Workplace Searches

By Dennis Nicewander
Assistant State Attorney
17th Judicial Circuit
Broward County, FL

O'Connor v. Ortega, 107 S.Ct. 1492 (1987): **Public**

Physician and psychiatrist, as state employee responsible for training physicians in hospital's psychiatric residency program, had reasonable expectation of privacy in his desk and file cabinets located in his office, for purpose of Fourth Amendment protection, where physician did not share desk or file cabinets with any other employees, and desk and file cabinet contained only personal items.

Public employers' intrusions on constitutionally protected privacy interest of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by standard of reasonableness under all the circumstances; under this standard, both inception and scope of intrusion must be reasonable.

Some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable. Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.

In determining the appropriate standard for a search conducted by a public employer in areas in which an employee has a reasonable expectation of privacy, what is a reasonable search depends on the context within which the search takes place, and requires balancing the employee's legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace. Requiring an employer to obtain a warrant whenever the employer wishes to enter an employee's office, desk, or file cabinets for a work-related purpose would seriously disrupt the routine conduct of business and would be unreasonable. Moreover, requiring a probable cause standard for searches of the type at issue here would impose intolerable burdens on public employers. Their 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. Under this

standard, both the inception and the scope of the intrusion must be reasonable.

The workplace includes those areas and items that are related to work and are generally within the employer's control. At a hospital, for [480 U.S. 716] example, the hallways, cafeteria, offices, desks, and file cabinets, among other areas, are all part of the workplace. These areas remain part of the workplace context even if the employee has placed personal items in them, such as a photograph placed in a desk or a letter posted on an employee bulletin board.

Not everything that passes through the confines of the business address can be considered part of the workplace context, however. An employee may bring closed luggage to the office prior to leaving on a trip, or a handbag or briefcase each workday. While whatever expectation of privacy the employee has in the existence and the outward appearance of the luggage is affected by its presence in the workplace, the employee's expectation of privacy in the contents of the luggage is not affected in the same way. The appropriate standard for a workplace search does not necessarily apply to a piece of closed personal luggage, a handbag or a briefcase that happens to be within the employer's business address.

But regardless of any legitimate right of access the Hospital staff may have had to the office as such, we recognize that the undisputed evidence suggests that Dr. Ortega had a reasonable expectation of privacy in his desk and file cabinets. The undisputed evidence discloses that Dr. Ortega did not share his desk or file cabinets with any other employees. Dr. Ortega had occupied the office for 17 years and he kept materials in his office, which included personal correspondence, medical files, correspondence from private patients unconnected to the Hospital, personal financial records, teaching aids and notes, and personal gifts and mementos. The files on physicians in residency training were kept outside Dr. Ortega's office.

In the case of searches conducted by a public employer, we must balance the invasion of the employees' legitimate expectations of privacy against [480 U.S. 720] the government's need for supervision, control, and the efficient operation of the workplace.

Discussion: This is the landmark case regarding searches by public employers. Since this case contains so much valuable information, I have chosen to simply include important segments

in the above paragraphs. In essence, however, the court is saying that an public employee may have a legitimate expectation of privacy in his office space, but that has to be determined on a case by case basis. If a legitimate expectation exists, the employer must have reasonable grounds to conduct a search. This standard is short of probable cause. The court made it clear that it was only ruling on the issues in this particular case, namely, "legitimate work-related searches" and "noninvestigatory intrusions as well as investigations of work-related conduct." The Court notes that requiring probable cause in work-related cases would grind public offices to a standstill and therefore, something less than probable cause is required. If someone's office is routinely entered by other employees and the public, that person will have no reasonable expectation of privacy in those things visible to everyone. If the employee's desk and filing cabinet are not shared by others, he or she may have such an expectation.

United States v. Ziegler, (9th Cir. 2006): (Private Company)

Defendant did not have a reasonable expectation of privacy in his workplace computer, and thus, he did not have standing to challenge search of computer's hard drive under Fourth Amendment; although defendant had to use individual log-in to access workplace computer, personnel from employer's internet technology (IT) department had complete administrative access to all employees' computers, employer prohibited private use of computers by employees, employer had installed a firewall that monitored employees' internet traffic on workplace computers, IT department reviewed log created by firewall on a regular basis, and employees were apprised in training and in employment manual of employer's monitoring efforts.

United States v. Thorn, F.3d (8th Cir. 2004)

The defendant worked for the Missouri Division of Child Support Enforcement. Thorn was accused of sending offensive email in the office, so his supervisor ordered an IT guy to do a remote search of his computer to see if he was using his office computer to send the emails. The technician found not only the email, but also evidence that Thorn was visiting porn web sites. A more thorough search was then done of the computer. During the investigation, Thorn asked his supervisor to retrieve his tax documents from his office drawer. During that search, the supervisor found more computer generated porn in the desk. Eventually, most everything in the office was searched. Child porn

was located and the police were called. The police obtained a warrant based on the work-related search information provided to them.

The court ruled that the employer conducted a legitimate work-related search. The court explains how each new discovery justified expanding the initial search.

Haynes v. Office of the Attorney General: F.Supp (D.K. 2004)

This case concerns an injunction filed by an assistant attorney general whose computer was searched when he was fired. The case has a good discussion about public employers searching employees' computers. This case involved a unique issue where there was a banner telling users they had no expectation of privacy, but during orientation, employees were advised how to set up one directory for personal files and another for public files. Although the court did not officially ruled on the ultimate issue, it seemed to be leaning in favor of the employee.

United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002) **University Computer**

In prosecution for possession of child pornography, professor did not have a
reasonable expectation of privacy in relation to university computer he used in his work, and therefore was not entitled to a Franks hearing or suppression of evidence found on computer; university's policies and procedures reserved right to audit and monitor Internet use and warned that information flowing through the university network was not confidential, users of university computers were warned of penalties for misuse and of university's right to conduct inspections, university owned computer and explicitly reserved ownership of data stored within it, professor's relationship with computer was incident to his employment, and latent pornographic images in computer were not under professor's immediate control after he attempted to delete them.

Muick v. Glenayre Electronics, 280 F.3d 741 (7th Cir. 2007): **Private**

Employer was not acting under color of federal law when it seized laptop computer it had issued to employee, at behest of federal agents, and held computer until government obtained search warrant to search it for evidence that employee possessed child

pornography, as required to support employee's *Bivens* claim against employer, alleging that employer's actions violated employee's Fourth and Fifth Amendment rights; federal agents wanted employer to give them laptop right away, but it refused until warrant was issued, and there was no agreement between government and employer appointing employer as agent of government.

Employee had no right of privacy in laptop computer that employer had issued to him for use in workplace, and which employer seized at behest of federal agents, and held until government obtained search warrant to search it for evidence that employee possessed child pornography, as required to support employee's *Bivens* claim against employer, alleging that employer's actions violated employee's Fourth Amendment rights; employer had announced policy that it could inspect laptops that it furnished for use of its employees.

If employer equips employee's office with safe, file cabinet, or other receptacle in which to keep his private papers, employee can assume that contents of receptacle are private under Fourth Amendment.

"Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that Muick might have had and so scotches his claim."

"The laptops were Glenayre's property and it could attach whatever conditions to their use it wanted to. They didn't have to be reasonable conditions; but the abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible."

United States v. Slanina, (5th Cir. 2002): **Public**

Note: Large portions of this case have been quoted because of the complexity of the various issues in this case. It reads like a law school exam question and should be studied carefully.

Facts: Slanina worked as the Fire Marshall for Webster, Texas for nine years. As Fire Marshall, his duties included public safety and fire prevention, as well as other related responsibilities. Slanina's immediate supervisor was Fire Chief Bruce Ure, who answered to

the Public Safety Director, Mike Keller. As Public Safety Director, Keller was in charge of both the police and fire departments. Keller had once been Slanina's direct supervisor, but in November 1998 Keller and the City Manager, Roger Carlisle, decided to hire a full-time fire chief, selecting Ure for that position. Prior to Ure's arrival, Keller conducted Slanina's performance evaluations. Although Ure later assumed this responsibility, Keller maintained ultimate authority over Slanina's employment, including the review of his evaluations and any salary increases.

Prior to June 1999, Slanina's desk was located in City Hall, where he had a city-provided computer with Internet access but no connection to the city's intra-office network. When a new fire station was built, however, Slanina moved into his own office in the new station. He brought with him his old computer, but in the new fire station he had no Internet access or network connection. On Friday, June 11, 1999, Ryan Smith, the Management Information Systems Coordinator, began working to install the city network on the fire station computers. At around 5:00 p.m., Smith entered Slanina's new office with a grand master key and attempted to continue his work. The computer was turned on, but a screen saver was in place. Smith moved the mouse and discovered that the screen saver was protected by a password. To bypass the screen saver password, Smith restarted the computer. When he rebooted, however, Smith found that Slanina had installed a BIOS password. Without this password, Smith was unable to immediately access the computer's hard drive and could not install the network on Slanina's computer. Smith then contacted Ure to inform him of the problem, and Ure directed Smith to call Slanina and obtain the password.

Slanina had not come to work that Friday, as he was still recuperating from his recent surgery to have his wisdom teeth removed. Smith did not feel comfortable calling Slanina, so Ure himself phoned him. Ure informed Slanina that the computer technician was in his office attempting to install the network, but was unable to do so because of the password. Slanina initially balked, but after Ure indicated that Smith was already working overtime and that the job had to be completed that day, Slanina agreed to call Smith. On the phone with Smith, Slanina sounded nervous and hesitated before giving his password. He wanted to know exactly what Smith would do to his computer, and Smith promised that he was simply installing the network and configuring his computer to the server.

Having received the password, Smith then resumed his work on Slanina's computer. In order to complete the task, Smith had to walk between Slanina's office and the server room. Upon returning

to the office, Smith unexpectedly encountered Slanina-just ten minutes after they had talked on the phone. Needless to say, Smith was surprised to see Slanina, his jaw still swollen from the surgery. Smith's suspicions were further aroused when after he left the room, Slanina jumped back on his computer. Finally, when Slanina asked how much longer the network installation process would take, Smith lied, telling him that it would be another "couple of hours." Smith overstated the time to give himself a chance to see if something was wrong.

When Slanina finally left, Smith saw that the email was running, but minimized on the screen. As Smith clicked on the email to close it, he noticed the presence of newsgroups. Three months earlier, Keller had told Smith that no one was permitted to have newsgroups on their computers, but the policy had not been disseminated to the fire station employees, including Slanina. Smith expanded the email to look further at the newsgroups and saw three titles suggesting the presence of pornography. It was widely known that employees were not allowed to have pornographic material on their computers. To further investigate, Smith clicked on one newsgroup title, "alt.erotica.xxx.preteen", and saw that about 25 of the approximately 60 files had been read. At that point, however, he did not view any of the files.

Before contacting Ure, Smith wanted to be certain that Slanina's computer did have pornographic material on it. He conducted a search for JPEG files, which contain photographic images, and GIF files, which are used for other graphic images. His search located one such file in the Recycle Bin, and Smith restored the file. When he saw that it contained an image of adult pornography, he printed the file and attempted to contact Slanina's superiors. Neither Ure nor Keller were available, though, and initially Smith was only able to reach the Assistant Fire Chief, Dean Spencer. By the time Spencer arrived at the station, Smith had spoken to Ure, telling him that he had found child pornography on Slanina's computer. Ure instructed him to secure the office, so at 7:00 p.m. Smith changed the lock on the door, turned the computer off, and left.

The next day, Smith spoke again to Ure, who by now had contacted Keller at an FBI conference in South Padre Island. Keller told Ure and Smith to remove the computer from the fire station and place it in his office, which was located in the police station. When they went to Slanina's office, Smith showed Ure the pornography before removing the computer. On Sunday afternoon, Keller returned from his conference and contacted Smith and Ure, asking them to meet him in his office at 3:00 p.m. Once there, Keller instructed Smith and Ure to get what was needed to view

the contents of Slanina's computer, as well as any zip disk or drive in Slanina's office. Smith and Ure then returned to Slanina's office and retrieved the monitor and disks before rejoining Keller in his office. Smith showed Keller the picture of adult pornography he had printed on Friday night, and also pointed him to where he had found the image on the computer. With Smith's assistance, Keller searched material on the computer and zip drive for about two hours, viewing explicit child pornography. Finally, Keller contacted City Manager Carlisle and informed him that child pornography had been discovered on Slanina's computer. Their discussion addressed the possibility of criminal violations as well as the misuse of city property. Human Resources was then contacted, and Keller indicated to Smith and Ure that they should notify the FBI the next day.

At 7:15 a.m. on Monday morning, Ure met Slanina in the parking lot as he arrived at work, milk and doughnuts in hand. Ure told Slanina that they needed to meet in Keller's office, and asked him to get into Ure's vehicle. Remembering that Slanina had undergone dental surgery the previous week, Ure asked him whether he had taken any medication that morning. Slanina said he had not, remarking that doing so would be a violation of city policy because he drove a city vehicle to work. In fact, though, he had taken medication, specifically the painkiller Vicodin. As they approached Keller's office at the police station, Slanina became visibly anxious, rocking back and forth. When they arrived, Slanina met Captain Ray Smiley of the Internal Affairs Division and was furnished with a written copy of the Internal Affairs investigation. He was told that he would be suspended pending the investigation, which concerned the misuse of city property by obtaining child pornography with a city computer. Keller informed him that they had seized his computer and ordered Slanina to surrender his badge and city identification.

Keller told Slanina that he was not in custody and could leave at any time, but Slanina stayed with them. He admitted to accessing the newsgroups and downloading the pictures of child pornography. Keller explained that they would be contacting the FBI. Slanina promised to comply with the investigation, saying that he wanted to get the process going. Although he was embarrassed, Slanina said that he was relieved that it was finally out in the open. He confessed that he had some more "stuff" at his home, which Keller understood to mean more pornography. Keller told Slanina that he could either consent to a search of his home computer or they could obtain a search warrant. Wanting to be present when the police came to his home and confronted his family, Slanina consented and accompanied Keller, Ure and Smiley to his house. Once there, Slanina spoke with his wife and

Keller informed her that her husband was under investigation for child pornography. Slanina then led them to his study, where he invited them to take the computer, zip drives and disks. After they gathered the equipment, Keller indicated to Slanina that he should return with them.

When they got back to the police station, Slanina waited in a conference room while Keller performed some administrative tasks related to the Internal Affairs investigation. Keller then searched the home computer and found more child pornography. Several weeks later, they discovered that the home computer actually belonged to the city. At about 9:00 a.m., Keller told Detective Sergeant Charles Propst to interview Slanina. He stated that although Slanina was not yet under arrest, they had found child pornography on his computer. Propst led Slanina into an interview room, where Sergeant Shari Burrows ("Burrows"), a Galveston child protective services officer, was present. The interview was taped, and Slanina was reminded again that he was not under arrest and was free to leave at any time. Nevertheless, pursuant to the Galveston County District Attorney's policy, Burrows provided Slanina with *Miranda* warnings. Slanina was fully cooperative and, at the end of the interview, signed a written statement. He then returned to Keller's office and offered to provide whatever help they needed. Finally, Slanina indicated that he wanted to leave, and was told that he could. Two days later, he was fired.

The office and home computer equipment, drives, and disks were turned over to the FBI, which examined active files and recovered deleted files from the hard drives. Each computer had two hard drives. Child pornography was found on each hard drive, and all together these hard drives contained thousands of files with such images. In addition, news servers had been installed on both computers, set to search for images of preteen and child sex. Additionally, three zip disks were also searched. The zip disk from Slanina's office contained more than one hundred files of child pornography. No child pornography was found on the two zip disks recovered from Slanina's home.

Holding:

- Slanina clearly demonstrated a subjective expectation of privacy with respect to his office and office computer equipment. He had closed and locked the door to his office. To limit access to his computer files, he installed passwords, thereby making it more difficult for another person to get past the screen saver and reboot his computer.
- Slanina did not forfeit his expectation of privacy in the files by providing the BIOS password to Smith, as he gave

Smith the password for the limited purpose of installing the network, not perusing his files.

- Slanina had a private office at the new fire station, and the ability of a select few of his coworkers to access the office does not mean that the office was "so open to fellow employees or the public that no expectation of privacy is reasonable." *O'Connor v. Ortega, 480 U.S. 709, 718, 94 L. Ed. 2d 714, 107 S. Ct. 1492 (1987)*
- Even though network administrators and computer technicians necessarily had some access to his computer, there is no evidence that such access was routine.
- Given the absence of a city policy placing Slanina on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer, we hold that Slanina's expectation of privacy was reasonable.
- Ensuring an efficient workplace should not be frustrated simply because the same misconduct that violates a government employer's policy also happens to be illegal.
- Keller's search of Slanina's office computer equipment, including the hard drives and zip disks, should be reviewed under the *O'Connor* standard. As an expert in child pornography investigations, Keller undoubtedly appreciated the possibility that the investigation into Slanina's misuse of city computer equipment might result in evidence of criminal violations. Nevertheless, any evidence of criminal acts was also proof of work-related misconduct. Once Smith and Ure uncovered evidence of work-related misconduct, the city did not lose its interest in being able to fully investigate such misconduct in a regular and efficient manner.
- To hold that a warrant is necessary any time a law enforcement official recognizes the possibility that an investigation into work-related misconduct will yield evidence of criminal acts would frustrate the government employer's interest in the efficient and proper operation of the workplace.
- Keller's search was justified at its inception and reasonably related to the circumstances justifying the interference in the first place. At the inception of his search, Smith had already discovered titles of newsgroups suggesting the presence of child pornography on Slanina's computer. Smith had also found an image of adult pornography,

which represented a violation of city policy. On this evidence alone, Keller was justified in conducting a full search of the computer and accompanying disks to look for evidence of misconduct. Moreover, the scope of the search was also reasonable. The computer had been provided to Slanina by the city, and any use of it to access pornography was a violation of city policy.

- We have no occasion to consider the constitutionality of a search of a government employee by a law enforcement officer who is not also the employee's supervisor. Moreover, we do not address the situation where the criminal acts of a government employee do not also violate workplace employment policy.
- Even though the FBI search does not fall under *O'Connor* warrant exception, their subsequent search was valid because once the employer found the images, Slanina's expectation of privacy in them had already been eroded. He cannot then complain about the FBI search of the same materials even though the FBI may have looked at more files than Keller.
- Slanina's consent to the search of his home computer was voluntary based upon:
    - He was extremely cooperative during the meeting in Keller's office and once they arrived at his house.
    - His main concern was minimizing the disruption to his wife and children.
    - He acknowledged that he was embarrassed about the pornography on his office computer, but said he was relieved that it was finally out in the open.
    - He displayed not signs that the pain killers were affecting his judgment, especially since he showed he was aware of the enormity of the situation and wanted to contain the damage to his family.

Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001):

Leventhal v. Knapek, 266 F.3d 64 (2nd Cir. 2001)

State agency employee had reasonable expectation of privacy in contents of his office computer, as required to support employee's § 1983 Fourth Amendment action against agency arising from unannounced after-hours search of computer to look for personal

files; employee occupied private office with door and had exclusive use of computer, and agency did not have routinely conduct searches of office computers nor had it adopted policy against mere storage of personal files, as opposed to use of agency time for personal business.

Gossmeyer v. McDonald, 128 F.3d 481 (7th Cir. 1997):

> Warrantless search of state employee's office, desk, storage unit, and file cabinet was workplace search, that only had to be reasonable under all the circumstances, though employee purchased storage unit and file cabinet herself and kept storage unit, file cabinet, and desk locked, where employee purchased and used storage unit and file cabinet to store mostly work-related items, she did not purchase desk and likely used it to store work-related items, and she was not only person with key to, at least, storage unit.
>
> If there are reasonable grounds to believe that workplace search will uncover evidence of government employee's misconduct, search is justified at its inception.
>
> Workplace search is reasonable in scope if measures taken by government employer are reasonably related to search's objective and they are not overly intrusive in light of nature of alleged misconduct.
>
> Anonymous tip that state child protective investigator was concealing child pornography in her office showed sufficient signs of reliability for workplace search to be justified at its inception, where tipster identified herself as coworker, made serious and specific allegations of misconduct, and stated where those pictures could be found, and investigator had unusual access to children and extraordinary authority to take such pictures.
>
> Workplace search of state child protective investigator's desk, storage unit, and file cabinet for child pornography was reasonable in scope, and was not transformed into criminal search requiring probable cause, though numerous officials, including outside law enforcement officials, were present, and it was possible that search would lead to criminal charges.

United States v. Taketa, 923 F.2d 665 (9th Cir. 1991):

> Search of state agent's private office at airport facility maintained

by Drug Enforcement Administration (DEA) was not subject to warrant requirement, and was instead governed by and acceptable under standard of reasonableness even though agent was not DEA employee; state agent worked at facility as part of informal arrangement between DEA and state authorities, and search was part of internal investigation initiated after receipt of report that federal agent with whom state agent purportedly conspired admitted rigging "pen registers" to record content of telephone calls; moreover, state agent's office was point at which phone lines at facility terminated and thus was only location for operating pen registers.

Video surveillance of private office at airport facility maintained by Drug Enforcement Administration (DEA) was not investigation of work-related employee misconduct such that it could be judged under standard of reasonableness, even though such standard applied to warrantless search of office as part of investigation into possible illegal wiretapping activity; government agent admitted that investigation had changed from internal affairs investigation into criminal investigation once confirmation of illegal wiretapping activity was made.

Warrantless videotaping in state agent's private office at airport facility maintained by Drug Enforcement Administration (DEA) violated agent's reasonable privacy interests in office inasmuch as videotaping took place after internal affairs investigation into possible illegal wiretapping activity had been converted into criminal investigation.

American Postal Union Workers Union v. U.S. Postal Service, 871 F.2d 556 (6th Cir. 1989):

Postal Service employees, who accepted assignment of lockers and acknowledged in writing that lockers were subject to inspection at any time by authorized personnel and who were parties to collective bargaining agreement which gave employer right to inspect lockers at any time and for any reason so long as union steward was given opportunity to be present, did not have reasonable expectation of privacy in lockers and expressly waived any Fourth Amendment rights in assigned lockers.

Right of Postal Service to conduct searches of employee lockers pursuant to postal regulation and collective bargaining agreement was not affected by Postal Service's failure to exercise that right at any facility at any time prior to search in question.

Showengerdt v. U.S., 944 F.2d 483 (9th Cir. 1991):

> Navy civilian engineer was on notice from his employer that searches of his private office, desk, or credenza at work could occur from time to time for work-related purposes, whether items were locked or unlocked, and, thus, no warrant for search was required.

Sheppard v. Beerman, 18 F.3d 147 (2d Cir. 1994):

> Law clerk for state judge had no reasonable expectation of privacy in his office furniture or file cabinets such that search of such items following his discharge violated Fourth Amendment; relationship between judge and law clerk is one that calls for absolute free flow of information.
>
> Even if law clerk's belongings were seized for short time during judge's search of his things, such short delay by judicial employer in returning disgruntled employee's belongings after employee was fired did not rise to level of Fourth Amendment violation; brief withholding of clerk's belongings while they were searched was not unreasonable in light of judicial employer's overriding interest in securing confidentiality of chambers' work product and in making sure that angry clerk did not attempt to confiscate or destroy important court property.

U.S. v. Mancini, 8 F.3d 104 (1st Cir. 1993):

> Fact that mayor's secretaries had access to appointment calendar did not preclude mayor from claiming legitimate expectation of privacy and standing to challenge seizure of appointment calendar; shared access to document did not prevent one from claiming Fourth Amendment protection in document.
>
> Mayor indicted for extortion demonstrated objectively reasonable expectation of privacy in town's archive attic, which was upstairs in building where he had maintained office for 19 years, for purposes of motion to suppress; moreover, mayor took steps to ensure that no one would have access to his files stored in archive attic without his prior authorization.

Vega-Rodriguez v. Puerto Rico Telephone Company, 110 F.3d 174 (1st Cir. 1997):

> Quasi-public telephone corporation was government actor subject

to suasion of Fourth Amendment.

Employees of quasi-public telephone corporation lacked objectively reasonable expectation of privacy against disclosed, soundless video surveillance while toiling in open and undifferentiated work area.

Mere fact that observation is accomplished by video camera rather than naked eye, and recorded on film rather than in supervisor's memory, does not transmogrify constitutionally innocent act into constitutionally forbidden one, for purposes of Fourth Amendment privacy analysis.

U.S. v. Simmons, 206 F.3d 392 (4th Cir. 2000):

Government employees may have a legitimate expectation of privacy, for Fourth Amendment purposes, in their offices or in parts of their offices such as their desks or file cabinets, but office practices, procedures, or regulations may reduce legitimate privacy expectations.

Public employer's remote, warrantless searches of employee's office computer did not violate his Fourth Amendment rights because, in light of employer's Internet policy, employee lacked a legitimate expectation of privacy in files downloaded from the Internet; Internet policy clearly stated that employer would "audit, inspect, and/or monitor" employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, "as deemed appropriate," and this policy placed employees on notice that they could not reasonably expect that their Internet activity would be private.

Public employer's warrantless entry into employee's office to retrieve his computer hard drive did not violate Fourth Amendment, despite employee's legitimate expectation of privacy in his office, since search was carried out for purpose of obtaining evidence of suspected work-related employee misfeasance, employer had interest in fully investigating employee's misconduct, even if the misconduct was criminal, employer had reasonable grounds for suspecting that hard drive would yield evidence of misconduct as it was already aware of some Internet misuse by employee, and entry into office was reasonably related to objective of the search and not excessively intrusive.

Federal employee possessed legitimate expectation of privacy in his office for Fourth Amendment purposes, where employee did

not share his office, and there was no evidence of any workplace practices, procedures, or regulations that had effect of diminishing his legitimate privacy expectations.

Public employer's Internet policy, stating that employer would "audit, inspect, and/or monitor" employees' use of the Internet, did not render employee's expectation of privacy in his office unreasonable for Fourth Amendment purposes; policy did not mention employees' offices, and, while it did not prohibit employer from carrying out its auditing, inspecting, and/or monitoring activities at employees' individual workstations, this fact alone was insufficient to render employee's subjective expectation of privacy unreasonable.

Discussion: This is an excellent case that should help tremendously in conducting investigations of public employees. A unique issue in this case involves dual levels of privacy. The court held that the employee did not have an expectation of privacy in his computer usage based upon office policies and regulations. On the other hand, he did have a reasonable expectation of privacy in his private office. The question that resulted was whether his employer could enter the office in order to retrieve the computer hard drive. The court ruled that since the employer entered the office for the narrow purpose of obtaining the evidence of employee misfeasance and did not rummage around other areas, the search was reasonable and thus, allowed.

Kelly v. State, 77 So.3d 818 (Fla. 4th DCA 2012);

Employee had no legitimate expectation of privacy regarding his desk at work, and thus warrantless search of desk did not violate Fourth Amendment; employee shared office with another employee, other employees had full access to office, no locks were on desk, desk drawers were accessible to others who, upon at least some occasions, did look through desk, and employee's permission was not always sought in going through his desk.

Employee's direct supervisor, who was employer's general manager, had common authority over the work premises and thus had authority to consent to police officer's search of employee's desk; supervisor had ultimate control over all work premises, and supervisor had authorized prior searches of desk for missing documents or keys.

Even where a private employee retains an expectation that his private office will not be the subject of an unreasonable

government search, such interest may be subject to the possibility of an employer's consent to a search of the premises which it owns.

State v. Young, 32 Fla. L. Weekly (1st DCA 2007):

Under Fourth Amendment, pastor had legitimate expectation of privacy in his office and workplace computer, and thus police could not search office and computer without obtaining search warrant or valid consent to search, although church owned computer; pastor kept office locked when he was away, use of pastor's office by others was for limited purposes, pastor was sole regular user of computer, and computer was not networked to other computers.

District superintendent's personal authority to enter pastor's office in church and to authorize others to do so did not rise to level of common authority that would enable superintendent to consent to search of pastor's office and workplace computer; office was kept locked, and church had no specific policy giving church officials the right to control and use office.

Police officers' reliance on church officials' representations of authority was unreasonable, and thus officers could not rely of officials' apparent authority to obtain valid consent to search pastor's office and workplace computer; officers knew nothing of chairperson of staff parish relations other than fact that he was "representative of the church" who had been told by a supervisor to consent to search

Pastor's incriminating statements during police interrogation that followed police officers' illegal search of pastor's office and workplace computer were fruit of the poisonous tree and thus were not admissible in criminal prosecution of pastor, whose workplace computer contained child pornography, although church officials had provided police with compact disc (CD) containing "questionable images" prior to search, and although printout of pastor's bookmarked websites was from CD; chain of illegality was not broken in that police did not tell pastor during interrogation that printout was from CD, not from computer.

Bateman v. State, 513 So.2d 1101 (Fla. 2d DCA 2001):

Violation of hospital employee's rights arising from warrantless search of his desk on premises of hospital operated by Department of Health and Rehabilitative Services was more egregious where

official initiating and conducting search was also law enforcement officer familiar with necessity of obtaining warrant.

Neither actual practices nor legitimate regulation reduced hospital employee's expectation of privacy in pill bottle in his desk on premises of hospital operated by Department of Health and Rehabilitative Services, where he had not shared office or desk with anyone else during his 19-year tenure at hospital, and where hospital regulations specified standard of reasonable cause and outlined search procedures which were not observed in search by government investigator and security guard.

Acquiescence by employee of hospital operated by Department of Health and Rehabilitative Services to hospital regulations governing searches of employee's personal property on hospital premises did not constitute unconditional waiver of constitutional rights, where regulations contained standards and procedures assuring protections which were not observed.

Discussion: The issue in this case was that the department had specific rules regarding the right to search an employee's office, but those procedures were not followed. The procedures implemented required a certain threshold before the employer could search the employee's office and therefore, the employee maintained a certain level of privacy. The court also pointed out that they would scrutinize these issues more closely when a law enforcement officer is involved in the search.

U.S. v. King, 509 F.3d 1338 (11th Cir. 2007):

Defendant, a civilian contractor who resided in a dormitory at an air base in Saudi Arabia, did not have an objectively reasonable expectation of privacy in the contents of his personal laptop computer when it was connected to the military base's network from his dorm room, and so he suffered no violation of his Fourth Amendment rights when his computer files were searched through the computer's connection to the base network; defendant's files were "shared" over the entire base network, and everyone on the network, that is, potentially thousands of individuals, had access to all of defendant's files and could observe them in exactly the same manner as did the computer specialist who had verified the presence of pornographic videos and explicit text files on the computer, such that, for privacy purposes, the contents of defendant's hard drive were akin to items stored in the unsecured common areas of a multi-unit apartment building or put in a dumpster accessible to the public.

U.S. v. Finley, 477 F.3d 250 (5th Cir. 2007):

> Defendant had standing to challenge the search of his cell phone, even if it was a business phone issued to him by his employer; defendant had possessory interest in phone, defendant had right to exclude others from using phone, employer permitted defendant to use phone for his own personal purposes, and defendant took normal precautions to maintain his privacy in phone.

U.S. v. Heckencamp, 482 F.3d 1142 (9th Cir. 2007):

> For Fourth Amendment purposes, defendant's objectively reasonable expectation of privacy in his computer was not eliminated when he attached computer to network of university at which he was a student; there was no announced monitoring policy on the network, university's computer policy stated that in general, all computer and electronic files should be free from access by any but the authorized user of those files, and defendant's computer was located in his dormitory room and was protected by a screensaver password.
>
> A person's reasonable expectation of privacy may be diminished in transmissions over the Internet or e-mail that have already arrived at the recipient; however, the mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer.
>
> State university computer network investigator's remote search of defendant's computer was justified under special needs exception to search warrant exception; corporation employee reported someone using computer on university's network had hacked into corporation's computer network, investigator found evidence that someone on university network, using computer Internet Protocol (IP) address that investigator connected to defendant, hacked into corporation's network and gained root access to university server that housed 60,000 campus accounts and processed 250,000 daily emails, and although investigator knew FBI was seeking warrant to search defendant's computer, he testified he acted to secure server and not to collect evidence for law enforcement, and he acted against FBI agent's request that he wait.
>
> Even if university police and university computer network investigator violated defendant's Fourth Amendment rights by entering his dormitory room to investigate whether defendant had

hacked into university server, evidence gathered by FBI agents in search of defendant's room pursuant to search warrant the following day was admissible under independent source exception to exclusionary rule, since warrant was supported by probable cause even without evidence gathered through search by university police; affidavit in support of warrant recited evidence that intrusion on server had been tracked to defendant's dormitory room computer, and that defendant had been disciplined in the past for unauthorized computer access to university's system.

Quon v. Archwireless, 529 F.3d 892 (9th Cir. 2008):

Police officer had reasonable expectation of privacy, under Fourth Amendment, in text messages sent to and from his city-owned pager, even though department's written computer and e-mail policy decreed that no expectation of privacy should attach to use of those resources, and even assuming that messages constituted public records under California Public Records Act (CPRA); police lieutenant in charge of pagers had established informal policy under which officer's messages would not be audited if he paid for usage overages, and CPRA did not diminish officer's reasonable expectation.

Police department's search of content of officers' text messages sent and received via city-owned pagers, which was reasonable at its inception based on noninvestigatory work-related purpose of ensuring that officers were not being required to pay for work-related expenses when they reimbursed city for usage overages, was nevertheless unreasonable in scope and thus violative of Fourth Amendment; less intrusive means existed to achieve same end, including warning officers that content of messages would be reviewed in future to ensure work-related uses.

Employees of city police department had expectation of privacy, under Fourth Amendment, in content of text messages that they sent and received using city-owned pagers, and that were archived by wireless service provider that contracted with city; fact that provider had capability to access content for its own purposes did not remove that expectation.

U.S. v. Barrows, 481 F.3d 1246 (10th Cir. 2007):

In determining whether public employee's claim to privacy from government search and seizure is reasonable in light of surrounding circumstances, those circumstances include (1) the employee's relationship to the item seized; (2) whether the item was in the immediate control of the employee when it was

seized; and (3) whether the employee took actions to maintain his privacy in the item.

City employee did not have reasonable expectation of privacy in personal computer that he brought to city hall for work-related use, hooked up to city's network for file sharing, kept continuously on, and failed to password protect or take any other steps to prevent third-party use despite computer's location in public area, and thus discovery of pornographic images on computer by another city worker was not a Fourth Amendment violation.

U.S. v. Rosario, 558 F.Supp.2d 723 (E.D. Ky. 2008):

Soldier who was on active duty in the United States Army lacked a reasonable expectation of privacy in his computer, and thus its warrantless seizure by Army personnel did not violate the Fourth Amendment; soldier lived in an Army barracks, where his computer was located in a long, open room, the computer was connected to a network through which its files were accessible by other computers on the network, soldier left his computer on all the time and allowed numerous individuals access to it, and the computer was not password-protected.

Under the plain view doctrine, warrantless seizure by United States Army personnel of a computer and discs belonging to a soldier did not violate the Fourth Amendment; computer was in soldier's living area in an Army barracks and thus in plain view, the personnel who carried out the seizure were legally present and they had probable cause to believe there was child pornography on the computer's hard drive or discs, and the risk of disappearance of the photos created exigent circumstances.