WORKPLACE SEARCH AND SEIZURE

MARY E. BAKER, *Houston*
Harris County Attorney's Office

State Bar of Texas
29TH ANNUAL
ADVANCED GOVERNMENT LAW
July 27-28, 2017
Austin

CHAPTER 6

MARY E. BAKER
Senior Assistant County Attorney
Harris County Attorney's Office
1019 Congress, 15th Floor
Houston, Texas 77002
(713) 274-5133
(713) 755-8924 (Fax)

BIOGRAPHICAL INFORMATION

EDUCATION

B.A. in English, Cum Laude, Canisius College
J.D., Fordham University School of Law

PROFESSIONAL ACTIVITIES

Senior Assistant County Attorney, Harris County Attorney's Office, 1996 to present
Secretary, Board of Directors, Solon Academy, 2003-2004
State Bar of Texas
Bar of the State of New York
Member, Texas District and County Attorney's Association
Member, Houston Bar Association

PUBLICATIONS, ACADEMIC APPOINTMENTS AND HONORS

Adjunct Instructor, Harris County Sheriff's Academy, 2008-present (Basic Peace Officer School, Officer Involved Shootings, Arrest, Search and Seizure)
Adjunct Instructor, Katy Independent School District Police Department (Qualified Immunity) -2012 to Present
Speaker, Texas District and County Attorney's Association (Officer Involved Shootings and Section 1983 Update)

TABLE OF CONTENTS

I. INTRODUCTION 1

II. THE FOURTH AMENDMENT 1

III. THE REASONABLE EXPECTATION OF PRIVACY 1

IV. SEARCH OF A PRIVATE SECTOR EMPLOYEE BY THE GOVERNMENT 2

V. THE PUBLIC SECTOR EMPLOYEE AND THE FOURTH AMENDMENT 4

VI. RECOMMENDATIONS FOR THE GOVERNMENT EMPLOYER 11

WORKPLACE SEARCH AND SEIZURE

I. INTRODUCTION

This article will examine the Fourth Amendment rights of an employee, whether public or private, with regard to a search of his or her workplace. The article reviews the employee's reasonable expectation of privacy in the workplace, and considers the factors applied by the courts to determine whether that expectation is one which society regards as reasonable. The article will also address the factors applied by the courts in determining whether a search violated the Fourth Amendment.

II. THE FOURTH AMENDMENT

The Fourth Amendment to the United States Constitution provides:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The core of the Fourth Amendment its to safeguard the privacy and security of individuals against arbitrary intrusions by government officials. The Fourth Amendment gives concrete expression to the right of the people which "is basic to a free society." *Wolf v. People of the State of Colo.*, 338 U.S. 25, 27 (1949). The Fourth Amendment protects society from two specific governmental intrusions: searches and seizures. A "search" occurs when an expectation of privacy that society is prepared to consider is reasonable is infringed. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984), *citing Smith v. Maryland*, 442 U.S. 735, 739-741 (1979); *Terry v. Ohio*, U.S. 1, 9 (1968). A "seizure" of property occurs when there is some meaningful interference with an individual's possessory interests. *United States v. Place*, 462 U.S. 696 (1983) (BRENNAN, J., concurring in result). The Fourth Amendment proscribes only government action; it is wholly inapplicable to a search or seizure, even an unreasonable one, by a private individual not acting as an agent of the government or with the participation or knowledge of any governmental official. *Walter v. United States*, 447 U.S. 649, 662 (1980) (BLACKMAN, J. dissenting). The Fourth Amendment is enforceable against the States through the Fourteenth Amendment. *Ker v. State of Cal.*, 374 U.S. 23, 30 (1963).

While the literal protections of the Fourth Amendment apply to an individual's person, house, papers and effects, the Supreme Court has held that the word "houses" is not to be taken literally. The protection of the Fourth Amendment may extend to a commercial premises. *See v. City of Seattle*, 387 U.S. 541 (1967); *Go-Bart Importing Co. v. United State*s, 282 U.S. 344 (1931). An employee may also have a reasonable expectation of privacy in his or her business office. *Oliver v. United States*, 466 U.S. 170, 178 n.8 (1984); ("The Fourth Amendment's protection of offices and commercial buildings, in which there may be legitimate expectations of privacy … is based on societal expectations that have deep roots in the amendment."); *Hoffa v. United States*, 385 U.S. 293, 301 (1996). The Fourth Amendment does not shield only those with title to a searched premises. Standing to challenge a Fourth Amendment search is conferred even on an individual who is legitimately present on the premises where a search occurs if the fruits of the search are to be used against him or her. *Jones v. United States*, 362 U.S. 257 (1960).

We are accustomed to applying the Fourth Amendment right to be free from unreasonable searches and seizures to the criminal investigative process. In that context, a search conducted without a warrant is presumptively unreasonable. *Dow Chemical Co. v. United States*, 476 U.S. 227, 234-235 (1986). It is well settled, however, that the Fourth Amendment's protection extends beyond the sphere of criminal investigations. *Camara v. Mun. Court of County of San Francisco*, 387 U.S. 523, 530 (1967). The Fourth Amendment "… guarantees the privacy, dignity and security of persons against certain arbitrary and invasive acts by officers of the government, without regard to whether the government actor is investigating crime or performing another function." *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2627 (2010), citing *Skinner v. Railway Labor Executive' Ass'n*, 489 U.S. 602, 613-614 (1989).

This article addresses the application of the Fourth Amendment in the workplace, whether in the public or private sector. We will closely examine the case law which addresses the application of the Fourth Amendment to the public workplace, *i.e.*, when the government itself is the employer.

III. THE REASONABLE EXPECTATION OF PRIVACY

The concept of an individual's reasonable expectation of privacy is fundamental to the Fourth Amendment analysis. *Katz v. United States*, 389 U.S. 347 (1967) introduced the concept of the reasonable expectation of privacy. In *Katz*, Petitioner was convicted in the federal district court for the Southern District of California under an eight count indictment charging him with transmitting wagering information by telephone from Los Angeles to Boston and Miami in violation of a federal statute. At trial, the Government

was permitted, over Katz's objection, to introduce evidence of Katz's end of the telephone conversations in which the wagering information was transmitted. These telephone conversations had been overheard by FBI agents, who had attached an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls. The FBI agents failed to obtain a warrant to place the bug. Affirming his conviction, the Ninth Circuit rejected Katz's contention that the recordings were obtained in violation of the Fourth Amendment, because the FBI had not physically placed the bug inside the telephone booth itself. The Supreme Court reversed Katz's conviction, holding that the Fourth Amendment protects people not places. It commented, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. *See Lewis v. United States*, 385 U.S. 206, 201, *United States v. Lee*, 274 U.S. 559, 563. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. *See Rios v. United States*, 364 U.S. 253; *Ex parte Jackson*, 96 U.S. 727, 733." *Katz, Id* at 351-352.

The Government argued that the fact that the telephone booth from which Katz made his calls was constructed partly of glass made Katz as visible when he entered the telephone booth as he would have been had he remained outside, and that thus, the Fourth Amendment was not implicated. *Katz, Id.* at 352. Dismissing this argument, the Supreme Court noted, "But what [Katz] sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment or in a taxicab, a person in a telephone booth may rely on the protection of the Fourth Amendment." *Katz, Id*. at 352.

Katz makes it clear that standing to claim the protection of the Fourth Amendment does not depend upon an individual having a property right in the invaded place. Rather, an individual's standing it depends on whether the area was one in which there was a reasonable expectation of freedom from governmental intrusion. *See Katz, Id*. at 352. A legitimate expectation of privacy is established when the claimant can show (1) a subjective expectation of privacy in the object of a challenged search; and (2) an objectively reasonable expectation of privacy. *Smith v. Maryland*, 442 U.S. 735 (1979). It was on this basis that the law with regard to an employee's reasonable expectation of privacy developed. *See e.g., Jones v. Houston Cmty, Coll. Sys.*, 816 F. Supp. 2d 418, 432 (S.D. Tex. 2011)(a reasonable expectation of privacy exists when: (1) a person "manifest[s] a subjective expectation of privacy in the object of the challenged search; and (2) "society [is] willing to recognize that expectation as reasonable.", *citing California v. Ciraolo*, 476 U.S. 207, 211 (1986)).

IV. SEARCH OF A PRIVATE SECTOR EMPLOYEE BY THE GOVERNMENT

The rules for conducting warrantless searches and seizures in private-sector workplaces generally mirror the rules for conducting warrantless searches in homes and other personal residences. Private sector employees generally retain a reasonable expectation of privacy in their workplaces. As a result, searches by law enforcement of a private workplace will usually require a warrant unless the agents obtain the consent of the employee, the employer or a co-worker with common authority.

As discussed above, employees may have a reasonable expectation of privacy in their business offices. *See Oliver, Id.* at 178 n.8; *Hoffa, Id.* at 301. The Supreme Court addressed that issue in *Mancusi v. DeForte*, 392 U.S. 364 (1968). In *Mancusi*, the respondent, Frank DeForte, a vice president of Teamsters Union Local 266, was indicted in Nassau County, New York. Alleging that he had misused his union office to organize owners of juke boxes and compel them to pay tribute, DeForte was charged with conspiracy, coercion and extortion. Prior to the return of the indictment, the Nassau County District Attorney's Office issued a subpoena duces tecum to Local 266, requiring the production of certain books and records. The subpoena was served on the Union at its offices. When the Union refused to comply, the state officials who had served the subpoena conducted a search and seized the union records from an office shared by DeForte and several other union officials. The search and seizure was conducted without a warrant, and took place over the protests of DeForte, who was present at the time. At trial, over DeForte's objection, the seized material was admitted against him and he was convicted. *Mancusi, Id.* at 365.

Relying on the Court's decision in *Katz*, the *Mancusi* Court identified the proper inquiry as whether the area which had been searched –DeForte's office— was one in which DeForte had a reasonable expectation of freedom from government intrusion. It stated, "The crucial issue, therefore, is whether, in light of all the circumstances, DeForte's office was such a place." *Mancusi, Id*. at 368.

The record revealed that the office where DeForte worked consisted of one large room, which he shared with several other union officials. The parties stipulated that DeForte spent a "considerable amount of time" in the office. DeForte had custody of the papers at the moment of their seizure. The Court pointed out that although DeForte shared the office with several other union officials, he could reasonably have expected that only these individuals and their personal or business guests would enter the office. The Court found that

DeForte could reasonably have expected that records would not be touched except with the permission of the other occupants of the office, or of union "higher ups". *Mancusi, Id.* at 369. On that basis, and in those circumstances, the Court held that DeForte had Fourth Amendment standing to object to the admission of the seized papers against him at trial. *Mancusi, Id.* at 369.

The Supreme Court further held that the search of DeForte's office was unreasonable within the meaning of the Fourth Amendment. The state did not deny that it conducted the search without a warrant. The subpoena issued by the Nassau County District Attorney's Office did not qualify as a search warrant as it was issued by the District Attorney himself and not by a neutral magistrate. Accordingly, the judgment of the Second Circuit, which directed that a writ of habeas corpus issue on DeForte's behalf, was affirmed. *Mancusi, Id.* at 365.

United States v. Ziegler, 474 F.3d 1184 (9th Cir. 2007) also addresses the Fourth Amendment issues involved in the search of an employee's workplace computer. *Ziegler* involved the criminal prosecution of an employee of Frontline Processing ("Frontline"), a company which services internet merchants by processing on-line electronic payments. On January 30, 2001, Anthony Cochenour, the owner of Frontline's internet-service provider, contacted FBI Special Agent James A. Kennedy, Jr. with a tip that a Frontline employee had accessed child pornography websites from a workplace computer. Agent Kennedy pursued the report that day. He first contacted Frontline's IT administrator, John Softich ("Softich"), whose duties included monitoring Frontline's employee use of workplace computers, including their internet access. Softich informed Kennedy that Frontline had a firewall,[1] which permitted constant monitoring of the employees' internet activities. During the interview, Softich confirmed Kennedy that a Frontline employee had accessed child pornography via the Internet, and informed to Kennedy that the sites were accessed from a computer in the office of Jeffrey Ziegler ("Ziegler"), Frontline's director of operations. Softich informed Kennedy that the IT department had placed a monitor on Ziegler's computer to record its internet traffic by copying its cache files. *Ziegler, Id.* at 1185.

Kennedy next interviewed William Schneider, Softich's subordinate in Frontline's IT department. He confirmed that the IT department had placed a device in Ziegler's computer which would record his internet activity, and that Schneider had "spot checked" Ziegler's cache files and uncovered several images of child pornography. The evidence established that Frontline owned and routinely monitored all workplace computers and that the employees were aware of the IT Department's monitoring activities. *Ziegler, Id.* at 1186.

Kennedy, Softich and Schneider disagree about what happened next. Softich and Schneider testified that Kennedy instructed them to make a copy of Ziegler's hard drive because he feared it might be tampered with before the FBI was able to make an arrest. Kennedy denied that he directed the Frontline employees to do anything, and testified that it was his understanding that the IT department had already made a backup copy of Ziegler's hard drive. Kennedy testified that he instructed Softich only to be sure that no one could tamper with the backup copy. About 10:00 p.m., Softich and Schneider obtained a key to Ziegler's private office from Frontline's chief financial officer, entered the office, opened Ziegler's computer's outer casing and made two copies of the hard drive. Several days later Frontline delivered Ziegler's computer tower, with the original hard drive and one of the hard drive copies made by Schneider and Softich to the FBI. Forensic examiners at the FBI discovered many images of child pornography and on May 23, 2003, Ziegler was indicted on three counts of receipt and possession of child pornography and obscene material. *Ziegler, Id.* at 1187.

Ziegler filed a motion to suppress the evidence obtained from the search of his workplace computer. He argued that Kennedy acted without a warrant in violation of the Fourth Amendment, by directing Softich and Schneider to enter his private office and search his computer. The government argued that the search was voluntary and therefore private in nature. Arguing that the workplace computer is similar to the desk drawer or file cabinet given Fourth Amendment protection in *O'Connor v. Ortega*, 480 U.S. 709 (1987),[2] Ziegler also contended that the search was conducted at the behest of Kennedy, who was "undeniably" seeking evidence of a crime. *Ziegler, Id.* at 1187. In response, the government argued:

> "Society could not deem objectively reasonable that privacy interest where an employee uses a computer paid for by the company; [sic] Internet access paid for by the company, in the company office where the company pays the rent….This is certainly

[1] A firewall is a piece of "computer hardware or software which prevents unauthorized access to private data (as on a company's local area network or intranet) by outsider computer users. *Merriam-Webster's Collegiate Dictionary* 471 (11th ed. 2003) The firewall can also be "programmed to analyze the network traffic flowing between [a] computer and the Internet"; it then "compares the information it monitors with a set of rules in its database" and [i]f it sees something not allowed…the firewall can block and prevent the action." *Newton's Telecom Dictionary* 392 (22nd ed. 2006).

[2] As will be discussed *infra.*, *O'Connor* is a case involving the search of a public employee's workplace, including desk and file cabinet

> even more so true where the company has installed a firewall and a whole department of people whose job it was to monitor their employee's internet activity. "

Ziegler, Id. at 1188-1189. The government did not contest Ziegler's claim that he had a subjective expectation of privacy in his office and computer. The Court held that the use of a password on his computer and the lock on his private office were sufficient evidence of Ziegler's subjective expectation of privacy. *Ziegler, Id*., *citing United States v. Bailey*, 272 F. Supp. 2d 822, 835 (D. Neb. 2003).

The Ninth Circuit held, however, that Ziegler's expectation of privacy in his office and workplace computer must also have been objectively reasonable. Citing *Mancusi*, the Ninth Circuit acknowledged that in the private employer context, employees retain at least some expectation of privacy in their offices. *Ziegler, Id.* at 1189, *citing Mancusi, Id* at 730. The Ninth Circuit thus held that Ziegler had a reasonable expectation of privacy in his office, and that therefore any search of that space and the items located therein must comply with the Fourth Amendment. *See Ziegler, Id*. at 1189.

The next step was to inquire whether there was a search or seizure by the government. Softich and Schneider were treated by the Ninth Circuit as "de facto" government agents and the Court concluded that a search occurred. ("The employees obtained a key in order to unlock the office, entered the office, copied Ziegler's hard drive, and left.") *Ziegler, Id*. at 1190. The remaining question, then was whether the search of Ziegler's office and the copying of his hard drive were unreasonable within the meaning of the Fourth Amendment. Distinguishing *Mancusi*, the Ninth Circuit held that the search of Ziegler's office was conducted with consent of his employer.

Voluntary consent is an exception to the rule that for purposes of the Fourth Amendment, except in certain carefully defined classes of cases, a search of private property without consent is unreasonable unless it has been authorized by a valid search warrant. *Mancusi, Id.* at 370. *See also Davis v. United States*, 328 U.S. 582 (1946). The government may prove consent by proving that permission to search was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected. *United Sates v. Matlock*, 415 U.S. 164 (1974).

Here, the Court held that Frontline exercised common authority over the office and the workplace computer such that it could validly consent to a search of Ziegler's office and computer.[3] For example, although use of each Frontline computer was subject to an individual log-in, Schneider and other IT department employees had complete administrative access to any employee's machine. Frontline had also installed a firewall to monitor its employees' internet traffic from within the organization. Monitoring was routine, and the IT department reviewed the log created by the firewall on a regular basis. Finally, upon hiring, each Frontline employee was apprised of its monitoring efforts through training and an employment manual, and they were told that the computers were company-owned and were not to be used for activities of a personal nature. *Ziegler, Id.* The Ninth Circuit concluded: "In this context, Ziegler could not reasonably have expected that the computer was his personal property, free from any type of control by his employer. The contents of his hard drive were work related items that contained business information and which were provided to, or created by, the employee in the context of the business relationship. Ziegler's downloading of personal items to the computer did not destroy Frontline's common authority." Accordingly, the district court's order denying suppression of the evidence of child pornography existing on Ziegler's computer was affirmed. *Ziegler, Id*. at 1193

Mancusi holds that a private employee may have a subjective expectation of privacy in his or her workplace and various items located therein. If it is determined that the employee's subjective explanation of privacy is reasonable, then it must be determined whether the subjective expectation of privacy is one that society is prepared to accept as objectively reasonable. *California v. Greenwood*, 486 U.S. 35, 39 (1988). In the case of an employee in the private sector, such as we found in *Ziegler,* the employer may be able to consent to the search of the employee's office, computer and effects. *See also, Mancusi, Id.* at 369.

V. THE PUBLIC SECTOR EMPLOYEE AND THE FOURTH AMENDMENT

The Fourth Amendment, applied to the States through the Fourteenth Amendment, has been applied to the conduct of governmental officials in various civil activities. *New Jersey v. T.L.O.*, 469 U.S. 325 (1985). For example, the Fourth Amendment governs the conduct of school officials, *see ibid*., building inspectors, *see Camara, Id.*, 387 U.S. at 528, and Occupational Safety and Health Act inspectors. *Marshall v. Barlow's, Inc*., 436 U.S. 307, 312-313 (1978). In *T.L.O.*, the Supreme Court noted that "[b]ecause the individual's interest in privacy and

[3] Although in *Mancusi* no consent to the search was given by the union or any of its officials, the Supreme Court recognized that even where a private employee retains an expectation that his private office will not be the subject of an unreasonable government search, the employee's interest is subject to the possibility of an employer's consent to the search of the premises. *Mancusi, Id.* at 369.

personal security 'suffers whether the government's motivation is to investigate violations of criminal laws or breaches of other statutory or regulatory standards'…it would be 'anomalous to say that the individual and his private property are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior." *T.L.O., Id.* at 335 (quoting *Marshall v. Barlow's, Inc).*

O'Connor v. Ortega, 480 U.S. 709 (1987), is the leading case on the Fourth Amendment rights of public employees. In *O'Connor*, the Supreme Court addressed two issues concerning those rights. First, it addressed the reasonable expectation of privacy of a public employee in his office, desk and file cabinets. Second, it addressed the appropriate Fourth Amendment standard for a search conducted by a public employer in an area in which a public employee is found to have a reasonable expectation of privacy. *O'Connor, Id.* at 716.

The facts in *O'Connor* are as follows. Dr. Magno Ortega, a physician and psychiatrist at a state hospital, held the position of Chief of Professional Education for seventeen years, until his dismissal from that position in 1981. He had primary responsibility for training young physicians in psychiatric residency programs. In July, 1981, hospital officials, including Dr. Dennis O'Connor, the hospital's Executive Director, became concerned about possible improprieties in Dr. Ortega's management of the residency program. They were concerned about his acquisition of an Apple II computer, with charges that Dr. Ortega had sexually harassed two female hospital employees, and with a charge that Dr. Ortega had taken inappropriate disciplinary action against a resident. *O'Connor, Id.* at 712.

On July 30, 1981, Dr. O'Connor requested that Dr. Ortega take paid administrative leave during the investigation of these charges. Dr. Ortega was permitted to take two weeks of vacation instead, but was requested to stay off hospital property for the duration of the investigation. On August 14, 1981, Dr. O'Connor informed Dr. Ortega that the investigation had not yet been completed and that he was being placed on paid administrative leave. Dr. Ortega remained on paid administrative leave until his employment was terminated on September 22, 1981. *O'Connor, Id*. at 713.

The investigation was conducted by several hospital personnel, including an accountant, a physician and a hospital security officer. The Hospital Administrator, Richard Friday ("Friday"), led the investigative team. At some point during the investigation, Friday decided to enter Dr. Ortega's office. The search of Dr. Ortega's office was "quite thorough". *O'Connor. Id.* at 713. The investigators entered Dr. Ortega's office a number of times and seized several items from his desk and file cabinets, including a Valentine's Day card, a photograph and a book of poetry sent to Dr. Ortega by a former resident physician. These items were later used in a proceeding before a hearing officer of the California State Personnel Board to impeach the credibility of the former resident, who testified on Dr. Ortega's behalf. No formal inventory of the property in the office was ever made, although the justification advanced for the search was that it was a routine inventory of state property in the office of a terminated employee. However, at the time of the search, Dr. Ortega had not yet been terminated. *O'Connor, Id*. at 713.

The Supreme Court first addressed the issue as to whether Dr. Ortega, a public employee, had a reasonable expectation of privacy in his office, desk and file cabinets. In its plurality opinion, the Court first delineated the boundaries of the workplace context, defining it as "…those areas and items that are related to work and are generally within the employee's control." *O'Connor, Id. at 715-716.* Rejecting the Solicitor General's argument that public employees can never have a reasonable expectation of privacy in their workplace, the Court noted that individuals do not lose Fourth Amendment rights "..merely because they work for the government instead of a private employer." *O'Connor Id*. at 719. In its plurality opinion, the Court held that: "The operational realities of the workplace…may make some employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. Public employees' expectations of privacy in their offices, desks and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." *O'Connor, Id.* at 719. The Court's plurality opinion holds that because it is the nature of government offices that fellow employees, supervisors, consensual visitors and the general public may have frequent access to an individual's office, the question of whether the public employee has a reasonable expectation of privacy in his or her workplace must be addressed on a case-by-case basis. *O'Connor, Id.* at 719.

Addressing this case, the plurality held that Dr. Ortega had a reasonable expectation of privacy in his desk and file cabinets. The evidence disclosed that Dr. Ortega did not share his desk or file cabinets with any other employees. He had occupied the office for seventeen years, and he kept materials in his office which included personal correspondence, medical files, correspondence from private patients unconnected to the hospital, personal financial records, teaching aids and notes and personal gifts and mementos. The files relating to the residents whom he supervised were kept outside Dr. Ortega's office. *O'Connor, Id*. at 724.

The Court next addressed the appropriate Fourth Amendment standard of reasonableness to be applied to a public employer's work –related search of its

employee's office, desk or file cabinet. Acknowledging that the legitimate privacy interests of public employees in private objects they bring to the workplace may be substantial, the Court noted that the "realities of the workplace" must be balanced against those interests. *O'Connor, Id.* at 720. Contrasting the work of law enforcement personnel, who conduct searches for the primary purpose of obtaining evidence for use in criminal or other enforcement proceedings, with that of a government employer, the Court noted that "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." *O'Connor, Id*. at 722. Thus, the Court held that requiring an employer to obtain a warrant whenever the employer wished to enter an employee's office, desk or file cabinet for a work-related purpose would seriously disrupt the routine conduct of government business and would be unduly burdensome. *O'Connor, Id.* at 722.

The Court held 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 circumstances, and not by the standard of probable cause. Under the reasonableness standard, both the inception and the scope of the intrusion must be reasonable. Citing *Terry v. Ohio*, the Court held that a two fold inquiry is required to determine reasonableness of the search. First, one must consider whether the search was justified at its inception. Second, one must determine whether the search as actually conducted 'was reasonably related in scope to the circumstances which justified the interference in the first place." *O'Connor, Id*. at 723, *quoting T.L.O., Id.* A search will normally be reasonable 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." *O'Connor, Id.* at 726. The 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 the light of … the nature of the misconduct." *O'Connor, Id.* at 724, *quoting TLO, Id.* at 351.

Although there are a number of situations in which a government employer would have occasion to intrude to some extent on an employee's expectation of privacy, the Court addressed only the two presented by the facts in the search of Dr. Ortega's office. Dr. O'Connor characterized the search as a noninvestigatory work-related intrusion. Dr. Ortega claimed that the search was an investigatory search for evidence of suspected work-related employee malfeasance. The Court found the governmental interest justifying work-related intrusions by public employers is the efficient and proper operation of the workplace, and the provision of myriad services to the public. Because the work of a government agency would suffer if a government employer were required to have probable cause before entering an employee's desk to find a file or a piece of office correspondence, the plurality opined that public employers must be given "wide latitude" to enter employee offices for work-related, noninvestigatory reasons. *O'Connor, Id*. at 724.

The Court came to a similar conclusion for searches conducted pursuant to an investigation of work-related employee misconduct. The Court also opined that a probable cause requirement for an investigation of work-related employee misconduct would impose an "intolerable burden" on public employers. It held, therefore, that public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for the investigation of work-related misconduct, should be judgement by the standard of reasonableness. *O'Connor, Id.* at 726. The Supreme Court held that in view of the factual issues, summary judgment was inappropriate. It reversed the judgment of the Court of Appeals, and remanded to that court for further proceedings in view of its opinion. *O'Connor, Id.* at 729.

Concurring in the judgment, Justice Scalia disagreed with the reason for the reversal given by the plurality opinion and with the standard it prescribes for the Fourth Amendment inquiry. Noting that the plurality opinion instructs the lower courts that the existence of Fourth Amendment protection for a public employee's office is to be assessed on a case by case basis, in light of whether the office is "so open to fellow employees or the public that no expectation of privacy is reasonable." *O'Connor, Id.* at 730. *Citing Mancusi*, Justice Scalia continued that the constitutional protection against unreasonable searches by the government does not disappear because the government has the right to make reasonable intrusions in its capacity as employer. For that reason, he would hold that the offices of government employees, including the drawers and files within those offices, are covered by Fourth Amendment protections as a general matter. *O'Connor, Id.* at 731. With respect to the issue as to whether the government intrusion was reasonable, in T.L.O., the Supreme Court recognized that it had recognized exceptions when "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable…". *T.L.O., Id*. at 351. Justice Scalia would hold that such "special needs" are present in government employment, and thus, that government searches to retrieve work-related materials or to investigate violations of workplace rules do not violate the Fourth Amendment. *O'Connor, Id*. at 732.

The Supreme Court next addressed the issues relating to a search of a public employee's workplace in *City of Ontario v. Quon*, 560 U.S. 746 (2010)(Stevens J., and Scalia, J. concurring). The facts in *Quon* were as follows. The City of Ontario ("the City") acquired pagers which were able to send and receive text messages. Its contract with its service provider, Arch Wireless, provided for a monthly limit on the number of characters each pager could send or receive, and specified that usage exceeding that number would result in an additional fee. The City issued the pagers to Quon, a police officer and member of the Ontario Police Department's ("OPD") Special Weapons and Tactics ("SWAT") team. *Quon, Id.* at 750.

Before acquiring the pagers, the City announced a computer usage, internet and email policy ("the Computer Policy") which applied to all employees. Among other provisions, it specified that the City "reserves the right to monitor and log all network activity including e-mail and internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." In March, 2000, Quon signed a statement acknowledging that he had read and understood the Computer Policy. *Quon, Id.* at 751.

On its face, the Computer Policy did not apply to the use of text messages. However, the City made it clear to its employees, including Quon, that it would treat text messages the same way it treated e-mails. This was reiterated at a meeting on April 18, 2001 at which Quon was present. There, he was told that text messages sent on the City's pagers are considered e-mail messages, which means that the messages would fall under the City's policy as public information and would be eligible for auditing. These comments were also reiterated in writing by the Chief of Police. *Quon, Id.* at 751-752.

Within the first or second billing cycle after the pagers were distributed, Quon exceeded his monthly text message character allotment. Although he was reminded by Chief Scharf that the messages sent on the pagers were considered email and could be audited, Scharf suggested to Quon that he reimburse the City for the overage fee, rather than have Scharf audit the messages. Quon and others who had exceeded their message character allotment wrote checks to the City for the overage. *Quon, Id.* at 752.

Over the next few months, Quon exceeded his character limit three or four times. Each time he reimbursed the City for the overage. After several months, Scharf decided that it was necessary to determine whether the existing character limit was too low, or if the overages which Quon and others were incurring were related to personal messages. Transcripts of Quon's text messages for a two month period were requested from Arch. Upon review of the text messages, it was determined that many of the messages sent and received on Quon's pager were not work related, and some were sexually explicit. After review, the matter was referred to Ontario Police Department ("OPD") internal affairs division, which issued a report concluding that Quon had violated OPD rules, and he was allegedly disciplined. *Quon, Id.* at 753. The same two months of transcripts were reviewed during the internal affairs investigation of Quon. However, any text messages sent after Quon's working hours were eliminated from the review process in order to eliminate the possibility of accessing personal messages. Therefore, at internal affairs, the review was even more limited than the original review done for audit purposes.

Quon filed suit, alleging that his Fourth Amendment rights and his rights under the Stored Communications Act[4] were violated when the City obtained and reviewed the transcripts of his text messages. The parties filed cross motions for summary judgment. Relying on *O'Connor*, the District Court determined that Quon had a reasonable expectation of privacy in the content of his text messages. It concluded, however, that whether the audit of the messages was nonetheless reasonable turned on Chief Scharf's intent: "If the purpose for the audit was to determine if Quon was using his pager to 'play 'games' and 'waste time', then the audit was not constitutionally reasonable; but if the audit's purpose was "to determine the efficacy of the existing character limits to ensure that officers were not paying hidden work-related costs… no constitutional violation occurred." *Quon v. Arch Wireless Operating Co*, 445 F. Supp. 2d 1115 (C.D. Cal. 2006). The District Court held a jury trial to determine the purpose of the audit. The jury concluded that Scharf ordered the audit to determine the efficacy of the character limits. Holding that there was no Fourth Amendment violation, the District Court entered judgment in the City's favor. The Ninth Circuit reversed in part, holding that even though the search was conducted for a legitimate, work-related rationale, it was unreasonable in scope. The Supreme Court granted the petition for certiorari filed by the City, OPD, and Chief Scharf. *Quon, Id.* at 759-760.

Concerned about the implications of a broad holding which might define the privacy expectations enjoyed by employees when using employer provided communication devices, the Court decided the issues presented in *Quon* on narrow grounds. It assumed that Quon had a reasonable expectation of privacy in the text

[4] This paper does not address the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*

messages sent on the pager provided to him by the City; that petitioners' review of the transcript of the text messages constituted a search within the meaning of the Fourth Amendment, and that the principles applicable to a government employer's search of an employee's physical office apply with "…at least the same force when the employer intrudes on the employee's privacy in the electronic sphere." *Quon, Id.* at 761.

Acknowledging that two separate standards are set out in the *O'Connor* decision, the Court applied them both to the facts in *Quon*. The *O'Connor* plurality held that when a search is conducted for a "noninvestigatory, work-related purpose" or for the "investigation of work related misconduct", a government employer's warrantless search is reasonable if it is "justified at its inception" and if "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the circumstances giving rise to the search." *O'Connor, Id*. at 725-726. Here, the Supreme Court held that the search was justified at its inception because there were reasonable grounds to suspect that it was necessary for a noninvestigatory, work-related purpose. As the jury found, Chief Scharf ordered the search to determine whether the character limit imposed by the City's contract with Arch was sufficient to meet the City's needs. This was a legitimate work-related rationale. Both the City and OPD had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets for work-related expenses, or on the other hand, that the City was not paying for extensive personal communications. *Quon, Id*. at 761.

The Court held that the scope of the search—*i.e*., reviewing the transcripts—was reasonable because it was an efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or personal use. The review was also not "excessively intrusive". Although Quon had exceeded his monthly allotment a number of times, OPD requested transcripts for only a two month period. The Court held that it was certainly reasonable for OPD to review messages for just two months to obtain a large enough sample to determine whether the character limits were appropriate for the City. *Quon, Id.* at 761.

Finally, the Court concluded that even if Quon could assume some level of privacy would inhere in his messages, it would not have been reasonable for him to conclude that his messages were in all circumstances immune from scrutiny. Quon was told that his messages were subject to audit. As a law enforcement officer, Quon would or should have known that his actions were likely to come under legal scrutiny. Finally, under the circumstances, a reasonable employee would be aware that sound management principles might require the audit of messages to determine whether the pager was being appropriately used. The Court therefore concluded that because the search was motivated by a legitimate work-related purpose and because it was not excessive in scope, the search was reasonable under the approach of the *O'Connor* plurality. *Quon, Id.* at 762. The Court also concluded that the search would satisfy the approach of Justice Scalia's concurrence. The search was reasonable. The Court concluded that the Court of Appeals erred by holding to the contrary, and reversed the judgment of the Ninth Circuit. *Quon, Id.* at 764.

The Fourth, Fifth, Seventh and Ninth Circuits have each addressed the Supreme Court's holding in *O'Connor*. In each of these cases, the warrantless search by the government employer also involved potential criminal conduct by the employee whose workplace was searched. *See United States v. Simons*, 206 F.3d 392 (4th Cir. 2000); *United States v. Fernandes*, 272 F.3d 938 (7th Cir. 2001); *U.S. v. Slanina*, 283 F.3d 670 (5th Cir. 2002), rev'd on other grounds, 537 U.S. 802 (2002); and *United States. v. Taketa*, 923 F.2d 665 (9th Cir. 1991).

The Fourth Circuit's decision in *U.S. v. Simons*, addresses the effect of a government employer's policy on the *O'Connor* legitimate expectation of privacy analysis. Simons was employed as an electrical engineer at the Foreign Bureau of Information Services ("FBIS"), a division of the Central Intelligence Agency ("CIA"). FBIS provided Simons with a private, unshared office, and a computer with internet access. *Simons, Id.* at 395. In June, 1998, FBIS instituted a policy regarding Internet usage by its employees. The policy stated that employees were to use the Internet for government business only. Accessing unlawful material was specifically prohibited. The policy further notified FBIS's employees that it would conduct electronic audits to insure compliance. *Simons, Id.* at 395. FBIS contracted with Science Applications International Corporation ("SAIC") to manage its computer network, including monitoring for any inappropriate use of computer resources. *Simons, Id.* at 395.

On July 17, 1998, during the testing of a firewall by SAIC, it was discovered that a large number of internet "hits" originating from Simons' computer were not visited for official FBIS purposes. This was reported to FBIS. Katherine Camer, FBIS's contact with SAIC, then instructed Clifford Mauck ("Mauck"), the SAIC employee, to view one of the websites which Simons had visited. Mauck discovered that the site contained pictures of nude women. At Camer's direction and from his own workstation, Harper, another SAIC employee, examined Simons' computer to determine whether he had downloaded any picture files from the internet; over 1,000 such files were located. Again from his own workplace, Harper viewed several of the pictures and observed that they were pornographic in nature. Again at Camer's request and again from his own workstation, Harper printed a list of

the titles of the downloaded picture files. He was then asked to copy all of the files on Simons' computer's hard drive. *Simons, Id*. at 396.

On July 31, 2998, two representatives from the CIA Office of Inspector General ("OIG"), one of whom was a criminal investigator, viewed selected files from the copy of Simons' hard drive; the pictures were of minors. Later that day, Harper physically entered Simons' office, removed the original hard drive, replaced it with a copy and gave the original to the FBIS Area Security Officer, who turned it over to the OIG investigator the same day. *Simons, Id*. at 395. On August 5, 1998, FBI Special Agent John Mesisca viewed over 50 of the images on the hard drive which had been removed from Simons' office; many of the images contained child pornography. An application for a warrant to search Simons' office and computer was prepared. *Simons, Id.* at 396. Two separate search warrants were ultimately executed. Simons was indicted on one count of knowingly receiving child pornography which had been transported in interstate commerce and one count of knowingly possessing material containing images of child pornography which had been transported in interstate commerce. Simons moved to suppress the evidence, arguing that the searches of his office and computer violated his Fourth Amendment rights. Following a hearing, the District Court denied the Motion and this appeal ensued. *Simons, Id.* at 397.

While acknowledging that government employees may have a legitimate expectation of privacy in their offices or in parts of their offices, such as their desks or file cabinets, the Fourth Circuit noted that "…office practices, procedures or regulations may reduce legitimate privacy expectations." *Simons, Id.* at 398, citing *O'Connor, Id*. at 716-718. The Fourth Circuit concluded 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 Policy clearly stated that FBIS would "audit, inspect, and/or monitor" employees' use of the Internet, which placed employees on notice that they could not reasonably expect that their Internet activity would be private. The Fourth Circuit held that "Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use. *Simons, Id*. at 398, *citing American Postal Workers Union v. United States Postal Serv.*, 871 F.2d 556, 560 (6th Cir. 1989)(concluding that employees had no reasonable expectation of privacy in lockers in light of policies allowing locker inspections). Accordingly, the remote search and seizure by Harper of the computer files downloaded from the Internet was held not to have violated the Fourth Amendment.

The Fourth Circuit separately analyzed the warrantless entry into Simons' office. There was no evidence in the record that any workplace practices, procedures or regulations had the effect of diminishing Simons' legitimate expectation of privacy. As discussed above, in *O'Connor*, the Supreme Court held that a government employer's interests in "the efficient and proper operation of the workplace" may justify warrantless work-related searches. *O'Connor, Id*. at 723. *O'Connor* further held that when a government employer conducts a search pursuant to an investigation of work-related misconduct, the Fourth Amendment will be satisfied if the search is reasonable in its inception and in its scope. *O'Connor, Id*. at 725-726.

The question then became whether the search of Simons' office falls within "…the ambit of the *O'Connor* exception to the warrant requirement", or in other words, whether it was carried out for the purpose of obtaining evidence of suspected work-related employee misfeasance." *O'Connor, Id.* at 723. In analyzing this issue, the Fourth Circuit agreed with the District Court, which reasoned that FBIS had an interest in fully investigating Simons' misconduct, even if the misconduct were criminal. *Simons, Id.* at 400. The Fourth Circuit assumed that the dominant purpose of the warrantless search of Simons' office was to acquire evidence of criminal activity, which had been committed at FBIS, using FBIS equipment. Nonetheless, the search remained within the *O'Connor* exception to the warrant requirement. It held that 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, citing *New York v. Burger*, 482 U.S. 691, 716 (1989)(holding that "the discovery of evidence of crimes in the course of an otherwise proper administrative inspection does not render that search illegal or the administrative scheme suspect"); *Gossmeyer v. McDonald*, 128 F. 3d 481, 492-93 (7th Cir. 1997)(concluding that the presence of law enforcement personnel at search of employee's office by government employer did not preclude application of *O'Connor*.). Further, 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. The search was also permissible in scope, in that it was reasonably related to the objective of the search, *i.e.*, retrieval of the hard drive. There was no evidence that the search was excessively intrusive. Harper simply crossed the floor of Simons' office, switched hard drives and exited. *Simons, Id.* at 401.

Simons thus presents a case in which there is a "conjunction" of the conduct which violated FBIS's internal policy with a situation in which the conduct also violated the criminal law. *Simons, Id.* The Fourth Circuit held: "In the final analysis, this case involves an employee's supervisor entering the employee's

government office and retrieving a piece of government equipment in which the employee had absolutely no expectation of privacy—equipment that the employer knew contained evidence of crimes committed by the employee in the employer's office. This situation may be contrasted with one in which the criminal acts of a government employee were unrelated to his employment…We consider that FBIS's intrusion into Simons' office to retrieve the hard drive is one in which a reasonable employer might engage…". *Simons, Id.* at 401. For that reason, the remote viewing of Simons' computer, as well as the warrantless search of his office, were upheld as reasonable.

A Fifth Circuit case, *United States v. Slanina*, 283 F.3d 670 (5th Cir. 2002), vacated on other grounds, 537 U.S. 802 (2002), also involved workplace misconduct as well as involved criminal conduct. Wesley Slanina ("Slanina") served as the Fire Marshall for Webster, Texas for nine years. Prior to June, 1999, Slanina's desk was located in City Hall, where he had a city-provided computer with Internet access, but no connection to the city's intra-office network. When a new fire station was built, Slanina moved into his own office in the new station. He brought his old computer with him, but in the new office he had no Internet access or network connection. In June, 1999, Ryan Smith ("Smith") the Management Information Systems Coordinator began working to install the city network on the fire station computers. Smith used a grand master key to enter Slanina's office and attempted to continue his work. However, the computer was protected by a password. Slanina was out that day, but was directed by his supervisor to provide his password to Smith. Slanina indicated some reluctance to do so, unexpectedly turned up at the office despite the fact that he had just had surgery to remove his wisdom teeth, signed onto his computer when Smith left the room, and finally left. *Slanina, Id.* at 672. Looking at Slanina's email, Smith discovered three titles suggesting the presence of pornography. Smith conducted a search for JPEG files and Gif files which are used for images. When he located one such file, he saw that it contained an image of adult pornography. He called the Assistant Fire Chief, and advised him of what he had found. The Assistant Fire Chief instructed Smith to secure the office, so Smith changed the lock, turned off the computer and left. *Slanina, Id.* at 673.

The next day, Smith spoke to Bruce Ure ("Ure"), the Webster Fire Chief, and Mike Keller ("Keller"), the Public Safety Director. He told them about the discovery. Keller instructed Ure and Smith to remove the computer from the fire station and place it in his office. When they went to Slanina's office, Smith showed Use the pornography before removing the computer. The three also viewed the computer for about two hours. Finally, Keller contacted the City Manager and told him that child pornography had been discovered on Slanina's computer. They discussed the possibility of criminal violations in addition to the misuse of city property. Human Resources was contacted and the group determined that they would notify the FBI the next day. *Slanina, Id.* at 673.

At 7:15 a.m. the next day, Ure met Slanina in the parking lot and advised him they needed to go to Keller's office. There, Slanina met Captain Ray Smiley of the Internal Affairs Division and was furnished with a written copy of the Internal Affairs investigation. Slanina was told that he would be suspended pending the investigation concerning the misuse of city property. Keller informed him that they had seized his computer and ordered him to surrender his badge and city identification. *Slanina, Id.* at 674. Although he was informed that they intended to contact the FBI, and that he was not in custody and was free to leave at any time, Slanina stayed with them. Slanina admitted to downloading the photographs of child pornography, and consented to a search of his residence. The office and home computer equipment, drives and disks were turned over to the FBI, which examined the active files and recovered deleted files from the hard drives. On February 14, 2000, Slanina was indicted on two counts of possession of child pornography. He moved to suppress all statements made by him to law enforcement officers and all evidence obtained from his office computer equipment and home computer equipment. The District Court denied the Motion. *Slanina, Id.* at 675.

The Fifth Circuit concluded that Slanina had a legitimate expectation of privacy with respect to his office and computer equipment. The Court noted that he had closed and locked the door to his office and had installed passwords to make it more difficult to get past the screen saver and reboot his computer. *Slanina, Id.* at 676. Further, the Fifth Circuit held that Slanina's expectation of privacy was reasonable. It noted that Slanina had a private office, and that only a select few of his co-workers could access the office. The Court pointed out that although network administrators and computer technicians necessarily had some access to his computer, there was no evidence that the access was routine. Finally, the city did not disseminate any policy which prevented the storage of personal information on city computers and also did not inform its employees that computer usage and internet access would be monitored. Therefore, in view of the absence of a city policy placing him on notice that his computer usage would be monitored, and because there was the lack of any indication that other employees had routine access to his computer, the Fifth Circuit held that Slanina's expectation of privacy with respect to his office and computer equipment was reasonable. *Slanina, Id.* at 676.

The Fifth Circuit then considered whether the search violated Slanina's Fourth Amendment rights.

Slanina differs from *O'Connor* in two respects. First, in *Slanina*, although his use of the city-provided computer equipment to access and store pornography constituted workplace misconduct, it also violated criminal law. *Slanina, Id.* at 677. It noted that *O'Connor* had specifically excepted this situation from its holding, declining to "address the appropriate standard when an employee is being investigated for criminal misconduct or breaches of other nonwork-related or regulatory standards." *O'Connor, Id*. at 729. Second, the *O'Connor* Court suggested that its holding might not extend to the context of investigations into work-related misconduct by government employers, who, like Keller, are also law enforcement officers. *O'Connor, Id.* at 729.

The Fifth Circuit concluded that Keller's search of Slanina's office computer equipment should be reviewed under the *O'Connor* standard. It cited the fact that any evidence of criminal acts was also proof of work related misconduct. Further, the record evidence demonstrated that as of the time of Keller's search, the investigation remained, at least partly, an investigation into employee misconduct. Therefore, to hold that a warrant is necessary any time a law enforcement official recognizes the possibility that an investigation into work-related misconduct will yield evidence of criminal acts would frustrate the government employer's interest in the efficient and proper operation of the workplace. *O'Connor, Id.*at 723. Finally, the Fifth Circuit found that Keller's search was justified at its inception and reasonably related to the circumstances justifying the interference in the first place. Because any use of the city provided computer by Slanina to access pornography was a violation of city policy, Keller was entitled to determine the extent of Slanina's violations. *Slanina, Id.* at 679.

VI. RECOMMENDATIONS FOR THE GOVERNMENT EMPLOYER

In the cases in which a government employer has performed a search of its employee's workplace, desk, files, or computer, the Courts which have reviewed these issues have emphasized the presence or absence of a policy regulating the manner in which the employer's resources, such as a government provided computer, may be used. For example, in *Quon*, the City of Ontario had announced a computer usage, internet and email policy which applied to all employees. It specified that the City reserved the right to monitor and log all network activity, including email and internet use, with or without notice. *Quon, Id.* at 751. The fact that Quon was on notice of the possibility of an audit of his text messages was used by the Court as one of the factors which suggest that it was not reasonable for Quon to assume that his messages would be free from scrutiny.

The Fifth Circuit also discussed the issue of a government policy regarding computer usage and monitoring in *Slanina.* In that case, however, the City had not disseminated any policy which prevented the storage of personal information on city computers and also did not inform its employees that computer usage and internet access would be monitored. On that basis, the Fifth Circuit held that Slanina's expectation of privacy in his computer was reasonable. *Slanina, Id.* at 677.

For this reason, the government employer should consider enacting a policy which outlines the manner in which computer usage, internet, text messages, email and other electronic communications and resources are to be used by its employees. If the employer intends to monitor and log all network activity, that should be included in the policy. In that manner, a government employee will be on notice that maintaining personal information on the government issued computer is not permitted. If a search is required, any argument that the employee had a legitimate expectation of privacy in his or her government owned computer will be diminished, if not eliminated.

If a government employer finds it necessary to search an employee's workplace, desk, file cabinets, computer system, and so on, the reason for the search should be documented. The search should be conducted in a manner to minimize the intrusiveness into the employee's privacy. The manner in which the search was performed, the area or areas which were actually searched should be identified, and included in the documentation. That way, the employee's ability to argue that a search was not reasonable will be reduced.