

WARRANTLESS WORKPLACE SEARCHES OF GOVERNMENT EMPLOYEES

*Bryan R. Lemons
Branch Chief*

There are a variety of reasons why a government supervisor might wish to search a government employee's workplace. For example, a supervisor might wish to conduct a search to locate a needed file or document; the supervisor might wish to search an employee's workplace to discover whether the employee is misusing government property, such as a government-owned computer; or, a supervisor might seek to search an employee's workplace because he has information that the employee is committing a crime, such as using the Internet to download child pornography.

In situations where a public employer wants to search an employee's office or desk, a number of questions typically arise and must be addressed, including: Can government employees have a reasonable expectation of privacy in their offices, desks, computers, and filing cabinets? If such an expectation of privacy does exist, what standards must a supervisor follow to lawfully conduct a warrantless search of those areas? Must a supervisor have probable cause to search a government employee's workplace? Or, is a search permitted on some lesser standard of suspicion?

While the Supreme Court addressed many of these questions in *O'Connor v. Ortega*,¹ it has fallen to lower courts to address others. The purpose of this article is to provide a framework

within which the principles outlined in *O'Connor* for "workplace" searches by government supervisors can be understood and applied. In sum, when a government supervisor is considering the search of a government employee's workspace, a two-part analysis can be utilized to simplify the process. First, determine whether the employee has a reasonable expectation of privacy in the area to be searched. If a reasonable expectation of privacy does exist, then consider how that expectation can be defeated.² Before turning to those issues, however, it is necessary to first define exactly what is meant by the term "workplace."

DEFINING THE "WORKPLACE"

"Workplace," as used in this article, "includes those areas and items that are related to work and are generally within the employer's control."³ This would include such areas as offices, desks, filing cabinets, and computers. However, "not everything that passes through the confines of the business address can be considered part of the workplace context."⁴ As a general rule, a government employee would continue to have an expectation of privacy in his or her personal belongings that have been brought into the workplace environment. Thus, "the appropriate standard for a workplace search does not necessarily

² See, e.g., *State v. Ziegler*, 637 So. 2d 109, 112 (La. 1994) ("The *O'Connor* Court set forth a two-pronged analysis for determining whether an employee's Fourth Amendment rights were violated by an administrative search and seizure. First, the employee must have a reasonable expectation of privacy in the area searched, or in the item seized. ... Second, if a reasonable expectation of privacy exists, the Fourth Amendment requires that the search be reasonable under all circumstances")

³ *O'Connor*, 480 U.S. at 715

⁴ *Id.* at 716

¹ 480 U.S. 709 (1987)(plurality)

apply to a piece of closed personal luggage, a handbag, or a briefcase that happens to be within the employer's business address.”⁵ This is not to say, of course, that a public employee's personal property can *never* be included within the workplace context. In fact, just the opposite is true. A public employee's private property may, in certain circumstances, fall within the scope of a “workplace” search.⁶ Although not always the case, this can occur when an employee is put on notice that his or her property can be searched as part of the workplace environment.

For example, in the Ninth Circuit case of *United States v. Gonzalez*,⁷ the defendant was an employee of a military exchange. Upon leaving work, he was stopped by a store detective, who sought permission to search a personal backpack that was in Gonzalez's possession. Because he had been required to sign a paper indicating that his belongings, such as his personal backpack, might be inspected as a means of deterring theft among the employees, Gonzalez consented. Approximately \$15.00 worth of stolen spark plugs were found in the backpack. After his motion to suppress this evidence was denied, Gonzalez pleaded guilty to larceny, but reserved his right to appeal. On appeal, Gonzalez claimed, among other things, that the search of his backpack violated the Fourth Amendment. In its ruling, the court did not reach the issue of whether the consent given by Gonzalez was valid or not. Instead, the court noted, the paper signed

by Gonzalez when he first began working at the exchange put him on notice that he might be required to submit to a search of his personal belongings. Thus, Gonzalez's “expectation of privacy was limited by his knowledge of the store policy of searching employees' belongings to deter and apprehend theft.”⁸

A similar result was reached by the Seventh Circuit Court of Appeals in *Gossmeier v. McDonald*.⁹ Gossmeier was employed by the Illinois Department of Children and Family Services (DCFS) as a Child Protective Investigator in the Joliet, Illinois, field office. Her “position required her to investigate instances of child neglect, abuse, and sexual abuse,” and “involved photographing evidence for use in court proceedings.”¹⁰ Because of a lack of storage space, Gossmeier, at her own expense, purchased two separate storage devices. Specifically, she bought a four-drawer filing cabinet, in which she kept “evidentiary photographs, photographic equipment, files, and documents,”¹¹ and a two-door storage unit, in which she kept various items. When a local detective received an anonymous tip from one of Gossmeier's co-workers stating that Gossmeier had pornographic pictures in these cabinets, the detective notified the DCFS Office of Inspector General. The next day, a warrantless search of Gossmeier's office, filing cabinet, storage unit, and desk occurred, with some items being seized. No charges were ever brought against Gossmeier, and she brought a lawsuit alleging the warrantless search violated her Fourth Amendment rights. Gossmeier asserted that because she had personally bought the

⁵ *Id.*

⁶ *See, e.g., United States v. Broadus*, 7 F.3d 460, 463 (6th Cir. 1993)(Upholding search of employee's jacket placed in locker where notice provided locker was “subject to inspection at any time by authorized personnel”)

⁷ 300 F.3d 1048 (9th Cir. 2002)

⁸ *Id.* at 1054

⁹ 128 F.3d 481 (7th Cir. 1997)

¹⁰ *Id.* at 484

¹¹ *Id.*

filing cabinet and storage unit, those items were not part of the “workplace” context, but rather her personal items not covered by the *O’Connor* rules. However, the court failed to “find an expectation of privacy in the cabinets simply because Gossmeier bought them herself.”¹² As noted by the court: “The cabinets were not personal containers which just happened to be in the workplace; they were containers purchased by Gossmeier primarily for the storage of work-related materials. ... These items were part of the ‘workplace,’ not part of Gossmeier’s personal domain.”¹³

DOES A REASONABLE EXPECTATION OF PRIVACY EXIST?

As noted previously, the first step in any search of a public employee’s workplace is to determine whether the employee has a “reasonable expectation of privacy” in that area or item. A reasonable expectation of privacy exists when (1) an individual exhibits an actual expectation of privacy, and (2) that expectation is one that society is prepared to recognize as being reasonable.¹⁴ If there is no reasonable expectation of privacy, “a workplace search by a public employer will not violate the Fourth Amendment, regardless of the search’s nature and scope.”¹⁵ Government employees can, and often do, establish expectations of privacy in their government offices, desks, computers, and filing cabinets.¹⁶ A

cursory glance into any government office will show that individual government employees typically expect some form of privacy, based on the intermingling of their personal and professional lives (e.g., pictures of kids on desks and diplomas on walls). To promote efficiency, many government agencies allow, if not encourage, individuals to perform some personal business while in a governmental workplace, such as using a government telephone to make a personal phone call during a lunch hour. Nonetheless, an “expectation of privacy in commercial premises ... is different from, and indeed less than, a similar expectation in an individual’s home.”¹⁷ A government employee’s expectation of privacy is limited by the “operational realities of the workplace,”¹⁸ and “whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.”¹⁹ Although government ownership of the property to be searched (e.g., a government-owned computer assigned to a government employee) is an “important consideration,”²⁰ it does not, standing

reasonable expectation of privacy in her office”); *People v. Rosa*, 928 P.2d 1365, 1369 (Colo. Ct. App. 1996)(“Generally, government employees ... have reasonable expectations of privacy in their offices and workplaces”)

¹⁷ *New York v. Burger*, 482 U.S. 691, 700 (1987); see also *Vega-Rodriguez v. Puerto Rico Telephone Company*, 110 F.3d 174, 178 (1st Cir. 1997)(“Ordinarily, business premises invite lesser privacy expectations than do residences”)[citing *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 353 (1977)]

¹⁸ *O’Connor*, 480 U.S. at 717 (plurality)

¹⁹ *Id.* at 718

²⁰ *United States v. Angevine*, 281 F.3d 1130, 1134 (10th Cir.)(citation omitted), cert. denied, ___ U.S. ___, 123 S. Ct. 182 (2002); see also *United States v. Salvucci*, 448 U.S. 83, 91 (1980)(While ownership of an item does not confer “automatic standing,” the Court has long recognized that property ownership is a “factor to be considered in determining whether an individual’s Fourth Amendment rights have been violated”); *Rawlings v. Kentucky*, 448 U.S. 98, 105

¹² *Id.* at 490

¹³ *Id.*

¹⁴ *Katz v. United States*, 389 U.S. 347, 361 (1967)(J. Harlan, concurring)

¹⁵ *Leventhal v. Knapek*, 266 F.3d 64, 73 (2d Cir. 2001)

¹⁶ *O’Connor*, 480 U.S. at 717 (plurality); see also *McGregor v. Greer*, 748 F. Supp. 881, 888 (D.D.C. 1990)(Reiterating *O’Connor’s* holding that “a government employee may be entitled to a

alone, dictate a finding that no reasonable expectation of privacy exists. “Applicability of the Fourth Amendment does not turn on the nature of the property interest in the searched premises, but on the reasonableness of the person’s privacy expectation.”²¹ Courts have utilized a variety of factors to determine whether a government employee has a reasonable expectation of privacy in his or her workspace. Among the most important are the following:

PRIOR NOTICE TO THE EMPLOYEE
(LEGITIMATE REGULATION)

In *O’Connor*, the Supreme Court held that an employee’s expectation of privacy can be reduced through “legitimate regulation.”²² For example, “government employees who are notified that their employer has retained rights to access or inspect information stored on the employer’s computers can have no reasonable expectation of privacy in the information stored there.”²³ *United States v. Simons*²⁴ illustrates this point. In *Simons*, the Foreign Bureau of Information Services (FBIS), a division of the Central Intelligence Agency, employed the defendant. FBIS had an Internet usage policy that (1) specifically prohibited accessing unlawful material, and (2) prohibited use of the Internet for anything

other than official business. Further, the policy noted that FBIS would “periodically audit, inspect, and/or monitor the user’s Internet access as deemed appropriate.”²⁵ When a keyword search indicated that Simons had been visiting numerous illicit web sites from his government computer, multiple searches of his hard drive were conducted from a remote location, resulting in the discovery of several pornographic images of minors. Simons challenged the search of his computer, claiming his Fourth Amendment rights had been violated. In rejecting this challenge, the Fourth Circuit Court of Appeals held that Simons “did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use in light of the FBIS Internet policy.”²⁶ Through its language, “this policy placed employees on notice that they could not reasonably expect that their Internet activity would be private.”²⁷

A similar result was reached by the Seventh Circuit in *Muick v. Glenayre Electronics*.²⁸ Muick was employed by Glenayre at the time of his arrest for receiving and possessing child pornography. At the request of federal authorities, Glenayre seized a laptop computer from Muick’s work area and held it until a search warrant could be obtained. The computer had been furnished to Muick for his use at work.²⁹ Although Muick was ultimately convicted for receipt and possession of child pornography, he brought a lawsuit against Glenayre. He claimed they had violated his Fourth Amendment rights by seizing the computer and turning it over to the federal officers because the computer

(1980) (“Petitioner’s ownership of the drugs is undoubtedly one fact to be considered” in deciding whether standing existed)

²¹ *Gillard v. Schmidt*, 579 F.2d 825, 829 (3rd Cir. 1978); see also *United States v. Taketa*, 923 F.2d 665, 672 (9th Cir. 1991)(noting that “privacy analysis does not turn on property rights”)

²² *O’Connor*, 480 U.S. at 717 (plurality)

²³ *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Computer Crime and Intellectual Property Section, Criminal Division, Department of Justice at 41 (March 2001)

²⁴ 206 F.3d 392 (4th Cir. 2000), cert. denied, 534 U.S. 930 (2001)

²⁵ *Id.* at 396

²⁶ *Id.* at 398

²⁷ *Id.*

²⁸ 280 F.3d 741 (7th Cir. 2002)

²⁹ *Id.* at 742

contained “proprietary and privileged personal financial and contact data.”³⁰ While the court determined that Glenayre was not acting as an agent of the federal government, it nonetheless addressed Muick’s expectation of privacy in the laptop computer that had been issued to him by the company. Initially, the court noted that it was possible to have “a right of privacy ... in employer-owned equipment furnished to an employee for use in his place of employment.”³¹ So, for example, “if the employer equips the employee’s office with a safe or file cabinet or other receptacle in which to keep his private papers, he can assume that the contents of the safe are private.”³² However, in this case, “Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees ...,” which “ ... destroyed any reasonable expectation of privacy that Muick might have had”³³ As stated by the court:

The laptops were Glenayre’s property and it could attach whatever conditions to their use it wanted. 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.³⁴

Likewise, in *State v. Francisco*,³⁵ a departmental policy was used to defeat a police officer’s claim of an expectation of privacy in a government vehicle. Francisco was a narcotics detective who had been issued a government vehicle that was assigned exclusively to him. When Francisco’s supervisor received information that he (Francisco) was distributing cocaine, the supervisor ordered a search of the government vehicle. Cocaine was found inside a briefcase located in the vehicle. In a motion to suppress, Francisco challenged the seizure of the cocaine, claiming that his Fourth Amendment rights had been violated through the search of the vehicle and briefcase. The court rejected this claim, finding that Francisco had no expectation of privacy in either area. In so holding, the court relied upon the department’s policy and procedure manual, which had a section titled “Search and Inspection of Department Vehicles (to avoid claims of privacy expectations).” This section provided, in part, that “all departmental vehicles (to include all enclosed containers) shall be subject to search and inspection by the Sheriff or his designated representative at anytime, day or night.”³⁶

COMMON PRACTICES AND PROCEDURES

In *O’Connor*, the Supreme Court recognized that “[p]ublic employees’ expectations of privacy in their offices, desks, and file cabinets ... may be reduced by virtue of actual office practices and

³⁰ *Id.*

³¹ *Id.* at 743

³² *Id.* (citations omitted)

³³ *Id.* (citations omitted)

³⁴ *Id.*

³⁵ 790 S.W. 2d 543 (Tenn. 1989)

³⁶ *Id.* at 544

procedures”³⁷ Alternatively, common office practices and procedures may permit a government employee to establish an expectation of privacy in an area where one would otherwise not exist.³⁸ For example, in the Third Circuit case of *United States v. Speights*,³⁹ the defendant was a police officer who retained a locker at his police headquarters. Both a personal lock and a lock that had been issued by the department were used to secure the locker. There were no regulations that addressed the issue of personal locks on the police lockers, nor was there any regulation or notice that the lockers could be searched. There was also no regulation as to what a police officer might keep in the locker. Upon receiving information that Speights had a sawed-off shotgun in his locker, the locker was opened with a master key (for the police-issued lock) and bolt cutters (for Speights’ personal lock). A sawed-off shotgun was recovered in the search, and Speights was convicted of illegally possessing the weapon. On appeal, he claimed his Fourth Amendment rights had been violated by the search of his locker. The Third Circuit Court of Appeals agreed, finding that “no regulation and no police practice” existed to justify the search of Speights’ locker. According to the court, “only if the police department had a practice of opening lockers with private locks without the consent of the user would [Speights’] privacy expectation

be unreasonable.”⁴⁰ While there had been scattered instances of inspections of the lockers for cleanliness (3-4 in 12 years), “there [was] insufficient evidence to conclude that the police department practice negated Speights’ otherwise reasonable expectation of privacy.”⁴¹

Other federal courts in analogous cases have reached parallel conclusions. For example, in *United States v. Donato*⁴², the search of a locker maintained by an employee of the United States Mint was upheld because, among other things, the locker was “regularly inspected by the Mint security guards for sanitation purposes.”⁴³ In *Shaffer v. Field*⁴⁴, the search of a police officer’s locker was upheld in part because three previous searches had been conducted in the past.⁴⁵ In *Schowengerdt v. United States*⁴⁶, the court found no reasonable expectation of privacy could be expected in an office or credenza due to “extremely tight security procedures,” to include “frequent scheduled and random searches by security guards.”⁴⁷ In each of these cases, the courts “relied on specific regulations and practices in finding that an expectation of privacy was not reasonable.”⁴⁸ Alternatively, in *United States v. Taketa*⁴⁹, the court held that a government employee had a reasonable expectation of privacy in his office because, among other things, the office was not “not open to the public and

³⁷ *O'Connor*, 480 U.S. at 717 (plurality); see also *Gillard v. Schmidt*, 579 F.2d 825, 829 (3rd Cir. 1978)(Holding that “an employer may conduct a search in accordance with a regulation or practice that would dispel in advance any expectations of privacy”(citation omitted)

³⁸ See, e.g., *Leventhal*, 266 F.3d at 74 (Finding employee had a reasonable expectation of privacy in the contents of office computer because, *inter alia*, his employer did not have a “general practice of routinely conducting searches of office computers”)

³⁹ 557 F.2d 362 (3rd Cir. 1977)

⁴⁰ *Id.* at 364

⁴¹ *Id.*

⁴² 269 F. Supp. 921 (E.D. Pa.), *aff'd*, 379 F.2d 288 (3rd Cir. 1967)

⁴³ *Id.* at 923

⁴⁴ 339 F. Supp. 997 (C.D. Cal. 1972), *aff'd*, 484 F.2d 1196 (9th Cir. 1973)

⁴⁵ *Id.* at 1001-03

⁴⁶ 944 F.2d 483 (9th Cir. 1991)

⁴⁷ *Id.* at 488

⁴⁸ *Speights*, 557 F.2d at 365

⁴⁹ 923 F.2d 665 (9th Cir. 1991)

was not subjected to regular visits of inspection by [agency] personnel.”⁵⁰

OPENNESS AND ACCESSIBILITY

Courts will often look to the openness and accessibility of a workspace to determine whether an expectation of privacy can be sustained.⁵¹ Generally speaking, the more an item or area in question is given over to an employee’s exclusive use, the more likely an expectation of privacy would be found.⁵² “Where a public employee has his or her own office or desk which co-workers and superiors normally do not enter, and where no agency policy or regulation warns the employee that an expectation of privacy is unreasonable, an expectation of privacy may be reasonable.”⁵³ The more accessible the item or area is to others, the less likely it is an individual employee’s claim of privacy would be accepted.⁵⁴

⁵⁰ *Id.* at 673

⁵¹ *See People v. Holland*, 591 N.Y.S. 2d 744, 747 (1992)(Noting “a person’s legitimate expectation of privacy in a work area will vary depending on an evaluation of the ‘surrounding circumstances’ including the function of the workplace and the person’s efforts to protect his area from intrusion. ... A receptionist in a hospital emergency room waiting area could not reasonably expect that his or her desk top would not be perused by those who seek to avail themselves of the hospital’s services but could legitimately expect that the drawers of that desk would not be invaded”)

⁵² *Taketa*, 923 F.2d at 671 (“[A] reasonable expectation of privacy ... exists in an area given over to an employee’s exclusive use”)

⁵³ *McGregor*, 748 F. Supp. at 888; *see also Holland*, 591 N.Y.S. 2d at 746 (Court noted “it is clear that an individual employee has an expectation of privacy in a locked, private office ...”)

⁵⁴ *United States v. Hamdan*, 891 F. Supp. 88, 95 (E.D.N.Y. 1995), *aff’d*, 101 F.3d 686 (2d Cir. 1996) (“By contrast, the less private a work area - and the less control a defendant has over that work area - the less likely standing is to be found”); *see also Shaul v. Cherry Valley-Springfield Central School District*, 218 F. Supp. 2d 266, 270 (N.D.N.Y. 2002)(Teacher had no

Offices that are “continually entered by fellow employees and other visitors during the workday for conferences, consultations, and other work-related visits ... may be so open to fellow employees or the public that no expectation of privacy is reasonable.”⁵⁵ Where areas are, by their very nature, “open” and “public,” no reasonable expectation of privacy can exist in that area.⁵⁶ Nevertheless, the fact that others may be permitted access to an employee’s office, desk, computer, or filing cabinet, does not alone automatically destroy an employee’s privacy expectation. As one court has noted: “Privacy does not require solitude.”⁵⁷ The existence of a master key will not defeat an employee’s expectation of privacy in his or her office,⁵⁸ nor will an

reasonable expectation of privacy in classroom where classroom was “open to students, colleagues, custodians, administrators, parents, and substitute teachers,” it was not a private office, and “he did not have exclusive use of any furniture in the room”); *State v. McLellan*, 144 N.H. 602, 605, 744 A.2d 611 (1999)

⁵⁵ *O’Connor*, 480 U.S. at 717, 718 (plurality); *see also Holland*, 591 N.Y.S. 2d at 746-47 (Noting “... it is ... obvious that an employee who has his desk positioned in the middle of an area open to the public cannot reasonably expect privacy from the eye of a stranger who is lawfully on the premises”)

⁵⁶ *Thompson v. Johnson County Community College*, 930 F. Supp. 501, 507 (D. Kan. 1996)(“Security personnel and other college employees, including maintenance and service personnel, had unfettered access to this storage room. Consequently, defendants argue that the open, public nature of the security personnel locker area defeats any reasonable expectation of privacy in this area. The court agrees”), *aff’d*, 108 F.3d 1388 (10th Cir. 1997); *O’Bryan v. KTVI Television*, 868 F. Supp. 1146, 1159 (N.D. Iowa 1994)(Court held that, where an unlocked desk or credenza was located in an “open, accessible area,” no reasonable expectation of privacy existed)

⁵⁷ *Taketa*, 923 F.2d at 673

⁵⁸ *Id.* (“Furthermore, the appellants correctly point out that allowing the existence of a master key to overcome the expectation of privacy would defeat the legitimate privacy interest of any

employee's failure to consistently shut and lock an office door automatically sacrifice any expectation of privacy in that area.⁵⁹

Illustrative on this concept is *Coats v. Cuyahoga Metropolitan Housing Authority*,⁶⁰ in which the employee (Coats) brought an attaché case containing a firearm to his workplace. He laid the attaché case next to his desk, which was located within a cubicle work station that had six-foot partitions for walls. Another employee entered the cubicle to answer a ringing phone, and observed the barrel of a firearm in plain view in the unzipped case. A Housing Authority police officer arrived, searched the attaché case, and confirmed the existence of the gun. Based on the incident, Coats was terminated. He then filed suit alleging, in part, that his Fourth Amendment rights had been violated by the search of his cubicle. The court disagreed, holding that Coats had no reasonable expectation of privacy in the cubicle. Specifically:

... Coats' cubicle was one of several cubicles in a larger office and was, in some situations, open to view from certain vantage points in the larger office. The cubicle was open to other employees with access to the cubicle for legitimate work-related reasons, such as, employees ... picking up telephone calls throughout the office using, in this instance, Coats' cubicle telephone line. Accordingly, Coats

hotel, office, or apartment occupant")

⁵⁹ *Id.* ("Nor was the expectation of privacy defeated by O'Brien's failure to shut and lock his door at all times")

⁶⁰ 2001 Ohio App. LEXIS 1699 (2001)

did not have a reasonable expectation of privacy in the cubicle itself. Thus, the entry of the cubicle ... did not violate Coats' Fourth Amendment protections.⁶¹

In *Brannen v. Board of Education*,⁶² the employees were custodians at a high school. Believing that some of the third-shift custodians were spending inordinate amounts of time in the break room during their shifts, their supervisor received permission from the school superintendent to install a hidden video camera in the break room. The camera recorded actions, but no sounds or conversations. The employees brought a lawsuit against the school, claiming the installation of the video camera violated their Fourth Amendment rights. In rejecting this claim, the court found the employees had no reasonable expectation of privacy in the break room, based upon its open and public nature. The court noted that other employees of the school had "unfettered access" to the break room, including "the principal and most of the teachers."⁶³ Additionally, the court found

the break room was more of an all-purpose utility room that contained a washing machine, clothes dryer, cleaning supplies, cleaning machines, lockers, a refrigerator, and a microwave oven. Teachers could access the room whenever they needed something contained inside. Crawford described the break room as "open all the

⁶¹ *Id.* at *10-11

⁶² 761 N.E. 2d 84 (Ohio 2001)

⁶³ *Id.* at 91

time.” The break room was so open to fellow employees that the custodians could not have a reasonable expectation of privacy in the break room.⁶⁴

On the other hand, the Second Circuit case of *Leventhal v. Knapek*⁶⁵ illustrates how the realities of the workplace can result in a finding that a reasonable expectation of privacy *does* exist. Leventhal had a private tax preparation business. In running the business, he impermissibly loaded unauthorized software on his government computer, which was a violation of agency policy. He committed a second violation when he improperly used agency computer equipment to print private tax returns. A warrantless search of his computer in response to an anonymous letter alleging misconduct uncovered the unauthorized software. After disciplinary actions were completed, Leventhal filed suit alleging the warrantless search of his computer was a violation of the Fourth Amendment. While the court ultimately disagreed with Leventhal’s assertion, they did find that he had a reasonable expectation of privacy in the computer. Specifically, Leventhal’s agency had neither “a general practice of routinely conducting searches of office computers,” nor had the agency “placed Leventhal on notice that he should have no expectation of privacy in the contents of his office computer.”⁶⁶ Additionally, the court noted:

Leventhal occupied a private office with a door. He had exclusive use of the desk, filing cabinet, and

computer in his office. Leventhal did not share use of his computer with other employees in the Accounting Bureau nor was there evidence that visitors or the public had access to his computer.⁶⁷

Finally, while support personnel may have had access to Leventhal’s computer at all times, “there was no evidence that these searches were frequent, widespread, or extensive enough to constitute an atmosphere so open to fellow employees or the public that no expectation of privacy is reasonable.”⁶⁸

THE POSITION OF THE EMPLOYEE

Courts will consider both the position occupied by the employee and the surrounding work environment when determining whether a reasonable expectation of privacy exists. For example, “when an individual enters into an employment situation with high security requirements, it becomes less reasonable for her to assume that her conduct on the job will be treated as private.”⁶⁹ As noted by the Supreme Court: “It is plain that certain forms of public employment may diminish privacy expectations even with respect to ... personal searches. Employees of the United States Mint, for example, should expect to be subject to certain routine personal searches when they leave the workplace every day.”⁷⁰ This is especially true where the subject of the search is a law enforcement officer. In cases

⁶⁷ *Id.* at 73-74

⁶⁸ *Id.* at 74

⁶⁹ *Cowles v. State*, 23 P.3d 1168, 1173 (Alaska 2001), *cert. denied*, 534 U.S. 1131 (2002)

⁷⁰ *Nat’l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 671 (1989)

⁶⁴ *Id.* at 91-92

⁶⁵ 266 F.3d 64 (2d Cir. 2001)

⁶⁶ *Id.* at 74

involving law enforcement officers, the officer's "special status must be factored into the reasonableness analysis, for it is within the State's power to regulate the conduct of its police officers even when the conduct involves the exercise of a constitutionally protected right."⁷¹ While law enforcement officers do not lose their Constitutional rights by virtue of accepting their position,⁷² there is a "substantial public interest in ensuring the appearance and actuality of police integrity," in that "a trustworthy police force is a precondition of minimal social stability in our imperfect society."⁷³ This "interest in police integrity ... may justify some intrusions on the privacy of police officers which the Fourth Amendment would not otherwise tolerate."⁷⁴

A case on point is *Biehunik v. Felicetta*,⁷⁵ involving allegations of police brutality. After several citizens were severely beaten by a large group of police officers, the police commissioner ordered 62 police officers to participate in a lineup for investigative purposes. The officers

⁷¹ *Morris v. Port Auth. of N.Y. & N.J.*, 290 A.D.2d 22, 28 (N.Y. 2002)(citations and internal quotation marks omitted)

⁷² *Garrity v. State of New Jersey*, 385 U.S. 493, 500 (1967)(Law enforcement officers "are not relegated to a watered-down version of Constitutional rights")

⁷³ *Biehunik v. Felicetta*, 441 F.2d 228, 230 (2d Cir. 1971)

⁷⁴ *Kirkpatrick v. The City of Los Angeles*, 803 F.2d 485, 488 (9th Cir. 1986); see also *Shaffer*, 339 F. Supp. at 1003 ("The Sheriff's Department has a substantial interest in assuring not only the appearance but the actuality of police integrity. It is not unreasonable that they have the right of inspection ... so that the public may have confidence in public servants"); *Morris*, 290 A.D. 2d at 28 (Noting "the privacy expectations of police officers must be regarded as even further diminished by virtue of their membership in a paramilitary force, the integrity of which is a recognized and important State concern")(citations and internal quotation marks omitted);

⁷⁵ 441 F.2d 228 (2d Cir. 1971)

moved to prevent the lineup, claiming that it violated their Constitutional rights. In rejecting the officers' argument, the Second Circuit noted, "policemen, who voluntarily accept the unique status of watchman of the social order, may not reasonably expect the same freedom from governmental restraints which are designed to ensure his fitness for office as from similar governmental actions not so designed."⁷⁶ Further, said the court, "[t]he policeman's employment relationship by its nature implies that in certain aspects of his affairs, he does not have the full privacy and liberty from police officials that he would otherwise enjoy."⁷⁷

A similar result was reached by the same court, albeit in a different context, in *Sheppard v. Beerman*.⁷⁸ Sheppard, a law clerk, brought a civil action against the judge for whom he clerked, alleging that the judge impermissibly searched his desk in violation of the Fourth Amendment. In holding that Sheppard had no reasonable expectation of privacy in the desk, the court relied upon the unique "working relationship between a judge and her clerk."⁷⁹

Unlike a typical employment relationship ..., in order for a judicial chambers to function efficiently, an absolute free flow of information between the clerk and the judge is usually necessary. Accordingly, the clerk has access to all the documents pertaining to a case. In turn, the judge necessarily

⁷⁶ *Id.* at 231

⁷⁷ *Id.*

⁷⁸ 18 F.3d 147 (2d Cir. 1994)

⁷⁹ *Id.* at 152

has access to the files and papers kept by the clerk, which will often include the clerk's notes from discussions with the judge. Because of this distinctive open access to documents characteristic of judicial chambers, we agree with the district court's determination that Sheppard had "no reasonable expectation of privacy in chambers' appurtenances, embracing desks, file cabinets or other work areas."⁸⁰

WAIVER OF RIGHTS

Government employees may actually waive their expectation of privacy as a precondition of receiving a certain benefit from their employer. In the Sixth Circuit case of *American Postal Workers Union v. United States Postal Service*,⁸¹ postal employees were eligible to receive personal lockers at their postal facility. Before being allowed to do so, however, each employee had to sign a waiver that noted the locker was "subject to inspection at any time by authorized personnel."⁸² Further, the administrative manual of the Postal Services noted that all property provided by the Postal Service was "at all times subject to examination and inspection by duly authorized postal officials in the discharge of their official duties."⁸³ Finally, the collective bargaining agreement for these employees "provided for random inspection of lockers under specified circumstances."⁸⁴

As noted by the court: "In light of the clearly expressed provisions permitting random and unannounced locker inspections under the conditions described above, the collective class of plaintiffs had no reasonable expectation of privacy in their respective lockers that was protected by the Fourth Amendment."⁸⁵

Similarly, in *United States v. Bunkers*,⁸⁶ the defendant was a postal employee suspected of stealing parcels from the mail. As an incident of her employment, she had been provided a locker "... to be used for [her] convenience and ... subject to search by supervisors and postal inspectors."⁸⁷ The Union Agreement provided that: "Except in matters where there is reasonable cause to suspect criminal activity, a steward or an employee shall be given the opportunity to be present in any inspection of employees' lockers." Following the recurring theft of C.O.D. parcels, investigators discovered that the defendant's work schedule coincided with the losses. Surveillance was initiated, and she was observed taking a parcel from her work area to the women's locker room and, within one minute, returning without the package. Investigators then requested the defendant's supervisor search the locker. Throughout the day, three warrantless searches of the locker were conducted outside of the defendant's presence, and a total of 9 mail parcels were discovered. Following her conviction for postal theft, the defendant appealed, claiming her Fourth Amendment rights were violated by the warrantless search of her locker. In rejecting her claim, the court determined the defendant

⁸⁰ *Id.*

⁸¹ 871 F.2d 556 (6th Cir. 1989)

⁸² *Id.* at 557

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ *Id.* at 560

⁸⁶ 521 F.2d 1217 (9th Cir.), *cert. denied*, 423 U.S. 989

⁸⁷ *Id.* at 1219

had relinquished her Fourth Amendment rights based on her “voluntary entrance into postal service employment and her acceptance and use of the locker subject to the regulatory leave of inspection and search and the labor union’s contractual rights of search upon reasonable suspicion of criminal activity”⁸⁸

IF A REASONABLE EXPECTATION OF PRIVACY DOES EXIST, HOW CAN THAT EXPECTATION BE DEFEATED?

If an employee has a reasonable expectation of privacy in his workplace, then an intrusion into that area qualifies as a “search” governed by the Fourth Amendment.⁸⁹ “The Fourth Amendment protects individuals from unreasonable searches conducted by the Government, even when the Government acts as an employer.”⁹⁰ Generally speaking, when searches are performed, courts have expressed a strong preference that they be performed pursuant to warrants.⁹¹ It is well-settled that searches conducted without warrants are *per se* unreasonable unless an exception to the warrant requirement, such as consent, is present.⁹²

⁸⁸ *Id.* at 1221 (citation omitted)

⁸⁹ *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (“A Fourth Amendment search does not occur ... unless ‘the individual manifested a subjective expectation of privacy in the object of the challenged search,’ and ‘society [is] willing to recognize that expectation as reasonable’”).

⁹⁰ *Nat’l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 665 (1989)

⁹¹ *United States v. Holloway*, 290 F.3d 1331, 1334 (11th Cir. 2002) (Noting “there is a strong preference for searches ... conducted under the judicial auspices of a warrant”)

⁹² See *Mincey v. Arizona*, 437 U.S. 385, 390 (1978) (Noting the “cardinal principle” that “searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment, subject only to a few specifically established and well-delineated

Nevertheless, the Court has recognized that in certain special situations, the requirement to obtain a warrant is impractical. “In particular, a warrant requirement is not appropriate when the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search.”⁹³ Such is the case with public employers, who find themselves in a somewhat unique situation. On the one hand, they are obligated to follow the mandates of the Fourth Amendment; on the other, they are responsible for ensuring the efficient and proper operation of their specific department or agency. In cases involving searches conducted by a public employer, courts must “balance the invasion of the employees’ legitimate expectations of privacy against the government’s need for supervision, control, and the efficient operation of the workplace.”⁹⁴ As noted by the Supreme Court:

Employers and supervisors are focused primarily on the need to complete the government agency’s work in a prompt and efficient manner. An employer may have need for correspondence, or a file or report available only in an employee’s office while the employee is away from the office. Or ... employers may need to safeguard or identify state property or records in an office in connection with a pending investigation into suspected

exceptions”) (emphasis in original) (citation omitted).

⁹³ *O’Connor*, 480 U.S. at 720 (plurality) (citation and internal quotation marks omitted)

⁹⁴ *Id.* at 719-720; see also *Morris v. Port Auth. of N.Y. & N.J.*, 290 A.D.2d 22, 27 (N.Y. 2002)

employee misfeasance. In our view, requiring an employer to obtain a warrant whenever the employer wished 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 unduly burdensome. Imposing unwieldy warrant procedures in such cases upon supervisors, who would otherwise have no reason to be familiar with such procedures, is simply unreasonable.⁹⁵

Accordingly, the Court has carved out an exception to the probable cause and warrant requirements for public employers, noting "the special needs, beyond the normal need for law enforcement make the ... probable-cause requirement impracticable for legitimate work-related, noninvestigatory intrusions as well as investigations of work-related misconduct."⁹⁶ In *O'Connor*, the Supreme

⁹⁵ *Id.* at 721-22

⁹⁶ *Id.* at 725 (internal quotation marks and citation omitted); see also *Leventhal*, 266 F.3d at 73 ("The 'special needs' of public employers may ... allow them to dispense with probable cause and warrant requirements when conducting workplace searches related to investigations of work-related misconduct")(citation omitted); *United States v. Fernandes*, 272 F.3d 398, 942 (7th Cir. 2001)("This court has held that a warrant or probable cause standard does not apply when a government employer conducts a search of its employees' offices, desks or files")(citation omitted); *United States v. Reilly*, 2002 U.S. Dist. LEXIS 9865 at *10 (S.D.N.Y. 2002)("Although the Fourth Amendment generally requires a warrant and probable cause, there are some well-established exceptions to these requirements. One such exception applies to the government's interest in the efficient and

Court outlined two basic categories of workplace searches: (1) Searches for work-related purposes (either non-investigatory or for the purpose of investigating workplace misconduct), and (2) searches for evidence of criminal violations. Each of these will be addressed in turn.

SEARCHES FOR WORK-RELATED PURPOSES

While "private citizens cannot [generally] have their property searched without probable cause ... in many circumstances government employees can."⁹⁷ Work-related searches typically fall within one of two similar, but distinct, circumstances. First, a search of a government employee's workspace may be conducted for a work-related, non-investigatory purpose, such as retrieving a needed file. "The governmental interest justifying work-related intrusions by public employers is the efficient and proper operation of the workplace."⁹⁸ Operational efficiency would suffer "if employers were required to have probable cause before they entered an employee's desk for the purpose of finding a file or piece of office correspondence."⁹⁹ For this reason, "public employers must be given wide latitude to enter employee offices for work-related, noninvestigatory reasons."¹⁰⁰

proper operation of a government workplace"); *Fink v. Ryan*, 174 Ill. 2d 302, 305 (1996), cert. denied, 521 U.S. 1118 (1997)(Noting the Supreme Court "has found the warrant and probable cause requirement impracticable in a variety of circumstances," including those involving "searches of government employees' desks and offices")

⁹⁷ *Rutan v. Republican Party of Illinois*, 497 U.S. 62, 94 (1990)(Scalia, J., dissenting)

⁹⁸ *Id.* at 723

⁹⁹ *Id.*

¹⁰⁰ *Id.*

Second, a search of an employee's workspace may be performed during an investigation into allegations of work-related misconduct, such as improper computer usage. As noted by the Supreme Court:

Public employers have an interest in ensuring that their agencies operate in an effective and efficient manner, and the work of these agencies inevitably suffers from the inefficiency, incompetence, mismanagement, or other work-related misfeasance of its employees. Indeed, in many cases, public employees are entrusted with tremendous responsibility, and the consequences of their misconduct or incompetence to both the agency and the public interest can be severe. ... In our view, therefore, a probable cause requirement for searches of the type at issue here would impose intolerable burdens on public employers. The delay in correcting the employee misconduct caused by the need for probable cause rather than reasonable suspicion will be translated into tangible and often irreparable damage to the agency's work, and ultimately to the public interest.¹⁰¹

¹⁰¹ *Id.* at 724

In either of the above situations, the search must be "reasonable" based on the totality of the circumstances.¹⁰² Generally, "a public employer's search of an area in which an employee had a reasonable expectation of privacy is 'reasonable' when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of its purpose."¹⁰³ Under this standard, the search must be (1) justified at its inception and (2) permissible in scope.¹⁰⁴

Justified At Inception

A supervisor's search of a government employee's office "will be 'justified at its inception' when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a non-investigatory, work-related purpose, such as to retrieve a needed

¹⁰² *Id.* at 725-26; *see also Fernandes*, 272 F.3d at 942 (Noting "government employers are subject to a reasonableness standard when they conduct workplace searches")(citation and internal brackets omitted); *Finkelstein v. State Personnel Bd.*, 218 Cal.App.3d 264, 268, 267 Cal.Rptr. 133 (1990)(Noting that "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")

¹⁰³ *Leventhal*, 266 F.3d at 73 (citation and internal quotation marks omitted)

¹⁰⁴ *Id.* at 726; *see also Brannen v. Board of Education*, 761 N.E.2d 84, 92 (Ohio 2001)("There is a two-part test to determine the reasonableness of a search conducted by a government employer. First, a court must consider whether the governmental action was justified at its inception. ... Second, the search as actually conducted must be reasonably related in scope to the circumstances that justified the interference in the first place")

file.”¹⁰⁵ Stated differently, a supervisor must have an articulable reason (or reasons) for believing that evidence of work-related misconduct or work-related materials are located in the place to be searched. This is essentially the “reasonable suspicion” standard introduced in *Terry v. Ohio*.¹⁰⁶

In *United States v. Simons*¹⁰⁷ (discussed in Part II, A, above), the employee’s computer was initially searched from a remote location, revealing over 1,000 picture files containing pornographic images. Approximately two weeks later, an individual “physically entered Simons’ office, removed the original hard drive, [and] replaced it with a copy”¹⁰⁸ No warrant had been obtained prior to this physical intrusion. While the court rejected Simons’ argument that he had a reasonable expectation of privacy in the computer (based on his employer’s Internet use policy), they noted the “entry into Simons’ office to retrieve the hard drive present[ed] a distinct question.” Unlike the computer itself, the court found Simons did have a reasonable expectation of privacy in his office.¹⁰⁹ The physical entry to retrieve the hard drive was a “search” implicating the Fourth Amendment. Accordingly, the court was required to determine whether the “warrantless entry into Simons’ office

to retrieve the hard drive was reasonable” Noting that *O’Connor* allowed a warrantless workplace search based on “a government employer’s interest in the ‘efficient and proper operation of the workplace,’”¹¹⁰ the court analyzed the physical entry into Simons’ office under that standard. The court found the search justified at its inception based on the information already in the hands of Simons’ employer at the time of the search. Specifically, “at the inception of the search, FBIS had ‘reasonable grounds for suspecting’ that the hard drive would yield evidence of misconduct because FBIS was already aware that Simons had misused his Internet access to download over a thousand pornographic images, some of which involved minors.”¹¹¹

In *Gossmeyer v. McDonald*¹¹² (discussed in Part I, above), the employee occupied a position that required her to investigate child sexual and physical abuse and to take photographs of the children for use in possible court proceedings. After an anonymous tip was received stating that Gossmeyer had “pornographic pictures of children in her file cabinet at work,”¹¹³ a warrantless search of Gossmeyer’s office, filing cabinet, storage unit, and desk was conducted. Some items were seized, but no charges were ever brought against her. Gossmeyer filed a lawsuit alleging the warrantless search violated her Fourth Amendment rights. In applying the *O’Connor* standard, the court initially addressed whether the search was justified at its inception. In finding that it was, the court relied on the following facts. First, while the search was initiated based upon an anonymous tip, the tip was sufficiently

¹⁰⁵ *Id.*

¹⁰⁶ 392 U.S. 1 (1968)

¹⁰⁷ 206 F.3d 392 (4th Cir. 2000), *cert. denied*, 534 U.S. 930 (2001)

¹⁰⁸ *Id.* at 396

¹⁰⁹ *Id.* at 399 (“Here, Simons has shown that he had an office that he did not share. As noted above, the operational realities of Simons’ workplace may have diminished his legitimate privacy expectation. However, there is no evidence in the record of any workplace practices, procedures, or regulations that had such an effect. We therefore conclude that, on this record, Simons possessed a legitimate expectation of privacy in his office”)(footnote omitted)

¹¹⁰ *Id.* at 400 (citation omitted)

¹¹¹ *Id.* at 401 (citation omitted)

¹¹² 128 F.3d 481 (7th Cir. 1997)

¹¹³ *Id.* at 485

reliable to justify the search that was ultimately conducted.

The informant identified herself as one of Gossmeier's co-workers in the Joliet office; made serious and specific allegations of misconduct - that Gossmeier had pornographic pictures of children; and stated where those pictures could be found - in Gossmeier's file cabinets and desk. The search took place one day after Farley received the tip and passed it on to the OIG. In addition, there was reason to believe that Gossmeier's cabinets were more likely than most to contain such pictures. She had unusual access to children and extraordinary authority (conferred by the state) to take such pictures.¹¹⁴

Additionally, Gossmeier's own duties supported the reasonableness of the search. She was the only person in the Joliet office who photographed and maintained pictures of abused children, which provided her an opportunity to commit the crimes alleged. Further, "the search was prompted by serious allegations of specific misconduct against an employee in a sensitive position."¹¹⁵ In the end, the "allegations called for prompt attention and ... the search was justified at its inception."¹¹⁶

Permissible In Scope

In order to be reasonable under the standard announced in *O'Connor*, the search must also be "permissible in scope." A search will be "permissible 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]."¹¹⁷ This means that the search may be made of only those areas where the item sought is reasonably expected to be located.

As an example, we can look once again at the *Simons* case. After receiving information that Simons had downloaded numerous pornographic images to his office computer, the hard drive of the computer was retrieved during a physical entry into Simons' office. This physical entry constituted a search, which the court analyzed under the *O'Connor* standard. As noted in the preceding section, the court found the physical intrusion to retrieve the hard drive justified at its inception. The court then addressed the second part of the reasonableness test, namely, whether the search was permissible in scope. In finding the scope of the search permissible, the court noted "the measure adopted, entering Simons' office, was reasonably related to the objective of the search, retrieval of the hard drive."¹¹⁸ The search was not found to be overly intrusive, because "there [was] no suggestion that Harper searched Simons' desk or any other items in the office; rather, [he] simply crossed the floor of Simons' office, switched hard drives, and exited."¹¹⁹

¹¹⁴ *Id.* at 491

¹¹⁵ *Id.*

¹¹⁶ *Id.*

¹¹⁷ *O'Connor*, 480 U.S. at 726 (plurality)

¹¹⁸ *Simons*, 206 F.3d at 401

¹¹⁹ *Id.*

In *Gossmeier*, the court also addressed whether the search of Gossmeier's office was permissible in scope. The court noted that "the targets of the search were those places where Gossmeier would likely store the alleged pornographic pictures."¹²⁰ Because the search "did not extend to places where the pictures would not reasonably have been found,"¹²¹ the court found it to be permissible in scope.

SEARCHES FOR EVIDENCE OF CRIMINAL VIOLATIONS

In *O'Connor*, the Supreme Court specifically declined to address the appropriate standard for searches when an employee is being investigated for criminal misconduct that does not violate some workforce policy.¹²² While not addressing the issue directly, the Court did comment on the distinction between criminal investigations and investigations into work-related misconduct. Specifically, the Court noted: "While police, and even administrative enforcement personnel, conduct searches for the primary purpose of obtaining evidence for use in criminal or other enforcement proceedings, employers most frequently need to enter the offices and desks of their employees for legitimate work-related reasons wholly unrelated to the illegal conduct."¹²³

¹²⁰ *Gossmeier*, 128 F.3d at 491

¹²¹ *Id.*

¹²² *O'Connor*, 480 U.S. at 723 ("Because the parties in this case have alleged that the search was either a noninvestigatory work-related intrusion or an investigatory search for evidence of suspected work-related employee misfeasance, we undertake to determine the appropriate Fourth Amendment standard of reasonableness *only* for these two types of employer intrusions and leave for another day inquiry into other circumstances")(emphasis in original)

¹²³ *Id.* at 721

Several lower courts have addressed the standard required for searches conducted solely for the purpose of obtaining criminal evidence, and found that "[t]he rationale for the lesser burden *O'Connor* places on public employers is not applicable for [public employers] engaged in a criminal investigation."¹²⁴ Thus, a public employer "may not cloak itself in its public employer robes in order to avoid the probable cause requirement when it is acquiring evidence for a criminal prosecution." Where the sole motivation behind a workplace search is to uncover evidence of criminal wrongdoing, the appropriate standard is probable cause.¹²⁵ In such situations, "the crucial question is not whether the investigation involves actions arising out of a [public employee's] duties, but whether the investigation's objective is to discipline the [employee] within the department or to seek criminal prosecution."¹²⁶

"DUAL-PURPOSE" SEARCHES

While the standards set out above appear relatively clear, there are often situations in which a government employee's misconduct might well fit into both the work-related misconduct and criminal violation categories. For example, a government employee may be receiving and downloading child pornography from a government computer. While clearly criminal in nature, this conduct also could (and most likely does) constitute a violation of workforce policy rules on appropriate government computer/Internet usage. In

¹²⁴ *Taketa*, 923 F.2d at 675

¹²⁵ *See, e.g., United States v. Jones*, 286 F. 3d 1146, 1151 (9th Cir. 2002)("The *O'Connor* standard is not applicable to federal agents engaged in a criminal investigation")

¹²⁶ *Cerrone v. Fresenius*, 246 F.3d 194, 200 (2d Cir. 2001)

such a situation, a supervisor really has two purposes in conducting a search: to uncover evidence of the administrative violation, and to uncover potential criminal evidence. In such situations, the question becomes obvious: When a government supervisor receives information that an activity is occurring that violates both workforce regulations and criminal statutes, what standard must be followed when searching the employee's workspace? Because of the work-related misconduct that is occurring, will the lesser standard of *O'Connor* suffice? Or, because of the criminal nature of the allegations, must the traditional probable cause and warrant requirements be met? "[T]he courts have adopted fairly generous interpretations of *O'Connor* when confronted with mixed-motive searches."¹²⁷

As an example, we can once more look to the *Simons* case for guidance. The court upheld the search of the Simons' office using the "reasonableness" standard set out in *O'Connor*. More importantly, the court noted they were doing so, even "assum[ing] that the dominant purpose of the warrantless search ... was to acquire evidence of criminal activity."¹²⁸

Nevertheless, the search remains within the *O'Connor* exception to the warrant requirement; FBIS did not lose its special need for "the efficient and proper operation of the workplace," merely because the evidence

obtained was evidence of a crime. Simons' violation of FBIS' Internet policy happened also to be a violation of criminal law; this does not mean that FBIS lost the capacity and interests of an employer.¹²⁹

Similarly, in *United States v. Reilly*,¹³⁰ the defendant was accessing child pornography from his government computer, a clear violation of both the Department of Labor's computer use policy and federal statutes. During a search of his cubicle, two diskettes were seized from the defendant, both of which were later found to contain child pornography. At trial, the defendant moved to suppress both diskettes, claiming the warrantless search and seizure violated his Fourth Amendment rights. The defendant claimed the seizure of the diskettes was not truly part of an investigation into work-related misconduct, because the agency was aware of his administrative violations prior to the seizure of the diskettes and could have taken action against him without seizing them. The defendant argued the search was actually made for the sole purpose of uncovering evidence of criminal violations, which would require probable cause and a warrant. In denying his motion to suppress, the District Court held the search of the diskettes fell within *O'Connor's* "work-related misconduct" exception. "Agent Wager's dual role as an investigator of workplace misfeasance and criminal activity does not invalidate the otherwise legitimate workplace search."¹³¹

¹²⁷ *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Computer Crime and Intellectual Property Section, Criminal Division, Department of Justice at 45 (March 2001)

¹²⁸ *Simons*, 206 F.3d at 400

¹²⁹ *Id.* (internal quotations and citations omitted)

¹³⁰ *Supra* at note 51

¹³¹ *Id.* at 9881

SUMMARY

A search of a government employee's workplace must comply with the Fourth Amendment. In addressing these situations, a two-part analysis can be used. First, it must be determined whether the employee had a reasonable expectation of privacy in the area searched. In making this determination, factors relied upon by courts include whether prior notice was provided to the employee; common practices of the agency; the openness and accessibility of the area; the position of the employee; and whether the employee waived his expectation of privacy. If the employee does not have a reasonable expectation of privacy in the area searched, the Fourth Amendment is not implicated. If a reasonable expectation of privacy does exist, then the purpose behind the search must be analyzed. A search for work-related purposes (either non-investigatory or for work-related misconduct) must be reasonable based on the totality of the circumstances. To qualify as reasonable, the search must be (1) justified at its inception, and (2) permissible in scope. If the search is made to solely uncover evidence of criminal misconduct, then probable cause and a search warrant are required, unless an exception to the warrant requirement of the Fourth Amendment exists (e.g., consent). In situations where the search is conducted for dual purposes, courts have been fairly generous in finding that the "special needs" rules announced in *O'Connor* apply.