Public Privacy: Warrantless Workplace Searches of Public Employees

Bryan R. Lemons†

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; a 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 some of these questions in O'Connor v. Ortega,1 it has fallen to lower courts to address many 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.2 If a reasonable expectation of privacy

† Mr. Lemons is the Branch Chief of the Legal Division at the Federal Law Enforcement Training Center for Border and Transportation Security, a division of the Department of Homeland Security.

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
does exist, then any search that ensues must be reasonable under the totality of the circumstances.\textsuperscript{3} Before turning to those issues, however, it is necessary to first define exactly what is meant by the term "workplace."

I. 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."\textsuperscript{4} This would include such areas as offices, desks, filing cabinets, computers, and government vehicles. However, "[n]ot everything that passes through the confines of the business address can be considered part of the workplace context . . . ."\textsuperscript{5} 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, "[t]he 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."\textsuperscript{6} This is not to say, of course, that a public employee's personal property can \textit{never} be included within the workplace context. In fact, just the opposite is true. While "a court is more apt to find an employee has standing to challenge the seizure of personal items or the search of an area where personal items are stored than the search or seizure of work-related documents or materials,"\textsuperscript{7} a public employee's private property may still, in certain rare circumstances, fall within the scope of a "workplace" search. This generally occurs where an employee is put on notice that his or her property can be searched as part of the workplace environment,\textsuperscript{8} or in situations where the employee is using the personally-owned property in the workplace to significantly assist the employee in carrying out his or her official duties.\textsuperscript{9}

For example, in the Ninth Circuit Court of Appeals case of \textit{United

\textsuperscript{3} Id. ("Second, if a reasonable expectation of privacy exists, the Fourth Amendment requires that the search be reasonable under all the circumstances.")
\textsuperscript{4} O'Connor, 480 U.S. at 715.
\textsuperscript{5} Id. at 716.
\textsuperscript{6} Id.
\textsuperscript{7} United States v. Anderson, 154 F.3d 1225, 1231 (10th Cir. 1998).
\textsuperscript{8} See, e.g., United States v. Broadus, 7 F.3d 460, 463-64 (6th Cir. 1993) (upholding search of employee's jacket placed in locker where the employee had signed a waiver explaining that lockers were "subject to inspection at any time by authorized personnel" (quotations omitted)).
\textsuperscript{9} See, e.g., Gossmeyer v. McDonald, 128 F.3d 481, 490 (7th Cir. 1997) (upholding search of storage unit and filing cabinet where the employee had purchased the items and brought them into the workplace to store work-related items).
WARRANTLESS WORKPLACE SEARCHES

States v. Gonzalez,\(^{10}\) the defendant was an employee of a military exchange. Upon leaving work, he was stopped by a store detective, who sought permission to search Gonzalez’s personal backpack.\(^{11}\) 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.\(^{12}\) Approximately $15.00 worth of stolen spark plugs were found in the backpack.\(^{13}\) After his motion to suppress this evidence was denied, Gonzalez pleaded guilty to larceny, but reserved his right to appeal.\(^{14}\) 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.\(^{15}\) Instead, the court noted that 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.\(^{16}\) Thus, “Gonzalez’s expectation of privacy was limited by his knowledge of the store policy of searching employees’ belongings to deter and apprehend theft.”\(^{17}\)

A similar result was reached by the Seventh Circuit Court of Appeals in Gossmeyer v. McDonald.\(^{18}\) Gossmeyer 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.”\(^{19}\) Because of a lack of storage space, Gossmeyer, at her own expense, purchased two separate storage devices.\(^{20}\) Specifically, she bought a four-drawer filing cabinet, in which she kept “evidentiary photographs, photographic equipment, files, and documents,”\(^{21}\) and a two-door storage unit, in which she kept various items. When a local detective received an anonymous tip from one of Gossmeyer’s co-workers stating that Gossmeyer had pornographic pictures in these cabinets, the detective notified the DCFS Office of Inspector General.\(^{22}\) The next day, officials conducted a warrantless search of Gossmeyer’s office, filing cabinet, storage unit, and

\(^{10}\) 300 F.3d 1048 (9th Cir. 2002).
\(^{11}\) Id. at 1050.
\(^{12}\) Id.
\(^{13}\) Id.
\(^{14}\) Id.
\(^{15}\) Id. at 1052.
\(^{16}\) Id.
\(^{17}\) Id. at 1054.
\(^{18}\) 128 F.3d at 490.
\(^{19}\) Id. at 484.
\(^{20}\) Id.
\(^{21}\) Id.
\(^{22}\) Id. at 485.
desk and seized some items. No charges were ever brought against Gossmeyer; however, she brought a lawsuit alleging the warrantless search violated her Fourth Amendment rights. Gossmeyer asserted that because she had personally bought the 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 Gossmeyer bought them herself.” As noted by the court: “The cabinets were not personal containers which just happened to be in the workplace; they were containers purchased by Gossmeyer primarily for the storage of work-related materials. . . . These items were part of the ‘workplace,’ not part of Gossmeyer’s personal domain.”

II. 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. 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.” Government employees can, and often do, establish expectations of privacy in their government offices, desks, computers, and filing cabinets. 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.,

23. Id.
24. Id. at 486.
25. Id. at 487.
26. Id. at 490.
27. Id.
29. Leventhal v. Knapec, 266 F.3d 64, 73 (2d Cir. 2001); Voyles v. State, 133 S.W. 3d 303, 305 (Tex. Ct. App. 2004) (“A defendant has standing to challenge the admission of evidence obtained by an intrusion by the government or a private individual only if he had a legitimate expectation of privacy in the place invaded.”).
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." A government employee's expectation of privacy is limited by the "operational realities of the workplace," and "whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." Although government ownership of the property to be searched (e.g., a government-owned computer assigned to a government employee) is an "important consideration," it does not, standing alone, dictate a finding that no reasonable expectation of privacy exists. Courts have found that "[a]pplicability 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." Courts have considered a variety of factors when determining whether a government employee has a reasonable expectation of privacy in his or her workspace. The discussion below describes some of the most important factors.

A. 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." 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.”

United States v. Simons 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.” 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.”

The court found that the language of the policy, “placed employees on

37. COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, U.S. DEP’T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, [hereinafter SEARCHING AND SEIZING] 32 (2002); see also United States v. Thorn, 375 F.3d 679, 683 (8th Cir. 2004) (finding employee had no expectation of privacy in use and contents of office computer where he “was fully aware of the computer-use policy, as evidenced by his written acknowledgment of the limits imposed on his computer-access rights”); State v. Meredith, 56 P.3d 943, 949 (Or. 2002) (Kistler, J. dissenting) (citations omitted):

To be sure, the operational realities of the workplace may limit the scope of an employee’s privacy rights. And the fact that a government employer tells its employees in advance that it will be monitoring their use of the office computers or phones can be an important factor in the analysis.


A company can legitimately regulate the use of its property and is entitled to adopt policies and practices which place restrictions and conditions on the personal use of computer equipment. Employees have no objectively reasonable basis to believe that their activities on a company computer are private when, through the company’s screen notification, they have actual knowledge that the computer can be searched and, through posted company policies and e-mail notifications, either know or should know they possess no expectation of privacy associated with the information they store in or send through these systems.

39. Simons, 206 F.3d at 396.

40. Id. at 398.
notice that they could not reasonably expect that their Internet activity would be private.\footnote{Id.}

A similar result was reached by the Seventh Circuit Court of Appeals in \textit{Muick v. Glenayre Electronics}.\footnote{280 F.3d 741 (7th Cir. 2002).} 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.\footnote{Id. at 742.} Although Muick was ultimately convicted for receipt and possession of child pornography, he brought a lawsuit against Glenayre. He claimed that they had violated his Fourth Amendment rights by seizing the computer and turning it over to the federal officers because the computer contained "'proprietary and privileged personal financial and contact data.'\footnote{Id. (citations omitted).} 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."\footnote{Id. at 743.} So, for example, "[i]f 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."\footnote{Id. (citations omitted). 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 . . . ."\footnote{Id. (citations omitted.)} As stated by the court:

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.\footnote{Id.}
Likewise, in *State v. Francisco*, 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. Upon receiving information that Francisco was distributing cocaine, a 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 Departmental vehicles (to avoid claims of privacy expectations)." This section provided, in part, that "all departmental vehicles shall be subject to search and inspection by the Sheriff or his designated representative at anytime, day or night." Departmental vehicles, as defined by the section, included "all enclosed containers."

While courts have consistently found that "legitimate regulation" in the form of an agency or departmental policy can eliminate an employee's expectation of privacy, at least one court has suggested that although the existence of a policy "weighs heavily in the determination of the reasonableness of the search," it is not dispositive. In *DeMaine v. Samuels*, the plaintiff was a Connecticut State Trooper who filed a federal civil rights lawsuit pursuant to Title 42 U.S.C. Section 1983 alleging his Fourth Amendment rights had been violated. At the time of the events in question, the CONNECTICUT STATE POLICE ADMINISTRATION AND OPERATIONS MANUAL [hereinafter A&O MANUAL] provided, in pertinent part, that "the Department reserves the right to inspect issued equipment at any other time for reasonable purposes," and "[t]he personal property of a trooper located on department property or within a department vehicle is subject to inspection or seizure without notice even if the trooper has locked any container or place where the property is kept." During an internal affairs investigation into overtime abuses, information was

50. *Id.* at 544.
51. *Id.* at 545.
52. *Id.* at 544.
53. *Id.*
54. *Id.*
56. *Id.*
57. *Id.* at *3-4.
uncovered that led investigators to believe DeMaine may have had notes in his possession regarding the activities of other officers that would be vital to the investigation. In due course, investigators searched DeMaine's computer, desk, government-issued vehicle, and personal day planner. None of these searches were conducted pursuant to a warrant. In his lawsuit, DeMaine claimed the searches violated his Fourth Amendment rights. The defendants moved for summary judgment, arguing that, based on the language contained in the A&O Manual, DeMaine had no reasonable expectation of privacy in the places searched. Although the court granted the motion for summary judgment, it noted:

[T]he fact that the A&O Manual authorizes searches of police-issued equipment at any time for reasonable purposes and any personal property located on or within department property, including a state-issued automobile, weighs heavily in the determination of the reasonableness of the search here. However, the existence of the policy does not, on its own, dispose of the question.  

Nevertheless, the court found DeMaine had no reasonable expectation of privacy in his computer. Here, the court relied in part on the fact that "all state employees had notice that their use of state computers was subject to monitoring." The court also found that "[g]iven the regulation and the fact that the desk was state property," DeMaine had no reasonable expectation of privacy in his desk. As for his government-issued vehicle, the court found no reasonable expectation of privacy existed because, among other things, "the A&O regulation clearly provided that the car and all items within it were subject to search at any time." While the court did find that DeMaine had an expectation of privacy in his day planner, the search of that item by the investigators was found to be permissible for reasons that are discussed more fully in Part III.

Finally, while policies and regulations may destroy a public employee's expectation of privacy in a government workplace, where an agency has contradictory or unclear policies and directives, that fact may actually assist an employee in establishing an expectation of privacy. For example, in Zaffuto v. City of Hammond, the Hammond, Louisiana police department automatically recorded all calls on certain telephone lines to a

58. Id. at *23.
59. Id. at *24.
60. Id. at *25.
61. Id. at *26.
62. 308 F.3d 485 (5th Cir. 2002).
central taping system. A police officer sued his supervisor for illegally recording a telephone call the officer made from his (the officer's) private office. In defense, the supervisor claimed that "a department policy that calls would be taped" made it "not be objectively reasonable for [the officer] to expect privacy in making a personal phone call from work." However, three police officers, including Zaffuto, testified that "they understood the policy to mean that only calls coming into the communications room (where outside citizens would call) were being recorded, not calls from private offices." Based on this testimony, the court determined that a "reasonable juror could conclude . . . that Zaffuto expected that his call to his wife would be private, and that that expectation was objectively reasonable."

Similarly, in *Haynes v. Office of Attorney General Kline*, the plaintiff was hired as an Assistant Attorney General. During an orientation he was given when hired, Haynes was informed that his government computer "had two files: private and public," and that "he could put personal information in the private file and that no one would have access to it." Additionally, he was notified that "he should put other documents concerning his work in the public file." However, the computers at the Attorney General's office also displayed a computer usage policy when they were turned on. Among other things, the policy noted that "[t]here shall be no expectation of privacy in using this system; however, intentional access to another user's e-mail without permission shall be prohibited . . . ." Within nine months of accepting the job, Haynes was terminated. Afterwards, "employees of the Attorney General's office retrieved and reviewed information contained on [Haynes's] computer, including personal e-mails."

Haynes filed a motion for a preliminary injunction, in which he asserted that members of the Attorney General's office had violated his Fourth Amendment rights by reviewing the personal information he had stored on his government computer. In response, the defendants claimed that no Fourth Amendment violation had occurred because Haynes had no expectation of privacy on the computer in light of the express statement displayed when the machine was turned on ("There shall be no expectation

63. Id. at 486.
64. Id. at 489.
65. Id.
66. Id.
68. Id. at 1157.
69. Id.
70. Id. at 1158.
71. Id.
of privacy in using this system\textsuperscript{72}). While finding that the computer use policy "obviously [had] considerable significance,"\textsuperscript{73} the court ultimately concluded that whether Haynes had an expectation of privacy remained an open question based on the contradictory information he had received:

The court, however, must consider this fact in conjunction with the other information provided in the policy as well as the oral representations made by AG employees to the plaintiff. These other facts, suggest that plaintiff's expectation of privacy was objectively reasonable. . . . The facts that we have learned include the following: employees are allowed to use their work computers for private communications; employees are told how to create "public" and "private" files; employees are advised that "intentional access to another user's e-mail without permission" is prohibited; employees are given passwords to prevent others from gaining access to their computers; and there was no evidence that any AG official had ever monitored or viewed any private files, documents or e-mails of any employee.\textsuperscript{74}

B. **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 procedures . . . ."\textsuperscript{75} 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.\textsuperscript{76} For example, in the Third Circuit

---

\textsuperscript{72}. *Id.* at 1162.

\textsuperscript{73}. *Id.*

\textsuperscript{74}. *Id.*

\textsuperscript{75}. *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) (plurality opinion); see also *Gillard v. Schmidt*, 579 F.2d 825, 829 (3d Cir. 1978) ("[A] employer may conduct a search in accordance with a regulation or practice that would dispel in advance any expectations of privacy." (citation omitted)); *People v. Neal*, 486 N.E.2d 898, 901 (Ill. 1985) (upholding the search of government-issued vehicle and raincoat where police officer had no expectation of privacy, in part, because these items "were subject to periodic inspections by the defendant's superiors under the policy and practice of the Illinois State Police," and "the defendant was aware of such inspections and the manner in which they were conducted"); *Moore v. Constantine*, 594 N.Y.S.2d 395, 397 (N.Y. App. Div. 1993) (affirming the search of police officer's locker where trooper "had no reasonable expectation of privacy from his superiors who routinely obtained access to the work-related contents of petitioner's locker.").

\textsuperscript{76}. See, e.g., *Leventhal v. Knapke*, 266 F.3d 64, 74 (2d Cir. 2001) (finding that an 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").
Court of Appeals case of United States v. Speights, 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.” While there had been scattered instances of inspections of the lockers for cleanliness (three or four in twelve years), “there [was] insufficient evidence to conclude that the police department practice negated Speights'[sic] otherwise reasonable expectation of privacy.”

Other federal courts, in analogous cases, have reached parallel conclusions. For example, in United States v. Donato, 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.” In Shaffer v. Field, the search of a police officer’s locker was upheld in part because three previous searches had been conducted in the past. In Schowengerdt v. United States, 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 of workspaces by security guards.” In each of these cases, the courts “relied on specific regulations and practices in finding that an expectation of privacy was not reasonable.” Alternatively, in United States v. Taketa,

77. 557 F.2d 362 (3d Cir. 1977).  
78. Id. at 364.  
79. Id.  
81. Id. at 923.  
82. 339 F. Supp. 997 (C.D. Cal. 1972), aff’d, 484 F.2d 1196 (9th Cir. 1973).  
83. Id. at 1003.  
84. 944 F.2d 483, 488 (9th Cir. 1991).  
85. Id. at 485.  
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 was not subjected to regular visits of inspection by [agency] personnel."^88

C. 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.^89 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.^90 For example, "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."^91 Similarly, the "use of passwords and locking office doors to restrict an employer's access to computer files is evidence of the employee's subjective expectation of privacy in those files."^92 Where an employee is the only individual to have a key to the area in question, that

---

87. 923 F.2d 665 (9th Cir. 1991).
88. Id. at 673.
89. See Stewart v. Evans, 351 F.3d 1239, 1243 (D.C. Cir. 2003) (finding that employee had no expectation of privacy in a safe where the employee "had no control whatever over access to the office containing the safe or to the safe itself"); People v. Holland, 591 N.Y.S.2d 744, 747 (N.Y. Crim. Ct. 1992):

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.

90. See United States v. Taketa, 923 F.2d 665, 671 (9th Cir. 1991) ("[A] reasonable expectation of privacy [exists] in an area 'given over to [an employee's] exclusive use.'"); Voyles v. State, 133 S.W.3d 303, 350 (Tex. Ct. App. 2004) (holding that an employee had no reasonable expectation of privacy over work computer where, inter alia, he did not have "complete dominion and control" over the computer and it was "available for use by [other] substitute teachers").
91. McGregor v. Greer, 748 F. Supp. 881, 888 (D.C. Cir. 1990); see also Holland, 591 N.Y.S. 2d at 746 ("[I]t is clear that an individual employee has an expectation of privacy in a locked, private office . . . .").
92. United States v. Bailey, 272 F. Supp. 2d 822, 835 (D. Neb. 2003); see also United States v. Slanina, 283 F.3d 670, 676 (5th Cir. 2002) (finding that employee demonstrated subjective expectation of privacy over his office and computer where door to office was closed and locked and passwords had been installed on the computer), remanded on other grounds, 537 U.S. 802, vacating judgment and remanding, 313 F.3d 891 (5th Cir. 2002).
factor, while perhaps not dispositive, would weigh in favor of the employee having an expectation of privacy.\footnote{3}

Alternatively, the more accessible the item or area is to others, the less likely an individual employee’s claim of privacy would be accepted.\footnote{4} Among the factors to consider in such a determination would include (a) whether the employee shared the area with anyone else, (b) whether others could be expected to enter the area or disturb papers in it without permission, (c) whether the employee took normal precautions customarily taken by those seeking privacy; and (d) whether the employee put the item or area to some private use.\footnote{5} 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.”\footnote{6} Additionally, where areas are, by their very nature, “open” and “public,” no

\footnote{3. United States v. Chaves, 169 F.3d 687, 691 (11th Cir. 1999) (holding that an employee who had only key to warehouse had a “measure of control and ability to exclude others” that resulted in finding of expectation of privacy). Nevertheless, the court noted in Chaves that “possession of a key, without more, might not be sufficient to establish a reasonable expectation of privacy.” \textit{Id.} at 691.}

\footnote{4. \textit{See, e.g., United States v. Thorn,} 375 F.3d 679, 684 (8th Cir. 2004) (finding that employee’s expectation of privacy in office, desk and filing cabinet “was limited in scope because other . . . employees had keys that allowed them to access the office and the contents of the desk and cabinets”); Luellen v. City of East Chicago, 350 F.3d 604, 612 n.5 (7th Cir. 2003) (suggesting, but not deciding, that employee likely could not have established expectation of privacy in government vehicle where (a) vehicle was owned and maintained by fire department; (b) vehicle was assigned to position, not employee personally; (c) fire department retained a key to vehicle; (d) Fire Chief testified vehicle could be inspected on his permission; and (e) Fire Chief had authorized such an inspection in the past); United States v. Hamdan, 891 F. Supp. 88, 95 (E.D.N.Y. 1995), \textit{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 Thornton v. Univ. Civil Serv. Merit Bd., 507 N.E.2d 1262, 1266 (Ill. App. Ct. 1987) (holding that there is no expectation of privacy for police officer where, \textit{inter alia}, “[t]he police department office was used by all . . . police officers to conduct police business and was not plaintiff’s private office”); State v. McLellan, 744 A.2d 611 (N.H. 1999); Shaul v. Cherry Valley-Springfield Cent. Sch. Dist., 218 F. Supp. 2d 266, 270 (N.D.N.Y. 2002) (holding that teacher had no 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”).}


\footnote{6. \textit{O’Connor,} 480 U.S. at 717-18 (plurality opinion); see also \textit{Holland,} 591 N.Y.S.2d at 746-47 (“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.”).}
reasonable expectation of privacy can exist in that area. So, for example, a public employee would not generally have an expectation of privacy in the common hallway of a business, because of its open access to visitors and other employees of the business.

Nevertheless, the fact that others may be permitted access to an employee’s office, desk, computer, or filing cabinet does not, standing alone, automatically destroy an employee’s privacy expectation. As one court has noted: “Privacy does not require solitude.” For example, “a private space (such as a desk) within an otherwise public space (such as a government building) will justify an expectation of privacy.” Additionally, the existence of a master key will not defeat an employee’s expectation of privacy in his or her office, nor will an employee’s failure to consistently shut and lock an office door automatically sacrifice any expectation of privacy in that area.

Illustrative on this concept is Coats v. Cuyahoga Metropolitan Housing Authority, 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 unzippered case. A Housing Authority police officer arrived, searched the

97. Thompson v. Johnson County Cmty. Coll., 930 F. Supp. 501, 507 (D. Kan. 1996) aff’d, 108 F.3d 1388 (10th Cir. 1997) (“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.”); O’Bryan v. KTIV Television, 868 F. Supp. 1146, 1159 (N.D. Iowa 1994) (holding that, where an unlocked desk or credenza was located in an “open, accessible area,” no reasonable expectation of privacy existed).

98. Gillespie v. Dallas Hous. Auth., No. 3:01-CV-895-R, 2003 U.S. Dist. LEXIS 29, at *22-23 (N.D. Tex. Jan. 2, 2003) (where video camera was mounted in a common hallway, the court noted that the employee “would certainly have no objectively reasonable expectation of privacy in the common hallway” because “[b]eing an undifferentiated area, all employees used the common hallway”).

99. See United States v. Slanina, 283 F.3d 670, 676 (5th Cir. 2002) (noting that, where employee had a private office, “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.’”) (citation omitted), remanded on other grounds by, 537 U.S. 802 (2002).

100. United States v. Taketa, 923 F.2d 665, 673 (9th Cir. 1991).

101. Caldarola v. County of Westchester, 343 F.3d 570, 575 (2d Cir. 2003).

102. Taketa, 923 F.2d at 673 (“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 hotel, office, or apartment occupant.”).

103. Id. (“Nor was the expectation of privacy defeated by O’Brien’s failure to shut and lock his door at all times.”).

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’[sic] 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’[sic] cubicle telephone line. Accordingly, Coats did not have a reasonable expectation of privacy in the cubicle itself. Thus, the entry of the cubicle . . . did not violate Coats’[sic] Fourth Amendment protections.105

In Brannen v. Kings Local School District Board of Education,106 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.”107 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 time.” The break room was so open to fellow employees that the custodians could not have a reasonable expectation of privacy in this area.108

105. Id. at *10-11.
107. Id. at 91.
108. Id. at 91-92.
On the other hand, the Second Circuit Court of Appeals case of Leventhal v. Knapek\(^{109}\) 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."\(^{110}\) 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.\(^{111}\)

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.'"\(^{112}\)

D. 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

\(^{109}\) 266 F.3d 64 (2d Cir. 2001).
\(^{110}\) Id. at 74.
\(^{111}\) Id. at 73-74.
\(^{112}\) Id. at 74 (citation omitted).
Likewise, where an employee is part of an industry that is subjected to pervasive regulation to ensure the safety and fitness of its employees, any expectation of privacy the employee might have may be reduced. As noted by the Supreme Court: "[I]t 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." This is especially true where the subject of the search is a law enforcement officer. In cases 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." While law enforcement officers do not lose their constitutional rights by virtue of accepting their position, 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." This "interest in police integrity . . . may justify some intrusions on the privacy of police officers which the Fourth Amendment would not otherwise tolerate."

A case on point is Biehunik v. Felicetta, involving allegations of police brutality. After several citizens were severely beaten by a large group of police officers, the police commissioner ordered sixty two police officers involved in the case to be subject to routine personal searches when they leave the workplace every day. See, e.g., Petersen v. City of Mesa, 83 P.3d 35, 41 (Ariz. 2004) ("[I]ndividuals who elect to become firefighters should anticipate a diminished expectation of privacy and should reasonably expect some intrusion into matters involving their health and fitness."); Chicago Fire Fighters Union, Local 2 v. City of Chicago, 717 F. Supp. 1314, 1318 (N.D. Ill. 1989) ("[T]he highly regulated nature of the fire department serves to lower the expectation of privacy of individual fire fighters.").
officers to participate in a lineup for investigative purposes. The officers moved to prevent the lineup, claiming that it violated their constitutional rights. In rejecting the officers' argument, the Second Circuit Court of Appeals noted, "policemen, who voluntarily accept the unique states 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." 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."

A similar result was reached by the same court, albeit in a different context, in Sheppard v. Beerman. 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 regards to the desk, the court relied upon the unique "working relationship between a judge and her law clerk."

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 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."

E. 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 Court of Appeals case of American Postal Workers Union v. United States Postal Service, postal employees were

121. Id. at 231.
122. Id.
123. 18 F.3d 147 (2d Cir. 1994).
124. Id. at 152.
125. Id.
126. 871 F.2d 556 (6th Cir. 1989).
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." 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." Finally, the collective bargaining agreement for these employees "provided for random inspection of the lockers under specified circumstances." 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."

Similarly, in *United States v. Bunkers*, 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." 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 nine 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 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 ... .  

---

127. *Id.* at 557.
128. *Id.*
129. *Id.*
130. *Id.* at 560.
131. 521 F.2d 1217 (9th Cir. 1975).
132. *Id.* at 1219.
133. *Id.*
134. *Id.* at 1221 (citation omitted).
III. IF A REASONABLE EXPECTATION OF PRIVACY DOES EXIST, WAS THE SEARCH REASONABLE?

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.¹³⁵ "[T]he Fourth Amendment protects individuals from unreasonable searches conducted by the Government, even when the Government acts as an employer."¹³⁶ Generally speaking, when searches are performed, courts have expressed a strong preference that they be performed pursuant to warrants.¹³⁷ 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.¹³⁸ 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."¹³⁹ 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

¹³⁵. See, e.g., 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.'") (citing California v. Ciraolo, 476 U.S. 207, 213 (1986)).
¹³⁷. 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").
¹³⁸. 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 exceptions") (emphasis in original) (citation omitted).
operation of the workplace." 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 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.

Accordingly, the Court has carved out an exception to the probable cause and warrant requirements for public employers, noting "[t]he 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." In O'Connor, the Supreme Court outlined two basic categories of workplace searches: (1) Searches for work-related purposes (either non-investigatory or for the purpose of investigating workplace

---

141. Id. at 721-22.
142. Id. at 725 (internal quotation marks and citation omitted); see also Leventhal v. Knapec, 266 F.3d 64, 73 (2d Cir. 2001) ("The 'special needs' of public employers may . . . allow them to dispense with the 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 918, 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, No. 01 CR 1114 (RPP), 2002 U.S. Dist. LEXIS 9685, at *10 n.2 (S.D.N.Y. May 31, 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 proper operation of a government workplace."); Fink v. Ryan, 673 N.E.2d 281, 284 (Ill. 1996), (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").
misconduct), and (2) searches for evidence of criminal violations. Each of these will be addressed in turn.

A. Searches for Work-Related Purposes

For the *O'Connor* exception to apply, the search in question must be work-related. "This element limits the *O'Connor* exception to circumstances in which the government actors who conduct the search act in their capacity as employers, rather than law enforcers." While "private citizens cannot [generally] have their property searched without probable cause . . . in many circumstances government employees can." 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." 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." For this reason, "public employers must be given wide latitude to enter employee offices for work-related, noninvestigatory reasons."

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

143. **SEARCHING AND SEIZING**, *supra* note 37, at 34.
146. *Id.* at 723.
147. *Id.* at 723.
damage to the agency's work, and ultimately to the public interest.\footnote{148}

In either of the above situations, the search must be “reasonable” based on the totality of the circumstances.\footnote{149} 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.”\footnote{150} Under this standard, the search must meet two requirements: (1) the search must be justified at its inception, and (2) the search must be permissible in scope.\footnote{151} This is the equivalent of the “reasonable suspicion” standard outlined by the Supreme Court in \textit{Terry v. Ohio}.\footnote{152}

1. 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 noninvestigatory work-related purpose such as to retrieve a needed file.”\footnote{149} 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.

\footnote{148} \textit{Id.} at 724.  
\footnote{149} \textit{Id.} at 725-26; \textit{see also} United States v. Fernandes, 272 F.3d 938, 942 (7th Cir. 2001) (noting “government employers are subject to a reasonableness standard when they conduct workplace searches” (citation and internal brackets omitted)); Finkelstein v. State Personnel Bd., 267 Cal. Rptr. 133, 135 (Cal. Ct. App. 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”).  
\footnote{150} Leventhal v. Knapek, 266 F.3d 64, 73 (2d Cir. 2001) (citation and internal quotation marks omitted).  
\footnote{151} O’Connor v. Ortega, 480 U.S. 709, 726 (1987); \textit{see also} Brannen v. Board of Education, 761 N.E.2d 84, 92 (Ohio Ct. App. 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.”).  
\footnote{152} 392 U.S. 1 (1968); \textit{see also} Wiley v. Dep’t of Justice, 328 F.3d 1346, 1351 (Fed. Cir. 2003) (noting Supreme Court has found “workplace searches undertaken either for noninvestigatory work-related purposes or to investigate work-related misconduct may be predicated on reasonable suspicion rather than probable cause”).  
\footnote{153} \textit{O’Connor}, 480 U.S. at 726.
In United States v. Simons\textsuperscript{154} (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...."\textsuperscript{155} No warrant had been obtained prior to this physical intrusion. While the court rejected Simons’ argument that he had a reasonable expectation of privacy regarding 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.”\textsuperscript{156} Unlike the computer itself, the court found Simons did have a reasonable expectation of privacy in his office.\textsuperscript{157} 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,’”\textsuperscript{158} 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.”\textsuperscript{159}

In Gossmeyer v. McDonald\textsuperscript{160} (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,”\textsuperscript{161} a warrantless search of Gossmeyer’s office, filing cabinet, storage unit, and desk was conducted. Some items were seized, but no charges

\textsuperscript{154.} 206 F.3d 392 (4th Cir. 2000).
\textsuperscript{155.} Id. at 396.
\textsuperscript{156.} Id. at 399.
\textsuperscript{157.} Id. (“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)).
\textsuperscript{158.} Id. at 400 (citation omitted).
\textsuperscript{159.} Id. at 401 (citation omitted).
\textsuperscript{160.} 128 F.3d 481 (7th Cir. 1997).
\textsuperscript{161.} Id. at 485.
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 reliable to justify the search that was ultimately conducted.

The informant identified herself as one of Gossmeyer's co-workers in the Joliet office; made serious and specific allegations of misconduct—that Gossmeyer had pornographic pictures of children; and stated where those pictures could be found—in Gossmeyer'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 Gossmeyer'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.162

Additionally, Gossmeyer'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."163 In the end, the "allegations called for prompt attention and . . . the search was justified at its inception."164

Finally, in *Williams v. Philadelphia Housing Authority*,165 the plaintiff was placed on leave of absence by his employer, the Philadelphia Housing Authority (PHA). Prior to leaving, however, Williams had been asked to remove his personal belongings from the work desk he used. A search of the desk by Williams' employer (Galeota) during his absence revealed a computer disk that, upon review, was found to contain both PHA legal documents and some of Williams' personal items. Williams claimed ownership of the disk, but his request for its return was denied by PHA. PHA did offer to provide a copy of the disk to Williams, but he refused. He then filed suit alleging his Fourth Amendment rights had been violated by the seizure and retention of the disk. The court rejected this claim. In deciding that the *O'Connor* "reasonableness" standard was the one to be applied in this case, the court noted:

---

162. *Id*. at 491.
163. *Id*.
164. *Id*.
[E]mployers most often enter their employees' work area for work-related reasons and not for reasons related to misconduct. For example, an employer may need to retrieve a file or report from the office of an employee who is away from the office in order to complete a task. Thus, in order to maintain efficiency and productivity, the [Supreme] Court has granted employers wide latitude to enter employers' offices for work-related, non-investigative reasons.  

Here, Williams failed to satisfy the first requirement of the O'Connor "reasonableness" standard. Specifically, he failed to present evidence that the search was not "justified at its inception." Williams himself acknowledged in his complaint that Galeota was acting in her "official capacity" when she seized the computer disk. Accordingly, said the court, "Galeota merely exercised her discretion in maintaining efficiency and productivity in the workplace. Galeota reasonably located the disk in order to distribute the vacated workload to the remaining attorneys." Thus, because the seizure of the computer disk was made for an official, work-related purpose, the seizure was "justified at its inception."

2. 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 its 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].'" 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 discussed in Part II A. 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,

166. Id. at 954.
167. Id.
whether the search was permissible in scope. In finding the scope of the search permissible, the court noted "[t]he measure adopted, entering Simons’ office, was reasonably related to the objective of the search, retrieval of the hard drive." 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."

In Gossmeyer, the court also addressed whether the search of Gossmeyer’s office was permissible in scope. The court noted that "[t]he targets of the search were those places where Gossmeyer would likely store the alleged pornographic pictures." Because the search "did not extend to places where the pictures would not reasonably have been found," the court found it to be permissible in scope.

B. 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. While not addressing the issue directly, the Court did comment on the distinction between criminal investigations and investigations into work-related misconduct: "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."

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

171. Id.
172. Gossmeyer v. McDonald, 128 F.3d 481, 491(7th Cir. 1997).
173. Id.
174. 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.

175. Id. at 721.
Thus, a public employer "cannot 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. Of course, "[t]he line between a legitimate work-related search and an illegitimate search for criminal evidence is clear in theory, but often blurry in fact." This is especially true in situations where the personnel conducting the search are members of an agency or department that is undeniably "in the business of investigating the violation of the criminal laws, which is a critical distinction from the situation presented to the Court in O'Connor. However, the mere involvement of law enforcement personnel will not automatically convert a work-related search into a criminal investigation. 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." Stated differently, "in looking to ascertain whether the investigation is criminal in nature, the proper focus is not on the positions or capabilities of the persons conducting the search, but rather the reason for the search itself." Among the factors considered by courts in making

176 United States v. Taketa, 923 F.2d 665, 675 (9th Cir. 1991).
177 Id.
178 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.").
179 SEARCHING AND SEIZING, supra note 37, at 35.
180 O'Connor, 480 U.S. at 722.
181 United States v. Slanina, 283 F.3d 670, 679 (5th Cir. 2002) (noting several federal circuit courts of appeal have upheld "searches by law enforcement personnel into work-related misconduct... under the O'Connor standard.").
182 Cerrone v. Brown, 246 F.3d 194, 200 (2d Cir. 2001); see also Lowe v. City of Macon, 720 F. Supp. 994, 998 (M.D. Ga. 1989), aff'd without opinion, 925 F.2d 1475 (11th Cir. 1991) ("It is the purpose behind the search which is controlling as to which standard, probable cause, or reasonable suspicion will be applied.").
183 Wiley v. Dep't of Justice 328 F.3d 1346, 1352 (Fed. Cir. 2003); see also United States v. Fernandes, 272 F.3d 938, 943 n.3 (7th Cir. 2001) (stating search ordered by prosecutor should be analyzed under O'Connor standard because it was not ordered as part of a criminal investigation, but rather was necessary to "'ensure that the work of the agency [was] conducted in a proper and efficient manner'" (alteration in original)); Gossmeyer v. McDonald, 128 F.3d 481, 492 (7th Cir. 1997) (noting that presence of OIG investigators during work-related misconduct search did not transform search into unlawful criminal investigation); Shields v. Burge, 874 F.2d 1201 (7th Cir. 1989) (analyzing search by internal affairs investigators under O'Connor, even though parallel criminal investigation was being conducted). But see Rossi v. Town of Pelham, 35 F. Supp. 2d 58, 65 (D.N.H. 1997) (stating that O'Connor exception was inapplicable where police officer searched town official's office; court noted "'[t]he status of the searcher, whether police officer or supervisor, bears on the constitutional reasonableness of a warrantless search of a public employee's private
this determination include whether a criminal investigation has been opened, whether a workforce policy was violated, and the position of the individual who conducted the search.

For example, in *United States v. Hagarty*, the defendant, a criminal investigator for the Internal Revenue Service, had been convicted of perjury based upon evidence gleaned from a listening device secretly installed without a warrant in another government employee’s office as part of a separate investigation. Hagarty appealed his conviction, claiming that the evidence obtained from the eavesdropping device violated his Fourth Amendment rights. In response, the government asserted, among other things, “that the Fourth Amendment [did] not apply to the search of government premises in the course of an investigation relating to the conduct of governmental business.” The Seventh Circuit Court of Appeals rejected the government’s argument. The court noted the eavesdropping was not intended to “supervise and investigate” Hagarty’s duties, but “was designed to detect [the] criminal activity” of another employee. Further, this was not a search “for ‘official property needed for official use’ or for anything belonging to the Government.” Instead, “this eavesdropping was part of an effort to secure evidence of crime,” and was “precisely the kind of search by policemen . . . against which the constitutional prohibition was directed.” Consequently, the evidence obtained from the eavesdropping device was obtained in violation of the Fourth Amendment.

Likewise, in *United States v. Kahan*, the defendant worked for the Immigration and Naturalization Service. Suspecting that Kahan was violating federal law, a criminal investigation was begun. As part of that investigation, daily searches of a wastebasket in Kahan’s office were conducted, resulting in various pieces of evidence being recovered. None of these searches were made pursuant to a warrant. At his trial, Kahan claimed the evidence had been seized in violation of the Fourth Amendment. The court agreed. Here, a supervisor or employee was not “looking for some needed document or record and inadvertently [happen] upon incriminating evidence in the desk or wastebasket of another employee.” Further, this was not a situation “where a supervisor [was]
inspecting the area used by a subordinate in order to examine his work or to evaluate his performance on the job.\textsuperscript{191} Instead, this was a "specifically focused investigation of the suspected criminal activities of an employee in the course of his employment . . ."\textsuperscript{192} In such cases,

\begin{quote}
[T]he supervisor's role is no longer that of a manager of an office, but that of a criminal investigator for the government. The purpose of the supervisor's surveillance is no longer simply to preserve efficiency in the office. It is specifically designed to prepare a criminal prosecution against the employee. In that case, searches and seizures by the supervisor or by other government agents are governed by the Fourth Amendment admonition that a warrant be obtained in the absence of exigent circumstances.\textsuperscript{193}
\end{quote}

\section*{C. 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 have a criminal dimension to it, thereby falling 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 such a situation, a public employer really has two purposes in conducting a search: (1) to uncover evidence of the administrative violation, and (2) to uncover potential criminal evidence. The question then 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 \textit{O'Connor} suffice? Or, because of the criminal nature of the allegations, must the traditional probable cause and warrant requirements be met? "The courts have adopted fairly generous interpretations of \textit{O'Connor} when confronted with mixed-motive searches."\textsuperscript{194}

\begin{footnotes}
\item[191.] Id.
\item[192.] Id.
\item[193.] Id.
\item[194.] United States v. Slanina, 283 F.3d 670, 678 (5th Cir. 2000) (holding \textit{O'Connor} standard applicable where misconduct investigation had criminal elements, because "\textit{O'Connor}'s goal of 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."); \textit{SEARCHING AND SEIZING}, supra note 37, at 35.
\end{footnotes}
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." 195

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. 196

Similarly, in United States v. Reilly, 197 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." 198

IV. 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

196. Id. (internal quotations and citations omitted).
197. 01 Cr. 1114 (RPP), 2002 U.S. Dist. LEXIS 9865, at *1 (S.D.N.Y. May 31, 2002).
198. Id. at *15-16.
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 solely to 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'Conner apply.