stone (W. A.), Acting P. J., and Harris, J., concurring.)

COUNSEL: Davis, Reno & Courtney, Alan C. Davis, Diane Ravnik and Cindy O'Hara-Varela for Plaintiff and Appellant.

Stan T. Yamamoto, City Attorney, Thomas J. Quinlan and Michael Milich, Deputy City Attorneys, for Defendants and Respondents.

JUDGES: Opinion by Thaxter, J., with Stone (W. A.), Acting [***2] P. J., and Harris, J., concurring.

OPINION BY: THAXTER

OPINION

[*530] [**207] May a public employer order one of its employees, on pain of suspension, demotion, or termination, to submit to drug testing without first complying with the "meet and confer" requirements of the Meyers-Milias-Brown Act (Gov. Code, [1] § 3500 et seq., hereinafter MMBA)? Under the circumstances of this case, we answer the question no.

1 All statutory references are to the Government Code unless otherwise indicated.

Summary of Facts and Procedural History

Appellant Jerry Allen Holliday concedes there is no factual dispute on appeal.

Holliday was a fire lieutenant with the City of Modesto, having been employed with the fire department for some 18 years. His past performance had been excellent.

On the evening of February 25, 1987, Holliday and fellow fire Lieutenant Bernard Ferris Cudney [2] were each cited by Modesto police officers for [*531] misdemeanor possession of marijuana (Health & Saf. Code, § 11357, subd. (b)); they had been observed smoking a marijuana cigarette [***3] in the parking lot of a bar. Cudney had supplied the marijuana. Neither Holliday nor Cudney was on duty at the time. Holliday worked a full 24-hour shift in a normal manner beginning at 7 a.m. the following day.

> 2 Cudney was a party to the proceedings below and originally joined in the appeal. Pursuant to a written stipulation of the parties, we dismissed Cudney's appeal by order filed April 18, 1990. Holliday is now the sole appellant.

On February 26, 1987, Fire Chief Laurence Sheldon learned of the incident. Without consulting anyone else, Chief Sheldon issued a memorandum to Holliday advising him that the incident "constitutes a violation of Modesto Fire Department Rules and Regulations, F.R. 213(f), 'Members of the department shall not use drugs or narcotics whose use or possession would be illegal, unless such drugs or narcotics are properly prescribed by a physician for an illness or injury.'" The memo further advised Holliday that before returning to work he would have to provide either a letter from a [***4] doctor stating that the marijuana had been medically prescribed or "medical results of a drug test conducted under the guidance of a licensed physician." Holliday was advised that the purpose of the drug test was to ensure his ability to perform his function as fire lieutenant and that the drug test must include an evaluation by the physician as to his ability to properly perform his job requirements, taking into account the drug test results. Finally, Holliday was directed to attend an investigative board hearing on March 3, 1987, "to determine if disciplinary action should be taken regarding this matter. . . . Their recommendations will be considered by this office prior to final disposition of this matter."

Holliday appeared as directed before the investigative board. He was asked three questions: (1) Do you want to tell us what happened that night?; (2) Have you submitted to a drug test?; and (3) Will you be willing to prepare written statements of the events that led to your being cited on February 25 prior to leaving the building today? Holliday answered each of the questions in the negative. He answered no to questions (1) and (3) because he had not had an opportunity [***5] to speak with a lawyer, he did not think he had to discuss his personal business even though he knew [**208] that possession of marijuana was a violation of department regulations, the investigative board was a new procedure for which he was unprepared, and he feared the consequences of speaking to the board.

After the hearing, Chief Sheldon sent Holliday a letter dated March 3, informing him that he would be suspended without pay until such time as Holliday complied with Chief Sheldon's drug-test directive of February 27 to ensure his ability to perform.

Holliday failed to comply with the February 27 and March 3 directives, and Chief Sheldon directed that his pay be discontinued effective [*532] immediately, leaving other benefits intact. On March 16, 1987, operations officer Thurman Norton wrote to Holliday informing him that he intended to recommend Holliday's dismissal effective March 31, 1987. Stated grounds included: (1) violation of fire department rule FR 258 ("Employees shall obey the lawful orders of a superior officer at all times"), in that Holliday failed to obey Chief Sheldon's orders of February 27 and March 3; (2) violation of rule FR 212 ("Employees, whether on duty or [***6] off duty, . . . shall commit no act which [would] bring reproach or discredit upon the Fire Department"); (3) violation of rule FR 106 ("An employee . . . who is in violation of any fire regulation or order, may receive appropriate discipline, such as reprimand, demotion, reduction in salary, or discharge"); and (4) violation of rule FR 213(f) ("Members of the Department shall not use drugs or narcotics whose use or possession would be illegal, unless such drugs or narcotics are properly prescribed by a physician for an illness or injury"). Norton went on to advise Holliday of his right to respond by March 30, and his right to appeal any disciplinary action pursuant to Modesto Municipal Code section 2-5.12.

On March 25, 1987, Holliday's union president, Captain Ronald Mendoza, requested that Chief Sheldon extend the response deadline to April 1 and arranged for a meeting on that date. On March 26, 1987, Chief Sheldon received from Mendoza a report from Dr. William Broderick dated March 23 and stating that "Jerry Holliday Was Examined by Me Today and the Results Revealed No Evidence of Any Health or Drug Problems. [para.] He Has the Ability to Properly Perform the Required Functions [***7] of His Position as a Lt. of the Modesto Fire Dept." Chief Sheldon accepted this as the required drug test report without knowing that no actual chemical drug test had been performed.

On March 30, 1987, Holliday took a urine test for illegal drugs, and tested "clean." He never presented those results to Chief Sheldon.

At the April 1 meeting, Chief Sheldon made no further inquiry regarding drug testing, and Holliday did not volunteer the results from his urine test of the previous day as they had not yet come in. After the hearing Sheldon rejected the proposed termination, instead returning him to the payroll as of April 2, demoting him two ranks (to firefighter), and requiring him to submit to drug testing "twice per calendar year beginning 7/1/87 and concluding 12/31/89."

Holliday appealed the disciplinary order and on January 6, 1988, the hearing officer issued his findings and conclusions. He found that Holliday had violated department rule FR 213(f) by using marijuana while off duty, and that rule FR 213(f) was valid. He found that such marijuana use also [*533] violated department rule FR 212. He further found that Chief Sheldon's directive that Holliday submit to drug [***8] testing was reasonable and within Sheldon's authority, and that Holliday's unreasonable delay in complying with this directive was a violation of department rule FR 258. He found that Sheldon was acting within his authority when he convened an investigative board and directed Holliday's appearance, and that Holliday's refusal to cooperate with the board was a violation of department rules FR 258 and FR 106.

The hearing officer further found that the MMBA did not prevent Chief Sheldon from ordering Holliday to submit to drug [**209] testing without meeting and conferring with union representatives.

Although finding that most of the charged rule violations were supported by the evidence, the hearing officer found the discipline imposed excessive. He instead recommended that Holliday receive a 60-day suspension (reduced to 39 days due to the 21 days of suspension already imposed), with no reduction in rank. He stated that a two-rank reduction would cause Holliday to lose an estimated $ 170,000 in salary and retirement benefits.

On January 21, 1988, City Manager Lipsky wrote to Holliday to inform him that he had adopted the findings and conclusions of the hearing officer, but rejected the officer's [***9] recommended discipline. "On balance, I find that the Fire Chief's original action in demoting you to the rank of Fire Fighter is justified." Lipsky also reimposed the biannual drug tests which Chief Sheldon had previously ordered.

On April 7, 1988, Holliday filed a verified petition for writ of mandate in the Stanislaus County Superior Court seeking relief from the ordered discipline (Code Civ. Proc., § 1094.5). Respondents City of Modesto, City Manager Lipsky, and Chief Sheldon answered on May 4.

Holliday subsequently moved for issuance of a peremptory writ of mandate. After hearing, the court issued a partial ruling on January 23, 1989. The court found that Holliday had violated rule FR 212 in that Holliday's conduct was such as could bring reproach to the fire department. The court disagreed with the hearing officer's conclusion that Holliday's conduct before the investigative board violated department rules. The court further found that Chief Sheldon had ordered Holliday to submit to drug testing, that this order was lawful and not in violation of the MMBA, and that the written statement by Dr. Broderick "was not what the Chief directed as [Holliday], using common sense, [***10] had to know that a 'drug test' meant a physical test."

[*534] The court found, as had the hearing officer, that the discipline imposed was "excessive." However, the court did not go so far as to hold that the discipline was an abuse of discretion. Instead, it requested additional briefing on this question.

Each side submitted additional points and authorities. On March 30, 1989, the court issued a minute order denying the petition for writ of mandate, finding no abuse of discretion in the discipline imposed. A formal statement of decision dated July 6, 1989, repeated the same theme:

"From the cases cited, it appears that Respondents could even have terminated Petitioners with the same result, supporting the position that the punishment imposed was of the nature where reasonable minds could differ." The statement of decision and judgment were filed on July 10. This appeal followed.

Discussion

I. *What Is The Appropriate Standard Of Review?* *

. . .

* See footnote, *ante*, page 528.

II. *Did Respondents'* [***11] *Actions in Requiring Drug Testing Without Union Involvement Violate the MMBA?*

The MMBA (§ 3500 et seq.) governs the rights of employees of public agencies to organize and negotiate with their employers.

"Recognized employee organizations shall have the right to represent their members in their employment relations with public agencies." (§ 3503.) "The scope of representation shall include all matters relating to employment conditions and employer-employee relations, including, but not limited to, wages, hours, and other terms and conditions of employment, . . ." (§ 3504.) The public agency employer "shall meet and confer in good faith regarding wages, hours, and other terms and conditions of employment with representatives of such recognized employee organizations . . . and shall consider fully such presentations as are made by the employee organization on behalf of its members prior to arriving at a determination of policy or [**210] course of action." (§ 3505.) Modesto's firefighters are represented by Modesto Fire Fighters Local 1289.

Holliday was ordered on February 27 and March 3, 1987, to submit to drug tests. The February 27 order directed him to do so "prior to returning [*535] [***12] to [his] normal duty assignment." The March 3 order was a suspension without pay pending compliance with the previous order, to begin on March 11. Apparently the ordering of drug tests was a brand new procedure unilaterally adopted by respondents without notice. To the best of Chief Sheldon's knowledge, no firefighter had ever previously been ordered to take a drug test.

On March 8, 1987, Local 1289's counsel wrote to Chief Sheldon, advising him that the ordered drug testing was a "new condition of continued employment" requiring prior negotiation with the union under the MMBA. "The City may not unilaterally impose a mandatory drug program prior to an impasse in negotiation." The respondents did not reply to the union's letter. In the proceedings below and on appeal the respondents contend that the drug testing ordered in this case was not subject to the MMBA.

"Although the Meyer-Milias-Brown Act [*sic*] requires that a government employer 'meet and confer' regarding 'wages, hours and other terms and conditions of employment' . . . a public entity does not need to meet and confer over 'considerations of the merits, necessity, or organization of any service activity provided [***13] by law or executive order' (*Government Code*, Section 3504)."

(1) In *Fire Fighters Union* v. *City of Vallejo* (1974) 12 Cal.3d 608 [116 Cal.Rptr. 507, 526 P.2d 971], the Supreme Court attempted to "reconcil[e] the two vague, seemingly overlapping phrases of the statute: 'wages, hours and working conditions,' which, broadly read could encompass practically any conceivable bargaining proposal; and 'merits, necessity or organization of any service' which, expansively interpreted, could swallow the whole provision for collective negotiation and relegate determination of all labor issues to the city's discretion." (*Id*. at p. 615.) The Supreme Court observed that "the Legislature included the limiting language not to restrict bargaining on matters directly affecting employees' legitimate interests in wages, hours and working conditions but rather to forestall any expansion of the language of 'wages, hours and working conditions' to include more general managerial policy decisions." (*Id*. at p. 616.)

Thus, the question here is whether respondents' orders that [***14] Holliday submit to drug testing constitute a condition of employment, and thus a subject of negotiation with the union, as opposed to a "more general managerial policy decision[]" beyond the scope of union representation and the MMBA's meet and confer requirement.

Apparently no reported California case deals with this issue. **(2)** However, any federal cases interpreting the National Labor Relations Act

(NLRA) are viewed as authority in analyzing the MMBA.

[*536] "The Meyers-Milias-Brown Act (Gov. Code, § 3500 et seq.) parallels the National Labor Relations Act (29 U.S.C. § 151 et seq. (NLRA)) and California courts should look to federal case law in interpreting the act." (*Public Employees Assn.* v. *Board of Supervisors* (1985) 167 Cal.App.3d 797, 806-807 [213 Cal.Rptr. 491].)

Holliday points out that the National Labor Relations Board (NLRB) has concluded that drug testing of current employees is a mandatory subject of bargaining under the NLRA.

"We find that the Respondent's newly imposed requirement of drug/alcohol testing for employees who require medical treatment for work injuries is a mandatory subject of bargaining. In *Ford Motor Co.* v. [***15] *NLRB*, the Supreme Court described mandatory subjects of bargaining as such matters that are 'plainly germane to the "working environment"' and 'not among those "managerial decisions, which lie at the core of entrepreneurial control."' Applying these standards to the issue before us, we find the drug/alcohol testing requirement to be [**211] both germane to the working environment, and outside the scope of managerial decisions lying at the core of entrepreneurial control." (*Johnson-Bateman Co*. (1989) 131 Lab.Rel.Ref. Manual (Bur.Nat.Affairs) pp. 1393, 1396, fns. omitted.)

Although the testing in *Johnson-Bateman* was of workers "who require medical treatment for work injuries," the rationale for the NLRB's conclusion appears to apply here. As in *Johnson-Bateman*, the instituted testing constitutes "a condition of employment because it has the potential to affect the continued employment of employees who become subject to it." (*Johnson-Bateman Co., supra*, 131 Lab.Rel.Ref. Manual at p. 1397.) The NLRB likened drug/alcohol testing to physical examinations and polygraph testing, both of which had previously been found to be mandatory subjects of bargaining. (*Id*. at p. 1396; [***16] see *Lockheed Shipbuilding Co*. (1984) 273 NLRB 171, 177 [physical examinations]; *LeRoy Machine Co*. (1964) 147 NLRB 1431, 1432, 1438-1439 [physical examinations]; *Austin-Berryhill, Inc*. (1979) 246 NLRB 1139 [polygraph testing]; *Medicenter, Mid-South Hospital* (1975) 221 NLRB 670 [polygraph testing].) "[T]he Respondent has introduced relatively sophisticated technology, substantially varying both the mode of the investigation and the character of proof on which an employee's job security might depend. [para.] In light of the above considerations, therefore, we conclude that the drug/alcohol testing requirement is entirely 'germane to the working environment,' . . . and thus, to that extent, it is a mandatory subject of bargaining." (*Johnson-Bateman Co., supra*, 131 Lab.Rel.Ref. Manual at p. 1397, fn. omitted.)

Similarly, the NLRB found that the drug-testing program was "outside the scope of managerial decisions lying at the core of entrepreneurial [*537] control." "It does not involve the commitment of investment capital and cannot otherwise be characterized as a decision taken with a view toward changing [***17] the scope or nature of the Respondent's enterprise. It is rather a more limited decision directed toward reducing workplace accidents and attendant insurance rates. Accordingly, we conclude that the instant drug/alcohol testing requirement is a mandatory subject of bargaining." (*Johnson-Bateman Co., supra*, 131 Lab.Rel.Ref. Manual at pp. 1397-1398, fn. omitted.)

Respondents seek to distinguish *Johnson-Bateman*, pointing out that it and other similar NLRB decisions did not involve testing based on individualized suspicion. They cite no authority for drawing the distinction, however, and we see no basis for it in the provisions of the MMBA or its NLRA counterpart. If a matter relates to the employment conditions of a single employee, even one who is reasonably suspected of drug use, it appears to fall within the scope of representation.

The court below apparently accepted respondents' argument that reasonable suspicion is a sufficient basis for ordering drug tests without prior negotiation. In its ruling and statement of decision the court, dismissing Holliday's MMBA-grounded contention, said:

". . . While [Holliday] may be correct that submission of drug tests in general [***18] by employees is subject to collective bargaining and cannot unilaterally be imposed by the employer, the Court concludes that the reasoning of the out of state cases cited by respondent[s] on this issue is compelling and that an employee reasonably believed to have been using drugs may be compelled to submit to a drug test at the direction of

his employer. *Turner* v. *Fraternal Order of Police* (1980) 500 A.2d 1005; *O'Connor* v. *Ortega* (1987) 107 S.Ct. 1492; *Everett* v. *Napper* (1987) 833 F.2d 1507; *Lovvern* [*sic*] v. *City of Chattanooga, Tenn*. (1988) 846 F.2d 1539. See also *White* v. *Davis* (1975) 13 C.3d 757, where compelling State interest overrides one's right to privacy."

None of the cases cited by the lower court, however, have anything to do with the bargaining requirements of the MMBA, or of the NLRA. Although the plaintiff in *O'Connor* v. *Ortega* (1987) 480 U.S. 709 [94 L.Ed.2d 714, 107 S.Ct. 1492] was apparently a California public employee covered by the MMBA, that case was framed purely [***19] on Fourth Amendment grounds. *Turner* v. *Fraternal Order of Police* (D.C. [**212] 1985) 500 A.2d 1005, *Everett* v. *Napper* (11th Cir. 1987) 833 F.2d 1507, and *Lovvorn* v. *City of Chattanooga, Tenn*. (6th Cir. 1988) 846 F.2d 1539, vacated and rehearing granted 861 F.2d 1388, substitute opinion *Penny* v. *Kennedy* (6th Cir. 1990) 915 F.2d 1065, all involved public employees outside California, thus beyond [*538] the reach of both the MMBA and the NLRA (which excludes from its purview "any State or political subdivision thereof"; see 29 U.S.C. § 152). Finally, *White* v. *Davis* (1975) 13 Cal.3d 757 [120 Cal.Rptr. 94, 533 P.2d 222] was a police search, not an employment-related matter at all.

As another justification for ordering drug tests without prior negotiation respondents cite *San Jose Peace Officer's Assn.* v. *City of San Jose* (1978) 78 Cal.App.3d 935 [144 Cal.Rptr. 638]. In that case San Jose's police department, without meeting and conferring with its employees' organization, adopted a regulation governing [***20] the circumstances under which a police officer would be permitted to discharge a firearm. The appellate court upheld the city's action because the "use of force policy is as closely akin to a managerial decision as any decision can be in running a police department, surpassed only by the decision as to whether force will be used at all. While private managerial concepts do not translate easily to the public sector, we can imagine few decisions more 'managerial' in nature than the one which involves the conditions under which an entity of the state will permit a human life to be taken." (*Id*. at p. 946.) The central theme of the court's reasoning seems to be that "the use of force policy is primarily a matter of public safety" which impinges only indirectly on a condition of employment. (*Id*. at p. 947.)

In reaching its decision, the *San Jose Peace Officer's Assn*. court distinguished *Fire Fighters Union* v. *City of Vallejo, supra*, 12 Cal.3d 608 in which the California Supreme Court indicated that if a constant manning procedure there under review "primarily" involved [***21] employee workload and safety it would relate to a condition of employment, but not if it "primarily" involved the city's fire protection policy. As noted, the *San Jose* court concluded that employee safety was not the city's primary motivation in adopting the use of force regulation.

Significantly, the *San Jose* court, while discussing the employee safety aspect of the city's use of force policy, noted a difference between the dangers facing policemen and those facing firemen. "[P]olice work presents danger from third parties, rather than from dangerous working conditions. Thus the employer cannot eliminate safety problems merely by purchasing better equipment or by increasing the work force, as in *Fire Fighters* [*Union* v. *City of Vallejo, supra*, 12 Cal.3d 608]." (78 Cal.App.3d at p. 946.)

Respondents urge us to apply the *San Jose* decision here. On this record, however, we are unable to do so.

Initially, we note that the trial court made no findings regarding the purposes respondents sought to accomplish by ordering drug testing. Had [*539] the court found that the order was designed [***22] *primarily* to protect public safety, the finding would not be supported by substantial evidence. Respondents offered no evidence that public safety was their primary consideration. Chief Sheldon testified Holliday's duties as a fire lieutenant were "to give orders and to direct men in fire suppression, EMS [emergency medical service] duties, routine duties, and the station's inspections, and a lot of other associated work in that regard." A lieutenant does not normally operate equipment. When asked to explain his reasons for requiring a drug test, Chief Sheldon responded:

"Any impaired judgment on [Holliday's] part or wrong action could impair the safety and the welfare of those men that work under [him], and, also, those men that worked with [him]. In a specific emergency circumstance which may or may not come up, but could come up in a moment's notice, any impairment could jeopardize [him] and other

men as well as the public."

[**213] Although Chief Sheldon's testimony would support a finding that public safety was one of his concerns in ordering a drug test, it does not show that public safety was his primary concern. In addition, other evidence throws doubt on respondents' contention. [***23] The first drug-test order was given on February 27, 1987, although Chief Sheldon learned of the marijuana smoking incident on February 26. When he first learned of the incident on the 26th, Chief Sheldon made no effort to ascertain whether Holliday was then on duty (he was). If public safety was Chief Sheldon's primary concern, one would expect him to take immediate steps to prevent Holliday from working. In neither of his written directives to Holliday, dated February 27 and March 3, did Chief Sheldon refer to public safety as a reason for ordering drug tests. Indeed, in the February 27 memorandum Chief Sheldon ordered that as an alternative to submitting to a drug test Holliday could present a statement by a licensed physician that "marijuana was prescribed for your use." Again, if Chief Sheldon's primary concern was that Holliday's marijuana use threatened public safety, it would not matter whether the use was legal or illegal.

While the trier of fact may not be required to draw the inferences we suggest (that is, that Chief Sheldon's primary reason for ordering a drug test was not the protection of public safety) the evidence clearly does not support the opposite inference.

[***24] Because of the fundamental differences between the use of force policy reviewed in the *San Jose* case and the drug-test order involved here, and because of the absence of evidence showing that respondents' primary purpose was protection of public safety, we cannot apply *San Jose* in this case.

[*540] **(3)** It is worth emphasizing here that the MMBA does not prohibit a public employer from adopting a mandatory drug testing program or adopting any other policy or course of action. The statute simply requires that the employer first meet and confer in good faith with the employee bargaining organization and fully consider that organization's presentations. (§ 3505.) The interests and concerns of any employee subjected to a mandatory drugtesting policy are obvious. Many serious and legitimate questions arise whenever a drug-testing program is considered, including: under what conditions is testing appropriate; what type of testing is appropriate; who conducts the tests; what safeguards are utilized for laboratory integrity and chain of custody of test samples; what retesting procedures are available? Good faith pursuit of the bargaining process will require attention to these and [***25] other pertinent issues and may result in a policy serving the interests of both employer and employees. Even if agreement is not reached, the employer, having satisfied its MMBA obligations, may implement a policy without submitting to mediation. (*Alameda County Employees' Assn.* v. *County of Alameda* (1973) 30 Cal.App.3d 518, 533-534 [106 Cal.Rptr. 441].) The MMBA also permits action by the public agency in cases of emergency. (§ 3504.5.)

We conclude that the order for Holliday to submit to drug testing was a matter "relating to employment conditions" not requiring "consideration of the merits, necessity, or organization of any service or activity provided by law . . . ." (§ 3504.) Before issuing the orders respondents were required to meet and confer in good faith with the employees' bargaining organization and fully consider the presentations of the organization. (§ 3505.) Respondents failed to comply with their MMBA obligations.

III., IV. *

. . .

* See footnote, *ante*, page 528

[***26] The judgment is reversed with directions to enter a new judgment granting Holliday's petition for writ of mandate ordering respondent Garth Lipsky, as Modesto City Manager, to set aside those portions of his determination of January 21, 1988, finding that appellant disobeyed direct orders of [**214] his superior and imposing discipline on appellant; the order shall further direct respondent Lipsky to make a new determination imposing discipline for appellant's violation of Modesto Fire Department rule FR 213(f) which [*541] is fair, just, and reasonable but is at a level less than a two-rank demotion and does not include drug-testing orders. Costs to appellant.