TCRP
Transit Cooperative Research Program
Sponsored by the Federal Transit Administration

LEGAL RESEARCH DIGEST

March 2000—Number 14

Subject Areas: IA Planning and Administration, IC Transportation Law, VI Public Transit

Treatment of Privacy Issues in the Public Transportation Industry

This report was prepared under TCRP Project J-5, "Legal Aspects of Transit and Intermodal Transportation Programs," for which the Transportation Research Board is the agency coordinating the research. The report was prepared by Mark McNulty. James B. McDaniel, TRB Counsel for Legal Research Projects, was the principal investigator and content editor.

THE PROBLEM AND ITS SOLUTION

The nation's transit agencies need to have access to a program that can provide authoritatively researched, specific, limited-scope studies of legal issues and problems having national significance and application to their businesses. The TCRP Project J-5 is designed to provide insight into the operating practices and legal elements of specific problems in transportation agencies.

The intermodal approach to surface transportation requires a partnership between transit and other transportation modes. To make the partnership work well, attorneys for each mode need to be familiar with the legal framework and processes of the other modes. Research studies in areas of common concern will be needed to determine what adaptations are necessary to carry on successful intermodal programs.

Transit attorneys have noted that they particularly need information in several areas of transportation law, including

- Environmental standards and requirements;
- Construction and procurement contract procedures and administration;
- Civil rights and labor standards; and
- Tort liability, risk management, and system safety.

In other areas of the law, transit programs may involve legal problems and issues that are not shared with other modes; as, for example, compliance with transit-equipment and operations guidelines, FTA financing initiatives, private-sector programs, and labor or environmental standards relating to transit operations. Emphasis is placed on research of current importance and applicability to transit and intermodal operations and programs.

APPLICATIONS

Transportation officials have expressed a need for a legal synthesis of legislation, case law, studies, and other available resource material related to privacy issues in the transportation industry. Every aspect of the transportation industry has been affected by technological advancements, particularly in collecting, transmitting, and storing information. The method for assuring security for this information, determining who has access, and determining when and how the documents should be destroyed are matters of utmost importance. Placement of surveillance equipment, notice to individuals in the presence of such equipment, use of the videos, and destruction procedures are likewise matters of concern.

This report provides a topical reference to these issues and should be useful for attorneys, administrators, human relation officers, security personnel, supervisors, and all officials who confront these issues.

TRANSPORTATION RESEARCH BOARD
NATIONAL RESEARCH COUNCIL

CONTENTS

TREATMENT OF PRIVACY ISSUES IN THE PUBLIC TRANSPORTATION INDUSTRY

By Mark McNulty, Special Counsel, Delaware Department of Transportation

I. INTRODUCTION

A. Statement of the Problem

It appears to be an inherent belief, at least in the United States today, that the "right" to privacy is an inalienable and unassailable protection indigenous to the human species. The underlying theoretical basis for the doctrine has provided a basis for decisionmaking in the common law since well before the founding of this Nation. However, it was only slightly over 100 years ago that privacy was identified as a distinct right.[1]

Jurisprudential treatment of the subject, and certainly the vast bulk of court decisions establishing its parameters, is of relatively recent origin, yet its importance is growing exponentially with each new technological advancement. The evolution of the law of privacy continues at a more frenetic pace today, and with a greater sense of urgency than most legal doctrines, because of the sheer rapidity of these technological changes, which appear to be outpacing the ability of the lawmakers and the courts to keep current.

Questions are being raised in many circles about access to the Internet; who will control the flow of information; and, more importantly, who will determine what information is collected, stored, and disseminated, as well as who will have access to such information.[2]

According to at least one survey of 275 Fortune 500 companies conducted by the University of Illinois, privacy has become the number one issue in the workplace.[3] The purpose of the study was to ascertain to what extent employers were monitoring activities of their employees. The authors found such intrusions into employees' privacy interests to be alarmingly extensive.[4]

Of the 126 companies who responded, the results indicated that in many instances employees enjoy little or no privacy either from their employer or from those making inquiries to their employer. The findings published in 1990 are illustrative of this point:

- 80 percent of the companies disclosed personal information to creditors.
- 60 percent gave such information to landlords.
- 28 percent gave this information to charitable institutions.
- 38 percent had no policy concerning the release of information to government agencies.
- 22 percent collected information about employees without informing the person.
- 58 percent of the companies had a drug-testing program.
- 57 percent did not tell their employees what types of records they maintain about them.
- 58 percent did not tell employees what information about them was released.

1. Origins

The early explorations of the law of privacy stemmed in large measure from an examination of Fourth Amendment prohibitions against "unreasonable searches and seizures." Much of the fundamental analysis, which has evolved into other areas, can be found in criminal case law decisions. Decisional law emanating from both the public and private workplaces, and certainly decisions stemming from the provision of public transportation, are even more recent in time and still somewhat sparse.

As foreboding as it might have sounded to some, but perhaps ludicrous to others in 1966, Justice William 0. Douglas said that "[w]e are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government."[5]

Few would find the actual and potential for infringement on personal privacy rights, particularly in the employment setting, less ominous today than 30 years ago. Indeed, there is a good case to be made that personal privacy, under the traditional status it has been afforded and the laws that govern its current application, may be at risk as a result of technological advancement.[6]

2. Privacy: Today and Tomorrow

The improvement and ever expanding use of microelectronics and circuitry, cellular and portable telephones, fax machines, email, the Internet, and telecommunications in all of its various forms has changed the world in a very short period of time. We have heard about these new technologies, some already in use and some yet to come, and how they are anticipated to change the world.

---

[1] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[2] The Electronic Privacy Information Center (epic.org).

[3] David F. Linowes and Ray C. Spencer, *Privacy: The Workplace Issue of the 90's*, 23 J. MARSHALL L. REV. 591, 593 (1990).

[4] *Also see*, Joan O'C. Hamilton, Stephen Baker, and Bill Vlasic, *The New Workplace*, BUS. WK., Apr. 29, 1996, at 106; Jeffrey Rothfeder, Michele Galen, and Lisa Driscoll, *Is Your Boss Spying On You?,* BUS. WK., Jan. 15, 1990, at 74.

[5] In his dissent in Osborne v. United States, 385 U.S. 323, at 341 (1966).

[6] Bob Herbert, *What Privacy Rights?*, N.Y. TIMES, Sept. 27, 1998, (Week in Review) at 15.

At the same time, there is an ongoing dispute concerning what is or should remain private within the work site. From the employers' perspective, whether public or private, it is absolutely essential that the employers' need for supervision, control, and efficiency be the focal point of employer-employee relations. Additionally, it can be argued that by the mere fact that the employer owns the building and equipment within the work site, the employer must and should have the right to monitor everything that goes on within that environment.

In the case of elected officials, access to information generated from within and flowing into public agencies is absolutely essential for a variety of reasons, not the least of which is to keep operations within the limitations established by the three branches of government. Private employers argue for control of access to all information because of the need to protect trade secrets and other issues involving competition, as well as to minimize adverse impacts on employee morale from leaks of competitive or inaccurate information.

Employees assert that despite these facts, there are certain areas into which the employer should not be allowed to infringe, such as personal phone calls, emails, etc., which most people would argue are an accepted component of modern working conditions.[7]

Against this backdrop, we know that according to a survey by the American Management Association, 35 percent of its members monitor employee email, phone calls, voice mail, and computer files.[8] A 1997 survey of American businesses by the Society for Human Resource Management found that 70 percent of the companies polled had no written policy on use of the Internet and about 50 percent had no policy regarding the use of email.[9] Evolving technologies raise even bigger questions.

Some of the technologies under development or improvement for future use have tremendous potential for both good and bad purposes. With their various names and acronyms, such as global positioning systems (GPS), global information systems (GIS), smart cards, intelligent vehicle-highway systems (IVHS), intelligent transportation systems (ITS), and electronic highways, they include the entire gamut of transmissions over the electromagnetic spectrum. These and the various other "Star Wars" advancements looming on the horizon have the potential to provide transportation planners and providers with enormous amounts of transportation-friendly data, but such information also has the potential to be misused.

Advertisers are constantly seeking more and more information about, and developing profiles of, their existing and potential customers. At the same time, there have been tremendous advances in eavesdropping, security, and surveillance technology. Security at home, in the workplace, and elsewhere has become a significant issue in our daily lives. Credit cards, ATMs, and security cameras have become commonplace, while at the same time providing someone someplace with ever more detailed information about each of us.

Within the broad topic of privacy in the workplace, privacy in public transportation is relatively narrow, without a great deal of authority directly on point. In some cases, it does not matter whether the workplace is public or private, while in other instances, we find that there are distinct differences between public and private employment and how the law is applied toward different work settings. For instance, it does appear that in certain situations, public employees enjoy a greater degree of protection than their counterparts in private industry (i.e., the Fourth Amendment prohibits state action against individuals, which presumably includes its own employees). Conversely there are situations in which public employees do not enjoy the same protections as private employees in similar settings (i.e., public employees are not exempt from the preemployment polygraph testing prohibition under 29 U.S.C.A. Section 2006[a]).

3. Intelligent Transportation Systems (ITS)

The specter of privacy concerns arising from new technological developments is a very real one that Congress and others have struggled with each time they have addressed the issue. None is more formidable than the concerns engendered by the evolution of ITS.

ITS is a term used to cover a very broad and diverse array of techniques, strategies, and new technologies being utilized, developed, or planned that are designed to facilitate the fast and efficient movement of surface transportation. These include all manners of proposed changes from traffic signal improvements, improving accident investigations, and providing better on-time information regarding train and bus schedules, to introducing new GPS applications, more efficient freight movement through satellite applications, and smart highways with electronically-guided people movers.

Various components of systems resulting from ITS are discussed individually throughout this report, but there will be no further delineation of ITS in the report. See Appendix A for further information on how ITS may affect privacy.

4. Focus of This Paper

This paper briefly discusses the development of the law of privacy and examines its continuing evolution within the context of societal and technological changes, particularly how these principles apply to the public transportation industry and its employees. The case law is instructional in looking at how the courts have traditionally balanced privacy and other competing constitutional interests in trying to determine how these principles might be applied prospectively. Hope-

---

[7] *Also see*, *Workplace Privacy in an Era of New Technologies,* MESSAGING MAGAZINE, Nov. 7, 1997.

[8] Ellen Goodman, *Whole World Knows Nothing Stays Private,* WILMINGTON NEWS JOURNAL, Feb. 21, 1998, at A7.

[9] *Firings Flag Need for Net Policy*, USA TODAY, Apr. 1, 1998.

fully, the cases and articles discussed will also provide some insight and provoke thought and discussion on this issue.

The paper then narrows its focus to look at some of the major privacy issues in public transportation, both from the standpoint of how these issues impact public employees within their work environment and how it affects members of the general public in their dealings with the public sector. The study concludes with some recommendations for public employers and employees regarding work site issues and the use and potential abuse of the new technology.

B. Constitutional Right of Privacy and Other Legally Protected Privacy Interests

Personal privacy is one of our most fundamental rights. However, it is not absolute and must give way in the face of more compelling governmental interests, but only to the extent required.[10] The "right" to privacy appears to have been first discussed as an independent right or at least perceived as a distinct right, along with its underlying legal principles, in a law review article by Warren and Brandeis (later Justice Brandeis) in which the authors referred to the right to privacy in its most basic terms as the "right to be let alone."[11] While the theoretical basis for the doctrine has not been credited to a single source since this article first appeared, nevertheless, the principle that the right to privacy is unique and a distinct right had taken hold.[12]

1. Constitution: Zone of Privacy

In *Griswold v. Connecticut*, the United States Supreme Court overturned a state statute prohibiting the use of contraceptive devices.[13] The Court found that although the right to privacy is not explicitly mentioned in the Constitution, it is an implicit right contained within the Bill of Rights and in what it termed a "zone of privacy" arising from the "penumbras" of constitutional guarantees. The Court found that constitutional protection regarding use of contraceptive devices was protected within those "zones of privacy."

A reading of the landmark decision in *Roe v. Wade* provides an illustrative history of the development and origins of the right to privacy in the United States.[14] The Supreme Court enunciated its principle that despite the fact that the right to privacy had not been specifically mentioned in the Constitution, the Court had long recognized the existence of a right of personal privacy and that "a guarantee of certain areas or zones of privacy, does exist under the Constitution."[15]

Justice Douglas, in his concurring opinion in *Roe*, observed that the Court had long recognized a right of privacy, older than the Bill of Rights, as being in a category that is fundamental and inextricably bound to those rights.[16] In discussing the origin of the right to privacy, he stated that although some rights are absolute, others, including privacy, can be regulated upon a showing of a "compelling state interest."

The Supreme Court decisions in both *Griswold* and *Roe* established the principle that privacy is a fundamental right inherent to the human race with origins that predate the Constitution in the form of a corollary to the specific guarantees contained in at least most of the first nine amendments. As the Supreme Court noted in *Griswold v. Connecticut*, privacy is among those rights that flow from the Constitution and that the "specific guarantees in the Bill of Rights have penumbras, formed by emanations from these guarantees that help give them life and substance."[17]

2. Tort: Breach of Personal Right to Privacy

The constitutional right to privacy has been defined as one that limits governmental action or interference vis à vis the rights of an individual. There also exists, simultaneously, a personal right of privacy for which a cause of action exists against tortious invasion that is generally left to the law of the states to determine.[18]

The most elemental form of invasion of privacy giving rise to an actionable tort is the public disclosure of facts that otherwise would remain private. There are three essential elements necessary for a cause of action to arise in that situation: (1) there must be a public disclosure, (2) the facts disclosed must be private facts, rather than public and, (3) the matter made public must be one that would be offensive and objectionable to a reasonable person of ordinary sensibilities.[19]

The simple fact is that "private" people have a right to have private information kept private, unless it is a matter of genuine public interest.[20] A public transportation official or employee must take pains to guard against the release of such information, unless it is disclosable by law, or for a reason recognized as legitimate. Legal review and advice is recommended. The fact that such information may be true, while it consti-

---

[10] Roe v. Wade, 410 U.S. 113 (1973).

[11] Warren and Brandeis, *supra*, n.1.

[12] For a good general discussion of the foundations of privacy as a recognized and unique right, see *Privacy*, 62A AM. JUR. 2D, § 3 (at 635-36), where a distinction is described between its common law and constitutional bases:

> While some courts have taken the view that the right is predicated upon federal constitutional guaranties, other courts have drawn a sharp distinction between one's constitutional right to privacy, which defends the individual against government action, and the right to privacy that is involved in a tort action. (footnote omitted) at 635-36.

[13] 381 U.S. 479 (1965).

[14] 410 U.S. 113 (1973).

[15] *Id*. at 152.

[16] 410 U.S. at 210-15.

[17] (Cite omit.) 381 U.S. at 484.

[18] Katz v. United States, 389 U.S. 347 (1967).

[19] *Privacy,* 62A AM. JUR. 2D*,* § 91.

[20] *Restatement 2d*, Torts, § 652D.

tutes a defense in a case of libel, is not a defense for an action for invasion of privacy or an infringement upon one's "right to be let alone."[21]

According to the *Restatement*, Torts, 652A, the right to privacy can be tortiously invaded in four different ways:

- The unreasonable intrusion upon the seclusion of another.
- The appropriation of another's name or likeness.
- Unreasonable publicity given to another's private life.
- Publicity that unreasonably places another in a false light before the public.

II. INVASION OF PRIVACY ISSUES GENERALLY

Questions regarding individual privacy rights have arisen in all manner of case law decisions, from backyard neighbor disputes to situations arising out of national security. Courts have sought to find the balance between the rights of the individual versus the rights of the community at large, within the context of the issue at hand. Courts have held that "[t]he constitutional protection afforded privacy interests is not absolute. State interests may become sufficiently compelling to sustain State regulations or activities, which burden the right of privacy. The regulations, however, must be narrowly drawn to express only those compelling State interests."[22]

In a case decided on the question of "freedom of association," the Supreme Court struck down an Arkansas statute and held that requiring teachers, as a condition of employment in a state-supported school or college, to annually file an affidavit listing every organization to which the teacher belonged or contributed for the previous 5 years, constituted a violation of the due process clause of the Fourteenth Amendment.[23] The State's interest was not compelling.

The issue in all such cases is essentially the same although ever more complex: What are the rights of the individual juxtaposed against the rights of society within a public context and a private context? Advances in technology only serve to make the issue more problematic. The following are illustrative examples of this dichotomy in several cases decided by the United States Supreme Court.

A major line of cases that addressed the privacy issue within the context of constitutional protection evolved in criminal law. These cases questioned law enforcement officials' ability to conduct certain types of searches in order to apprehend the culprit. These cases are also illustrative of the legal evolution of the doctrine and how the balancing test has been expanded into other areas.[24]

A murder case, in which the defendant's car was towed from a public lot to a police impoundment lot and then searched after the defendant's arrest, raised the issue.[25] The Court found that the search was not unreasonable under the Fourth and Fourteenth Amendments and that any "invasion of privacy" caused by the search was justified under the circumstances. The Court found that there was a clear distinction between the right of privacy as applied in a personal capacity, with a physical search of the person or a search conducted within a building being more sacrosanct than an automobile search. The Court made the distinction on the basis that the latter was "far less intrusive."[26]

A. Public Highways

The Supreme Court in *Cardwell* clearly established a line of demarcation in "search and seizure" cases between those involving the search of the person, or that person's place of residence, and a "search" conducted on a public highway. In another case,[27] the Court quoted from *Cardwell* and found that:

> One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view. (Cit. Omit.)[28]

In a 1983 Supreme Court case, Minnesota law enforcement agents placed a radio transmitting beeper inside a 55 gallon drum of chloroform purchased by one of the defendants, which was subsequently put into the defendant's truck.[29] The vehicle was then tracked, through the use of the beeper, video cameras, and visual observation, to a cabin where drug manufacturing was occurring. The Court indicated that a person traveling the public streets has no reasonable expectation of privacy and that the actions of the agents did not constitute a search and seizure protected by the Fourth Amendment.[30] This decision and similar holdings could have significant implications on the issue of privacy as it relates to some of the more advanced traffic monitoring and GPS applications.[31]

The Supreme Court has determined that any activities conducted in public, or otherwise exposed to public view, are not protected activities under the Constitu-

---

[21] Afro-American Publishing Co. v. Joffe, 366 F.2d 649 (1966).

[22] McKenna v. Fargo, 451 F. Supp. 1355, 1381; *aff'd*. 601 F.2d 575 (1978).

[23] Shelton v. Tucker, 364 U.S. 479 (1960).

[24] *See*, for example, Terry v. Ohio, 392 U.S. 1 (1968).

[25] Cardwell v. Lewis, 417 U.S. 583 (1974).

[26] *Id*. at 590.

[27] New York v. Class, 475 U.S. 106 (1986).

[28] *Id*. at 112-13.

[29] U.S. v. Knotts, 460 U.S. 276 (1983).

[30] *See also* Hester v. United States, 265 U.S. 57 (1924).

[31] *See also infra*, Section II.C., *Farecards.*

tion. In *Katz v. United States*,[32] the Supreme Court had previously held that:

> The Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. (Cit. Omit.) But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[33]

One area that has drawn considerable attention is the use of photographic equipment for traffic enforcement.[34] Following the holdings and the reasoning utilized in *Katz* and *Cardwell*, it would appear that, provided certain reliability safeguards are included, the use of photographic evidence for traffic and safety enforcement is constitutionally permissible.[35]

B. Transit Facilities, Buses, and Trains

Activities that take place in transit facilities, or on what is characterized as public transportation, including buses, trains, and airplanes, are generally considered as being "public" activities and are exempt from constitutional protections on that basis alone. Under the same reasoning discussed in *Katz* and *Cardwell*, courts have held that the use of cameras for safety and surveillance purposes in areas that are accessible to the public does not infringe upon an individual's constitutional right to privacy.[36] The privacy interests of persons in transit, or in public transit facilities, have been determined to be "substantially less" than those that attach to a fixed dwelling.[37]

C. Farecards

The use of smart cards or farecards for transit patrons provides convenience and quick access into the system. Similar card systems are being used for automobile traffic and usually involve a card reader at a tollbooth, at the entrance to the system, or on the transit vehicle itself.[38] Such cards usually require a prepayment either in the form of cash or a credit card charge and provide some information about the user. For transportation planners, information garnered from the use of such instruments helps in understanding various "use" patterns generally. At the same time, it can also serve to provide more specific information about specific users, which raises corresponding privacy questions.[39] No case involving the use of smart transit cards or farecards was found directly on point, but there is no reason to believe that the courts would find that activities conducted or undertaken in public would have any constitutional protection.[40] As these technologies become more and more sophisticated, the implications to privacy considerations become more profound.[41]

D. Related Issues

The Court upheld the right of the U.S. Environmental Protection Agency (EPA) to use aerial photography to "search" Dow Chemicals' manufacturing facility from the air without a warrant, when filmed from an aircraft within lawful navigable airspace.[42] Despite the fact that EPA had other means to conduct a search of the property, including an actual search pursuant to a warrant, the Court determined that the aerial photography in this case was not a search prohibited by the Fourth Amendment.

The contents of a garbage container placed at curbside for pickup were not protected from a warrantless police search and seizure under the Fourth Amendment.[43] The Court stated that:

> [T]he police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public. Hence, "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[44]

For purposes of this discussion, it is also noteworthy that the Court reasoned that the respondent Greenwood was only entitled to Fourth Amendment protection if he "manifested a subjective expectation of privacy in their garbage that society accepts as objectively reasonable."[45]

The Supreme Court upheld a New York statute requiring the recording of the names and addresses of all persons using certain regulated prescriptions drugs as a reasonable exercise of the State's police powers.[46] The Court expounded upon the origins of the right of privacy and in a footnote identifies at least three of its aspects:

> 1. A person's right to be free from government surveillance and intrusion in his private affairs.
>
> 2. A person's right not to have his private affairs made public by the government.

---

[32] 389 U.S. 347 (1967).

[33] *Id.* at 351.

[34] *See* Daniel T. Gilbert, Nina T. Sineo, and Brandon E. Bell, *Photographic Traffic Law Enforcement,* LEGAL RESEARCH DIGEST 36 (Trans. Research Board) Dec. 1996.

[35] *Id*. at III.C, p. 9.

[36] *See* III.B.7., *Privacy Rights on Public Transit***,** *infra*, this paper.

[37] *Id*. United States v. McDonald, 100 F.3d 1320 (7th Cir. 1996).

[38] E-Z Pass, Washington Metro System.

[39] *See* III.B.7., *Privacy Rights on Public Transit*, *infra,* this paper.

[40] *Id*.

[41] *See infra*, IV., *Intelligent Transportation Systems (ITS)*.

[42] Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

[43] California v. Greenwood, 486 U.S. 35 (1988).

[44] *Id.* at 41.

[45] *Id*. at 39.

[46] Whalen v. Roe, 429 U.S. 589 (1977).

3. A person's right to be free from government coercion in his actions, thoughts, experiences and beliefs.[47]

In 1972, California adopted an amendment to its state constitution known as the "Privacy Initiative," which was intended to apply "a right to privacy" policy to private actions, as well as governmental actions. A case was brought pursuant to the Privacy Initiative against the National Collegiate Athletic Association (NCAA), a private association, alleging that the NCAA's drug testing policy was violative of the student athletes' privacy rights.[48] The court held that privacy concerns, while important, are not absolute in nature and have to be balanced against competing interests. In this case, because of the students' "lowered expectation of privacy" as a result of being student athletes, their privacy interests did not overcome the compelling interests of the NCAA in protecting the health and safety of the student athletes, as well as providing a fair and competitive atmosphere for athletic competition.

An important distinction to keep in mind in this discussion regarding the privacy rights and responsibilities of public transportation employees is that a constitutional distinction exists between state and private action. The most notable difference is that constitutional guarantees are only invocative as to governmental actions, which forms the basis for saying that, at least in theory, public employees have a higher degree of protection in the workplace on constitutional grounds than their private counterparts. As noted in the case of *O'Connor v. Ortega*,[49] discussed below, it is somewhat illusory.

In reading each of the cases cited above within the context of the facts contained therein, one has little difficulty understanding the holding of the Court in balancing the rights of the individual versus the rights of society. However, applying these same principles to a world in which technological advances allow for precise satellite photography, super-sensitive listening devices, computerized data banks, and the like underscores the need for greater scrutiny of privacy protection.

III. SPECIFIC PRIVACY ISSUES

A. The Standard of Care

The standard by which an invasion of privacy is generally measured in order to constitute tortious conduct is whether the conduct exhibited would offend a reasonable person of ordinary or reasonable sensibilities.[50] However, it has been held that there can be no liability for the disclosure of facts that are a matter of public record.[51] Sometimes these rights are in conflict.

In a Florida case, the U.S. Supreme Court determined that the publication of a rape victim's name, although prohibited by Florida statute, did not violate the victim's right of privacy under the circumstances of the release of the information and for purposes of protecting the First Amendment rights of the newspaper.[52]

Public facts, as opposed to public records, do not remain public forever and thereby carry a privilege of impunity for their release for only a limited period of time. In fact, public facts become private facts once the item is no longer newsworthy.[53] The standard for what may constitute newsworthiness appears somewhat subjective, as it is a case of when an issue becomes a matter consistent with community mores.[54] The constitutional standard is much more elusive and courts appear to be divided in many cases as to what may constitute an abridgement of constitutional protections.

B. Privacy in the Public Workplace

1. Introduction

Employees in the workplace, whether public or private, generally enjoy very little protection under the law. Historically, the courts have been loath to interfere in the employment relationship and usually do so only when the conduct of the employer has been so unconscionable or egregious that it shocks the court into action. Generally, persistent abuses have caused legislative bodies to act but oftentimes it results in a negotiated piece of legislation, which in some cases amounts to "too little too late."

Public employees arguably have a greater degree of protection against state action under the Fourth Amendment to the Constitution. However, this is somewhat illusory and what protection there may be is often made on a piecemeal basis.[55] More significantly, the United States Supreme Court has held that the governmental authority has wider latitude to impose restrictive regulations on its employees than it does on regulating the citizenry at large.[56]

An important case in the area of privacy in public employment is *O'Connor v. Ortega.*[57] Dr. Ortega was employed as a psychiatrist at a state hospital in California for 17 years as the chief of professional education. Hospital officials instituted an investigation based upon allegations of improprieties in the management of the hospital residency program. The specifics of the claims centered on an allegation that Dr. Ortega had acquired a computer using coerced contributions from hospital residents, as well as alleged incidents of sexual

---

[47] *Id*. at 599, n.24

[48] Hill v. National Collegiate Athletic Association, 865 P.2d. 633 (Cal. 1994).

[49] 480 U.S. 709 (1987).

[50] Roscoe Pound, *Interests of Personalities*, 28 HARV. L. REV. 343, 362-63 (Feb. 1915).

[51] Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

[52] The Florida Star v. B.J.F., 491 U.S. 524 (1989).

[53] *Privacy*, 62A AM. JUR. 2D § 104.

[54] Virgil v. Sports Illustrated, 424 F. Supp. 1286 (S.D. Cal. 1976).

[55] Laura B. Pincus and Clayton Trotter, *The Disparity Between Public and Private Employee Protection*, 33/1 AM. BUS. L. J. at 51 (1995).

[56] Kelly v. Johnson 425 U.S. 238 (1976).

[57] 480 U.S. 709 (1987).

harassment of female employees and an alleged incident of imposing inappropriate disciplinary action against a resident.

Dr. Ortega was placed on paid administrative leave while the hospital investigated the charges. As part of the investigation, hospital officials searched the doctor's office several times and seized several personal items from the office, as well as items from areas outside the office, although no formal inventory of the items seized was made. The seized items, all of which were on state property, including the personal items from the doctor's office, were subsequently used as evidence during an administrative hearing, as a result of which Dr. Ortega was terminated.

Dr. Ortega filed an action under 42 U.S.C. Section 1983, alleging that the search of his office constituted a violation of the Fourth Amendment. On appeal to the U. S. Supreme Court, two issues were raised: (1) Does a work-related search constitute an exception to the warrant and probable cause requirements of the Fourth Amendment?, and (2) How should the courts balance the competing interests of the government employer and the government employee in deciding whether the search was reasonable under the Constitution?

The Court remanded the case to the district court for further fact finding to determine the justification for the search and seizure and to evaluate the reasonableness of both the inception of the search and its scope. The decision is illustrative in the area under discussion for a number of reasons. Primarily it established a standard, although somewhat amorphous, for employees in the public workplace.

Noting that the hospital had no administrative regulations in place concerning personal items of employees at the work site, the Court found that public employees did have a reasonable expectation of privacy, albeit qualified:

> The operational realities of the workplace...may make *some* employees' expectations of privacy unrealistic 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.[58]

Although the Court determined that, under the facts of this case, Dr. Ortega had a reasonable expectation of privacy in his office, and that employees working for the government still retained their Fourth Amendment rights, the majority of the Court held that such decisions must be made upon a case by case basis. Moreover, the Court said that "[t]he legitimate privacy interests of public employees in the private objects they bring to the workplace may be substantial. Against these privacy interests, however, must be balanced the realities of the workplace, which strongly suggest that a warrant requirement would be unworkable."[59]

In a further discussion of the realities of the public workplace, the Court went on to say that "work-related searches are merely incident to the primary business of the agency. Under these circumstances, the imposition of a warrant requirement would conflict with 'the common-sense realization that government offices could not function if every employment decision became a constitutional matter.'"[60]

As noted, the plurality determined that a requirement of probable cause to institute a search of a public employee's office was impracticable and unworkable under the conditions of the public workplace. In its stead, the Court indicated that the standard to be used is one of reasonableness in determining whether the search was justified at its inception, and whether the search as conducted is reasonably related in its scope to the circumstances that originally justified the interference.

What we know from the *Ortega* decision is that the Fourth Amendment does provide constitutional protection to employees in the public sector and that such employees do enjoy a "reasonable expectation of privacy" in the workplace; however, depending upon the circumstances of each case, this expectation may be very limited. Balanced against this expectation is the government employer's need for "supervision, control, and the efficient operation of the workplace" and ultimately whether the search conducted was reasonable under the circumstances.

It seems clear that if Dr. Ortega's office had been readily accessible to a number of employees, or if the facts demonstrated that the search was justified at its inception and permissible in its scope, the Court would have found the search to be permissible and upheld the dismissal. The search would be justified in this case, at its inception, if there were reasonable grounds to believe that a search would uncover evidence of the employees' work-related misconduct, or if the search were necessary for a noninvestigatory purpose, such as to retrieve a file. It is permissible in its scope when the search is reasonably related to its objectives and not "excessively intrusive" in light of its purpose.

After years in the courts, Dr. Ortega obtained a jury verdict holding the defendants liable under 42 U.S.C. Section 1983. The judgment was affirmed by the Ninth Circuit on the basis that there was insufficient evidence on the claim of sexual harassment to justify the search at the outset and that therefore the search was unreasonable.[61]

(A) REASONABLE EXPECTATION OF PRIVACY: CIRCUIT COURT DECISIONS

Reasonable notice that employment areas are subject to a management search override an employee's expectation of privacy. A decision held that language contained in a collective bargaining agreement, along with a waiver signed by individual workers permitting ran-

[58] *Id.* at 717.
[59] *Id.* at 721.
[60] *Id.* at 722.
[61] Ortega v. O'Connor, 146 F.3d 1149 (9th Cir. 1998).

dom inspection of workers' lockers, in fact provided the employees with notice of the random inspection policy, thereby lessening the employees' expectation of privacy.[62] As a result, the court held that the employees had "no reasonable expectation of privacy" that would be protected by the Fourth Amendment.

In another case, the plaintiff was employed by the Navy as a civilian engineer to work on secret weapons-related projects and had the necessary security clearance to do so.[63] The employer, acting on an anonymous tip, seized an envelope from the plaintiff's credenza containing the offensive material for which the plaintiff was subsequently fired. In this case, the court held that while the plaintiff may have had a subjective expectation of privacy regarding an allegedly locked credenza and a manila envelope contained therein, he could not have an objectively reasonable expectation of privacy because of the nature of the work he was doing.

Random mandatory drug testing by urinalysis of U.S. Army civilian employees in sensitive positions was held not to violate the Fourth Amendment.[64] However, the same test administered to employees considered to be performing work of a less sensitive nature was held to be violative of their Fourth Amendment guarantees. Distinguishing the first group, the court in citing *O'Connor v. Ortega*, supra, stated that "[the] operational realities of the work place...are such that a diminished expectation of privacy attaches to information relating to the physical condition of covered employees."[65]

A "diminished expectation of privacy" is a counterpart to the expectation of privacy. It has been held that an employee does enjoy a reasonable expectation of privacy in areas given over to his or her exclusive control, unless the employee had been put on notice by his employer that searches of the employee's desk might occur periodically for work-related purposes.[66] The Third Circuit held that random breathalyzer and urinalysis testing for drugs and alcohol was permitted as an exception to the warrant requirement for the activity being conducted, in this case horse racing, since it was a highly regulated practice by the State, carrying with it a diminished expectation of privacy.[67]

Regarding a related issue, in *United States v. Buettner-Janusch*,[68] the Second Circuit held that the consent to search may be given by persons having coexisting authority over, or a sufficient relationship to, access to certain areas even if the materials that are being sought belong to a third party. Despite whatever independent expectation of privacy the appellant may have had in certain areas of the laboratory, his granting permission of access to another empowered the latter to provide access to government agents without a warrant.

(B) THE SCOPE OF THE SEARCH

Under the *Ortega* line of cases, the search of an employee's premises is reasonable in scope if the action taken by the employer is reasonably related to the search's objectives and is not overly intrusive in light of the nature of the alleged misconduct. In a case heard by the Seventh Circuit, the complainant was a state child protection investigator for the State of Illinois.[69] Because of a lack of adequate storage space, the employee, Gossmeyer, had purchased at her own expense a four-drawer file cabinet with a lock and a two-door storage unit with a lock. Acting on an anonymous tip that Gossmeyer kept child pornography in her file cabinet, the State Office of the Inspector General essentially raided the office, pried open her desk and file cabinet, and found nothing. In this case, the court held that a workplace search was reasonable if justified at its inception and reasonably related in scope to the circumstances that prompted the search.

Interpreting and following the *Ortega* case, the Seventh Circuit found that a warrantless search of a police officer's desk and his locked personal briefcase, as part of an internal investigation, did not violate the plaintiff"s Fourth Amendment privacy rights.[70] The court indicated that a "reasonableness" standard is to be applied to such cases and as long as the search is based upon a reasonable suspicion that a search will retrieve work-related materials or materials indicating a violation of law or rules, it is acceptable. In describing the standard, the court stated that "[r]easonableness depends upon the circumstances presented in a given situation and upon balancing the public, governmental, and private interests at stake in the situation."[71]

2. Personnel Records

A basic thrust of the Federal Freedom of Information Act (FOIA) and its state counterparts is that these acts require public disclosure of all information possessed by public agencies unless specifically excepted.[72] These exceptions are to be narrowly construed to effect the purpose of the Act, which has been defined as disclo-

---

[62] American Postal Workers Union v. United States Postal Service, 871 F.2d 556 (6th Cir. 1989).

[63] Schowengerdt v. United States, 944 F.2d 483 (9th Cir. 1991).

[64] National Fed'n of Fed. Employees v. Chaney, 884 F.2d 603 (D.C. Cir. 1989).

[65] 884 F.2d 603 at 613.

[66] Schowengerdt v. General Dynamics Corp. 823 F.2d. 1328 (9th Cir. 1987).

[67] Schoemaker v. Handel, 795 F.2d 1136 (3d Cir. 1986).

[68] 646 F.2d 759 (2d Cir. 1981).

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

[70] Shields v. Burge, 874 F.2d. 1201 (7th Cir. 1989).

[71] *Supra* at 1204.

[72] For an indepth discussion of FOIA, see Orrin F. Finch and Gary A. Geren, *Freedom of Information Acts, Federal Data Collections, and Disclosure Statutes Applicable to Highway Projects and the Discovery Process,* National Cooperative Highway Research Program, LEGAL RESEARCH DIGEST 33 (Trans. Research Board) April 1995.

sure rather than secrecy.[73] Generally, with regard to the state FOIAs, with few exceptions, they are similar to the Federal Act and generally contain the same types of exemptions.[74]

Department of the Air Force v. Rose[75] expresses the general rule. This case involved a petition against the Department of the Air Force and certain officers by current and former student editors of the *New York University Law Review* seeking access to case summaries of Air Force Academy disciplinary hearings. The Air Force denied access on the basis that the records contained personal information about cadets and were therefore exempt under the FOIA.[76] The Court found that summaries should be produced before the trial court for an in camera inspection and redaction of identifying materials in order to safeguard the privacy interests of the individuals involved.

The clear purpose of the Federal FOIA was to overcome government secrecy, the inherent characteristic of bureaucracy to keep its secrets, and to open up government records to the public. At the same time, it was recognized that there are certain things that by their very nature must remain privileged from disclosure to the general public. The most notable exception to the release of information pursuant to the FOIA for purposes of the subject under review is 5 U.S.C. Section 532(b)(6), which precludes disclosure of "[p]ersonnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy…."

It has been held that the term "similar files" as used in the statute includes all information pertaining to that particular individual.[77]

(A) STANDARD FOR RELEASE OF PERSONNEL RECORDS

The Supreme Court in *Rose* noted that the exemption under discussion recognized the sanctity of individual personnel and medical records; however, there were limitations. The Court held that the purpose of the exemptions was not to provide blanket exclusions for anything that might be contained in a personnel or medical file, but rather "[t]he limitation of a 'clearly unwarranted invasion of personal privacy' provides a proper balance between the protection of an individual's right of privacy and the preservation of the public's right to government information by excluding those kinds of files, the disclosure of which might harm the individual."[78]

In the *Rose* case, the Court held that summaries of the type of information sought and redacted versions, excluding the names of specific cadets, were outside the realm of exemption and clearly discoverable under the FOIA. While the Court clearly understood Congress's concern for the protection of confidential personal data, unless the information satisfies the criteria of being an "unwarranted invasion of privacy," it enjoys no privilege from discovery.

In another case a newspaper brought suit against the government for information regarding an alleged narcotics conspiracy involving a former sheriff.[79] The court determined that where a request for such information would "not contribute significantly to public understanding of the operations or activities of the government and seeks law enforcement information on private individuals, the court need not undertake a balancing test or order an *in camera* inspection before it decides that the documents are exempt from disclosure."[80]

However, where information or affidavits utilized to support the need for the exemption are insufficiently detailed or contradictory, the court may be precluded from exempting such information without an *in camera* inspection.[81]

The Fifth Circuit permitted an employer to get the unredacted list of its employees who voted in an National Labor Relations Board (NLRB)-sponsored election on the basis that it did not constitute a clearly unwarranted invasion of personal privacy.[82] While upholding the principle that disclosure would not be permitted if the information did not serve the purpose of informing citizens about the activities of the government, nevertheless the court found that employees who attended the election had no protected privacy interests on that mere fact alone.

A Seventh Circuit case found that the FOIA did not require the disclosure of names and home addresses of employees, since the disclosure would constitute a violation of 5 U.S.C.A. Section 552 (b)(6).[83] A decision made less than 2 months later by the Fifth Circuit was diametrically opposed, in that the court held that the names and addresses of employees are fully discoverable under the FOIA and did not prohibit disclosure under the exemption on the basis that the union had a paramount vested interest in obtaining the names and addresses of employees for collective bargaining purposes.[84]

---

[73] 5 U.S.C.S. § 552(b); Dept. of the Air Force v. Rose, 425 U.S. 352 (1976).

[74] 26 A.L.R. 666, *What Constitutes Personal Matters Exempt from Disclosure by Invasion of Privacy Exemption Under State Freedom of Information Act*.

[75] 425 U.S. 352 (1976).

[76] 5 U.S.C.S. § 552(b)(6).

[77] Lepelletier v. FDIC, 977 F. Supp. 456 (D.C. Dist. 1997).

[78] 425 U.S. 352, 372.

[79] McNamara v. United States Dept. of Justice, 974 F. Supp. 946 (W.D. Tex. 1977).

[80] *Supra* at 955.

[81] Armstrong v. Executive Office of the President, 97 F.3d 575 (D.C. Cir. 1966).

[82] Avondale Industries Inc. v. NLRB, 90 F.3d 955 (5th Cir. 1966).

[83] United States Dept. of Labor v. Federal Labor Relations Auth., 975 F.2d 348 (7th Cir. 1992).

[84] Federal Labor Relations Auth. v. United States Dept. of Defense, 975 F.2d 1105 (5th Cir. 1992).

While holding that employees' sick leave records are closely akin to medical files and therefore constituted "similar files" under the terms of the FOIA exemption, the Ninth Circuit Court held that the public had a right to the disclosure of sick leave records of an FCC employee, in effect ruling that the privacy interests of the employees were superseded by compelling public interest in knowing the contents of the sick leave records.[85]

It should be noted that certain matters that might otherwise be private under 5 U.S.C.S. Section 552(b) may in fact be subject to disclosure under another statutory provision. Federal agencies have a great deal of information about every United States citizen, such as social security number, IRS information, etc., generally protected by law from disclosure to others, although there are certain conditions under which such information may be released.[86] This exception has led to a great deal of discussion as to when disclosure has been authorized because of a "routine use" of that record.[87]

(B) BURDEN OF PROOF

As a general rule, the party asserting the exemption to prevent disclosure has the burden to prove that the claim is warranted under the circumstances.[88] It is also axiomatic that documents containing otherwise privileged information may become available for public inspection, if the privileged information can be removed. As an example, a New Jersey court held that federal housing assistance contracts were subject to disclosure since information that was otherwise privileged was redacted from the documents.[89]

Although ostensibly matters that are truly personal contained in a personnel file are generally exempt from disclosure, in a close case the decision generally will be based upon the purpose for which the records are being sought. The names and addresses of retired and disabled federal employees were nondisclosable under the FOIA to an association of retired federal employees on the grounds that it would clearly be an unwarranted invasion of personal privacy.[90] Conversely, another court held that payroll records of a government contractor, which included names, addresses, phone numbers, and social security numbers, were discoverable on the basis that public interest in ensuring compliance with Davis Bacon rates was superior to privacy interests of the employees.[91]

(C) STATE COURT DECISIONS

State courts have dealt with similar issues regarding when and what information from personal files can be released. In a Michigan case,[92] the plaintiff sought release of the police department's traffic accident computer tape, which contained names, addresses and other information of persons involved in city accidents in 1980, for purposes of doing a statistical analysis. The court in this case overlooked the purpose for which the records were being sought, but held that the records were exempt from disclosure based upon the nature of the information contained therein.

A corporation engaged in representing public employment retirees was determined to be entitled to obtain the names and addresses of public employee retirees.[93] However, because of the nature of the information being sought and perhaps the misuse to which the information could be applied, a New York court held that the release of correction officers' social security numbers was precluded from disclosure under the FOIA absent written consent.[94]

A person who sought disclosure of another vehicle owner's home address from the Motor Vehicle Division for personal informational purposes was denied access.[95] The court held that even though such disclosure may serve the public interest in certain circumstances, once it has been established that the records are of a personal nature, clear and convincing evidence must be submitted in order to allow an unreasonable invasion of privacy.

A Pennsylvania newspaper sought the disclosure of itemized cellular telephone bills of county officials.[96] The court held that the privacy interests in telephone numbers listed on the telephone bills did not outweigh the public's right to know how its tax dollars were being spent, and therefore the court required disclosure of the telephone numbers called.

3. Polygraph Testing

Since the inception of its use the reliability of the polygraph has been consistently called into question. Its use as an employment tool has caused substantial difficulties both from the employer and the employee perspective, to the extent that its results have often been disallowed or statutory protections have been devised to prevent its use. In 1988, Congress enacted the Employee Protection Act of 1988, 29 U.S.C.S. Section 2000 et. seq., which prohibits employers "engaged in or affecting commerce or the production of goods for com-

---

[85] Dobronski v. FCC, 17 F.3d 275 (9th Cir. 1994).

[86] 5 U.S.C.S. § 552 a(b).

[87] *See* 107 A.L.R. FED 857, *What Constitutes "Routine Use" Disclosure of Employee Records Exempted From Provisions of the Privacy Act of 1974 Under 5 U.S.C.S. Section 552a(b)(3)*.

[88] Rosenfeld v. United States Dept. of Justice, 57 F.3d 803 (9th Cir. 1995).

[89] Lakewood Residents v. Lakewood Housing Auth., 682 A.2d 1201 (N.J. Super. A.D. 1996).

[90] National Assn. of Retired Fed. Employees v. Horner, 879 F.2d 873 (D.C. Cir. 1989).

[91] Painting Industry of Hawaii v. United States Dept. of Air Force, 756 F. Supp. 452 (D. Haw. 1990).

[92] Mullen v. Detroit Police Dept, 348 N.W.2d 708 (Mich. 1984).

[93] State *ex rel*. Public Employee Retirees v. Public Employees Retirement System of Ohio, 397 N.E.2d 1191 (1979).

[94] Seelig v. Sielaff, 607 N.Y.S.2d 300 (A.D. 1 Dept. 1994).

[95] Jordan v. MVD, 763 P.2d 420 (Or. App. 1988) *aff'd*. 781 P.2d 1203 (Or. 1989).

[96] PG Publishing Co. v. County of Washington, 638 A.2d 422 (Pa. Commw. 1994).

merce" from requiring employees to take a lie detector test as a precondition or condition of continued employment. There are several exemptions contained within the Act; the most notable for purposes of this paper is 29 U.S.C.S. Section 2006(a), which reads "[t]his Act...shall not apply with respect to the United States Government, any State or local government, or any political subdivision of a State or local government."

While it may be left open to interpretation regarding the reason Congress chose to exclude public employees, some states have addressed the exclusion by adopting legislation to cover all employees working within the state, including public employees.[97] For example, the State of Delaware has a blanket exclusion clause against the use of a polygraph as a condition or precondition of employment. There is the notable exception of detective/ polygraph tests utilized by law enforcement agencies in the performance of their duties and specifically to permit law enforcement agencies to perform background examinations of police applicants. 19 Delaware Code Section 704(s). The reader is advised to consult the statutory authority within the pertinent jurisdiction. In those jurisdictions that have not adopted exclusory legislation, the common law is still applicable.

(A) STATE COURT CASES INVOLVING PUBLIC EMPLOYEES

The Missouri Court of Appeals upheld the dismissal of two Kansas City Water Department employees for their refusal to submit to a polygraph examination in connection with a missing property investigation.[98] The court held that, while the results of a polygraph examination would be inadmissible in a criminal proceeding, requiring employees to submit to the lie detector test and its use as a part of a lawful investigation regarding missing property was permissible, and that the city had the right to discharge such employees for their refusal to take the test. In a similar case, the New York Court of Appeals held that a water and sewer maintenance employee did not have a constitutional right to refuse to submit to a lie detector test when directed to do so by his employer.[99]

Similarly, a police officer being investigated for use of marijuana was directed to take a polygraph test pursuant to city regulation upon the condition that the results would not be used in a subsequent criminal proceeding against her, but that she would be dismissed for insubordination for her refusal to take the test.[100] Relying on the United States Supreme Court decisions in *Lefkowitz v. Turley*,[101] *Kastigar v. United States*,[102] *Gardner v. Broderick*,[103] *Garrity v. New Jersey*,[104] and others, the Supreme Court of Mississippi reiterated the requirement to take a polygraph test in that circumstance and held that the appellant "had no constitutional right to refuse and that her refusal justified her dismissal."

One court reached a contrary ruling. The Florida Supreme Court refused to uphold the dismissal of a police officer under investigation for an attempted theft of money from a bank where the officer served special duty as a security guard at the time of the incident.[105] The court cited the unreliability of the test and also indicated that once hired, the police officer had certain constitutional protections against job deprivation.

4. Psychological Testing

Release of psychological records and the results of psychological testing results follows the same logic as that which applies to personnel records. Generally, they are exempt from disclosure on privacy grounds unless some supervening reason exists to warrant their release.

A municipal requirement that job applicants for firefighter positions undergo personality testing in order to determine their ability to withstand stress was upheld by a federal district court in New Jersey.[106] The basis for the decision was that the municipality's interests in maintaining public safety was sufficiently important to override any privacy rights that the applicants may have had. It is noteworthy that in this case the court required the municipality to have specific regulations limiting access to the data.

McKenna was filed as a 1983 action by successful and unsuccessful applicants for the Jersey City Fire Department on the basis that they were required to undergo a battery of psychological testing prior to being considered for the position. The district court found that the testing included questions about social, sexual, and political beliefs and that the process constituted an infringement upon the privacy rights of the plaintiffs in derogation of their First and Fourteenth Amendment rights. Nevertheless, the basis for the decision against the plaintiffs was that the city's interest in ensuring that the applicants could cope with the psychological pressures of the job superseded the rights of the individuals.

Certain tests are excluded on the basis of reliability. Use of the results of a psychological stress evaluation (PSE) or voice stress tests has generally been held to be inadmissible in both civil and criminal proceedings because of the unreliability of such tests.[107]

---

[97] 19 DEL. CODE 704.

[98] Campbell v. Personnel Board of Kansas City, 666 S.W.2d 806 (Mo. App. 1984).

[99] People v. Mandel, 401 N.E.2d 185 (N.Y. App. 1979).

[100] Knebel v. City of Biloxi, 453 So. 2d 1037 (Miss. 1984).

[101] 414 U.S. 70 (1973).

[102] 406 U.S. 441 (1972).

[103] 392 U.S. 273 (1968).

[104] 385 U.S. 493 (1967).

[105] Farmer v. City of Ft. Lauderdale, 427 So. 2d 187 (Fla. 1983).

[106] McKenna v. Fargo, 451 F. Supp. 1355 (D. N.J. 1978) *aff'd* 601 F.2d 575 (3d Cir. 1979).

[107] U.S. v. Traficant, 566 F. Supp. 1046 (ND Ohio 1983).

5. Drug and Alcohol Testing

Historically, medical information regarding an individual and its inviolability has been held to be privileged between the doctor and the patient. At least one federal district court has held that confidentiality of such information is a constitutionally protected privacy interest. The Ninth Circuit has held that employees have a right to genetic and medical privacy.[108] The court held that nonconsensual testing for sensitive medical information pursuant to general employee health examinations stated a cause of action for invasion of privacy against the defendant, a research facility operated by federal and state agencies. The court noted that "[t]he constitutionally protected privacy interest in avoiding disclosure of personal matters clearly encompasses medical information and its confidentiality."[109]

Courts have recognized the importance of public employers' creating a safe working environment and have held that drug-testing policies do not necessarily constitute an invasion of privacy.[110] In *Skinner,* the Supreme Court upheld the Federal Railroad Administration's mandatory drug and alcohol testing program of employees in safety-sensitive positions on a postaccident basis or in circumstances in which employees were deemed to have violated certain safety rules, holding that such testing was not violative of the employee's rights against unreasonable searches and seizures.

The Court in *Skinner* held that the implementation of the policy did in fact constitute a search within the context of the Fourth Amendment. However, based upon the nature of the work performed by the employees, such searches were reasonable even though conducted without a search warrant or based upon any showing of individualized suspicion. The Court used a balancing test and held that drug testing was not an "unduly extensive imposition" on the subjected person's privacy. Moreover, employees working in a highly regulated industry had "diminished privacy expectations" in order to insure the safety of the public.

In *O'Connor v. Ortega*,[111] the Supreme Court held that a prerequisite showing of "individualized suspicion," constituting an essential element of a "reasonableness" standard previously adopted by the Court, was not required, since it was a critical element of the factual setting of the case and initiated the hospital officials' actions. In *Skinner*, the Court found that where important governmental interests, such as safety on the railroads, were advanced by minimal intrusion on the privacy of the employees, individualized suspicion would not be a necessary element.

In another case involving a public transit agency, the Southeastern Pennsylvania Transportation Authority (SEPTA) instituted a program to audit prescription drug use by its employees in order to determine:

- Whether employees were submitting fraudulent claims.
- Whether there was drug abuse among the employees.
- Whether the sole provider of prescription drugs to SEPTA employees was using generic drugs rather than the name brands in order to hold down costs.
- The cost to SEPTA of fertility drugs and the cost of medications to help employees stop smoking.[112]

In this case the pharmacy submitted information to SEPTA, which included names of the employees who had filled prescriptions costing $100.00 or more in a one month period, information regarding the prescribing physician, the date of the prescription, the name of the drug prescribed, the number of days supplied, and the total cost. Based upon this information SEPTA was able to determine that one of its employees had AIDS. This information was related to several SEPTA managers, and when the employee found out, he filed suit.

The Third Circuit in *Doe* found for SEPTA, ruling that the self-insured employers' need for accessibility to the employees' prescription records, pursuant to SEPTA's program to monitor its prescription plan, outweighed the interests of the employee in keeping his prescriptions confidential, provided that the disclosure was limited to those with a need to know. The court determined that the intrusion into the plaintiff's privacy was minimal and did not give rise to the level of a constitutional violation, particularly since the plaintiff had suffered no discrimination, harassment, or economic loss.

On the same day as the *Skinner*[113] decision, the U. S. Supreme Court issued an opinion in another drug testing case.[114] The latter companion case also dealt with the conflict caused by a drug-testing requirement and the privacy interests of public employees. Consistent with the holding in *Skinner*, in *Von Raab*, the U.S. Customs Service adopted a urinalysis drug testing program for its employees on a pre-ascension basis. If an employee sought promotion or transfer to a position that: (1) involved the interdiction of illegal drugs; (2) required the carrying of a firearm; or (3) required the handling of classified information, they were required to take the test as a precondition of the new employment status.

As in *Skinner*, the Court held that there was a significant government "action involved, making the 4th Amendment" applicable and thereby extending its protection to the affected employees. Nevertheless, a war-

---

[108] Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260 (9th Cir. 1998).

[109] *Id*. at 1269.

[110] Skinner v. Railway Labor Executives' Ass'n., 489 U.S. 602 (1989).

[111] 480 U.S. 709 (1987).

[112] In Doe vs. Southeastern Pa. Transp. Auth., 72 F.3d 1133 (3d Cir. 1995); *Cert. Den*.,____ U.S. __, 117 S. Ct. 51 (1996).

[113] Skinner v. Railway Labor Executives' Ass'n., 489 U.S. 602 (1989).

[114] National Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989).

rantless, suspicionless search in the first two instances was reasonable, since the government interests outweighed the privacy rights of its employees. The Court did not decide the constitutionality of the search involving the employees who handled "classified" material since the record was somewhat vague on what type of information fit that category and to whom it would apply. The case was remanded to the trial court for further findings of fact on the last issue.

A physician enrolled in a medical residency program was requested to submit to private urinalysis drug testing based upon her supervisor's observation of what appeared to be erratic behavior.[115] The plaintiff alleged a violation of her Fourth Amendment rights and brought suit pursuant to 42 U.S.C.S. Section 1983, 28 U.S.C. Section 2201. The court determined that this instance did not rise to the level required for individualized suspicion; nevertheless, the fact that she was a physician created a circumstance in which the requirement of a drug test was warranted based upon "special need."

Systematic, formalized testing procedures have been upheld as reasonable.[116] The Ninth Circuit has held that the Federal Highway Administration regulations that authorized random biennial, preemployment, and postaccident testing of motor carrier employees were not a violation of their Fourth Amendment rights.

A case brought against the Secretary of Defense involved the constitutionality of the United States Army's policy of mandatory random urinalysis drug testing for civilian employees.[117] The court held that the policy did not violate the Fourth Amendment with regard to employees in safety sensitive positions in aviation, police work, and security, and "direct service staff" who were primarily drug counselors, citing the *Ortega* case for the proposition that persons in these types of positions necessarily have a "diminished expectation of privacy."[118] However, random mandatory drug testing by urinalysis of civilian employees deemed to be in less safety sensitive positions was held to be violative of the Fourth Amendment. In making the distinction, the court said "these employees lack the necessary causal connection between the employees' duties and the feared harm."[119]

(A) STATE COURT CASES

State courts appear to have adopted the same trend as the Supreme Court in carving out exceptions to personal privacy interests where greater public policy interests are at stake. The Supreme Judicial Court of Massachusetts upheld the employers' universal drug testing program, which required at-will employees to be randomly selected for drug testing at least once every 3 years as a condition of continued employment.[120] A state court in Florida upheld as constitutional a regulation requiring job applicants to sign an affidavit stating that they had not used tobacco in the preceding year as a precondition of having their applications considered.[121] The court found that the requirement did not violate the privacy protection the job applicants might have under the Constitution and that their interests were not within the "zone of privacy" enunciated in *Roe*[122] or the state constitution.

The California Supreme Court weighed the privacy interests of student athletes against the NCAA requirement of athletic event drug testing in order to protect the safety of the student athletes and to provide for fair and vigorous competition.[123] The court, in upholding the NCAA testing, determined by the nature of the type of activity involved that the student athlete had a reduced expectation of privacy as a result of his or her participation and that consequently the NCAA's interests were more compelling.

6. Surveillance

Surveillance of one's activities conducted in the open cannot give rise to a Fourth Amendment constitutional claim.[124] In order for the Fourth Amendment to apply, the claimant must have a protected interest that is invaded by some governmental activity. As the Supreme Court said in *Smith,* "[t]he application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."[125]

The Supreme Court in *Smith* also commented on its decision in *Katz v. United States*,[126] which overruled its decision in *Olmstead v. United States*.[127] The Supreme Court, in *Katz*, ruled that by attaching an electronic listening device to the outside of a public phone booth, government agents had violated the constitutional rights of the claimant, thereby rejecting the argument that a search protected by the Fourth Amendment had to involve a "physical intrusion" into a "constitutionally protected area." In *Katz*, supra, the question was whether the claimant had a reasonable expectation of privacy. In *Smith*, supra, this was to be determined by saying that:

> This inquiry...normally embraces two discrete questions. The first is whether the individual, by his conduct has, "exhibited an actual (subjective) expectation of pri-

---

[115] Pearce v. Smith, 117 F.3d. 866 (5th Cir. 1997).

[116] International Bhd. of Teamsters v. Department of Transp., 932 F.2d 1292 (9th Cir. 1991).

[117] National Fed'n of Fed. Employees v. Chaney, 884 F. 2d 603 (D.C. Cir. 1989).

[118] O'Connor v. Ortega, 480 U.S. 709 (1987).

[119] 884 F.2d 603 at 614.

[120] Webster v. Motorola, Inc., 637 N.E.2d 203 (Mass. 1994).

[121] City of North Miami v. Kurtz, 653 So. 2d 1025 (Fla. 1995).

[122] Roe v. Wade, 410 U.S. 113 (1973).

[123] Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994).

[124] Smith v. Maryland, 442 U.S. 735 (1979).

[125] *Id.* at 740.

[126] 389 U.S. 347 (1967).

[127] 277 U.S. 438 (1928).

> vacy,"...whether...the individual has shown that he seeks to preserve (something) as private"...The second question is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as reasonable"...whether...the individual's expectation, viewed objectively, is "justifiable" under the circumstances."[128]

An employer who routinely filmed its factory and employees in the performance of their duties in order to improve safety, efficiency, manufacturing methods, and processes was found not to have invaded its employees' privacy rights. [129] However, it has been held that people using a restroom facility have a "reasonable expectation of privacy" from such intrusions.[130]

In a case in the Seventh Circuit, seven female employees and a female independent contractor appealed a district court dismissal of their suit against the company alleging that video surveillance of the workplace violated their right to privacy.[131] The employer argued that it had the right to videotape its employees under the "management rights" clause of the collective bargaining agreement. Arbitration was determined to be the proper remedy for the employees. The female independent contractor argued that a videotape in the ladies' locker room (pointed at the door) violated her right to privacy, but the court held that in the absence of evidence that she used the locker room, or that her privacy was compromised, the case was dismissed.

In an Oregon case, the court dismissed an invasion of privacy case against the company for taking several roles of film of the plaintiff, who had filed a workman's compensation case against the company.[132] The company, through use of the film that it had taken, was able to demonstrate to the court that the plaintiff was able to perform various tasks in and around the home. The court reasoned that the employer had the right to reasonably investigate the claim and that the employee, by filing the claim, waived his right of privacy.[133]

A school district that videotaped a classroom in session over the objection of a teacher did not violate the teacher's right to privacy.[134] As the court in this case stated, there can be no invasion of privacy when one's activity is performed in public view. A cause of action for invasion of privacy can only arise if the activity falls within one's "zone of privacy," which in turn can only be present when one has a reasonable expectation of privacy.

In looking at this rule in light of the decision in *O'Connor v. Ortega*,[135] it would appear that public employees have no reasonable expectation of privacy in the public workplace and that there would be no prohibition against videotaping, photographing, or otherwise committing to film public employees in this setting. Perhaps only in the case of an employee having his or her own office to which others are denied access could one have a reasonable expectation of privacy, and then only depending upon the totality of circumstances may one be protected from such intrusions.

7. Privacy Rights on Public Transit

Although it appears that the courts have yet to deal with a case clearly dispositive of the issue concerning the extent to which the governmental authority can monitor the movement of the transit-using public or the information garnered from the use of smart fare-cards, there is authority to suggest that one utilizing these services has a lesser expectation of privacy than one can expect in their personal residence.[136] It has been held that persons traveling on public transportation have exposed themselves to the public arena and do not have the same privacy interests that attach to a person in his house.[137] As noted by the court "it is generally recognized that the privacy interest of people who are in transit [i.e. on a bus, train, or airplane] on public thoroughfares [is] substantially less than those that attach to a fixed dwelling."[138]

The Constitution does not guarantee to each passenger on public transit the same right that is secured to persons within their homes.[139] The interests of all parties must be considered as well as the nature of the intrusion. A public conveyance has different characteristics with relation to privacy than that accorded to a personal dwelling.[140] As an example, a train passenger has a reduced expectation of privacy in a "roomette" based upon a reasonable belief by law enforcement officials that it contains illegal goods and is therefore not entitled to the protection of probable cause.[141] A warrantless search of a mobile home was considered to not constitute a violation of the Fourth Amendment since it was not a "fixed dwelling."[142]

Cameras used for law enforcement purposes in public areas appear to be a legitimate exercise of police power

---

[128] 422 U.S. 740 (Cit. Omit.).

[129] Thomas v. General Elec. Co., 207 F. Supp. 792 (W.D. Ky. 1962).

[130] 74 A.L.R. 4th 508, *Privacy Expectations in Restrooms.*

[131] Brazinski v. Amoco Petroleum Additives Co., 6 F.3d 1176 (7th Cir. 1993).

[132] McClain v. Boise Cascade Corp., 533 P.2d 343 (Or. 1975).

[133] *Also see*, 13 A.L.R. 3d 1025, *Right of Privacy-Surveillance.*

[134] Roberts v. Houston Indep. School Dist., 788 S.W.2d 107 (Tex. App., Hous. 1st Dist. 1990).

[135] 480 U.S. 709 (1987).

[136] New York v. Class, 475 U.S. 106 (1986); Cardell v. Lewis, 417 U.S. 583 (1974); Katz v. United States, 389 U.S. 347 (1967).

[137] U.S. v. McDonald, 100 F.3d 1320 (7th Cir. 1996).

[138] *Id.* at 1324-25, citing United States v. Rem, 984 F.2d 806 (7th Cir. 1993), *cert. den.* 510 U.S. 913 (1993).

[139] Public Util. Comm'n v. Pollak, 343 U.S. 451 (1952).

[140] United States v. Whitehead, 849 F.2d 849 (4th Cir. 1988).

[141] United States v. Trayer, 701 F. Supp. 250 (D. DC 1988) *aff'd* 898 F.2d 805, *cert. den*. 498 U.S. 839 (1990).

[142] California v. Carney, 471 U.S. 386 (1985).

without infringing on the rights of motorists.[143] The placement of cameras for safety purposes at public transportation facilities and even on transit vehicles may depend upon whether the character of the location is classified as a public or nonpublic location.[144] The Supreme Court has delineated what constitutes a public forum.[145] Discreet and reasonable surveillance conducted in a public place is not actionable as an invasion of one's constitutional rights.[146] As to what constitutes the expectations of the individual in any situation arising on a transit vehicle or facility will be determined by balancing the interests of the individual against those of the public at large.[147] More than likely, the interests of the government in placing cameras at strategic locations for safety purposes will be paramount to personal privacy interests.[148] It has been held that persons being videotaped while riding a bus did not have a reasonable expectation of privacy.[149] In *Hoffman*, the plaintiff claimed that the City of New York and the Metropolitan Transportation Authority (MTA) had conducted videotaping of her movement on various public buses and subways throughout the city for an 11-year period. She brought an action pursuant to 42 U.S.C. Section 1983, claiming a violation of her constitutional right to privacy. Defendants moved to dismiss on the basis that the plaintiff failed to state a cognizable claim under 42 U.S.C. Section 1983.

Citing *Katz* and other authorities,[150] the court held that by riding public transit, the plaintiff knowingly exposed herself to public observation and therefore had no recognizable claim. The court found that in order to go forward the plaintiff needed to have a "constitutionally protected reasonable expectation of privacy," which is the standard to be used in a Fourth Amendment analysis of the facts. Even if the plaintiff had taken measures to conceal her activity, but was observed from a public vantage point, she has no constitutionally protected interest.[151]

[143] *Photographic Traffic Law Enforcement, supra*, n.34.

[144] New York Magazine v. Metropolitan Transp. Auth., 136 F.3d 123 (2d Cir. 1998); *Also see*; Herring and D'Auri*, Restrictions on Speech and Expressive Activities in Transit Terminals and Facilities*, 10 LEGAL RESEARCH DIG. (1998).

[145] *See* International Soc'y for Krisna Consciousness v. Lee, 505 U.S. 672, and other cases cited in New York Magazine v. Metropolitan Transp. Auth., *supra,* 136 F.3d at 128.

[146] Frazier v. Southeastern Pa. Transp. Auth., 907 F. Supp. 116 (E.D. Pa. 1995).

[147] Div. 241 Amalgamated Transit U. (AFL-CIO) v. Suscy, 538 F.2d 1264 (7th Cir. 1976).

[148] Roe v. Wade, 410 U.S. 113 (1973).

[149] Hoffman v. City of New York, 1998 WL 212894 (E.D. N.Y.).

[150] Katz v. United States, 389 U.S. 347 (1976); California v. Ciraolo, 476 U.S. 207 (1986); United States v. Caputo, 808 F.2d 963 (2nd Cir. 1987); United States v. Fields, 113 F.3d 313 (2d Cir.), *cert. den*. U.S.___, 118 S. Ct. 434 (1997).

[151] California v. Ciraolo, and United States v. Fields, *supra*.

8. Privacy Rights and Public Records

Generally stated, under federal and state FOIAs, any matter not otherwise privileged is subject to discovery.[152] Included as items that are protected under the law are personnel records, medical records, and similar files. The Federal FOIA provides for very limited exceptions from disclosure at 5 U.S.C.S. Section 552 (b)(6).[153] It has been held that the Federal FOIA is to be liberally construed in favor of disclosure, and its exemptions are to be narrowly construed.[154]

While it has been held that the FOIA was not intended as a substitute for discovery in litigation,[155] very few public records are held sacrosanct. Moreover, unless some claim of privilege cognizable under law is asserted, any member of the public has a right to the access and the disclosure of the public record, even though such person may have a special interest in its disclosure.[156]

Thus it would seem that unless a particular record is excepted from disclosure by statute, it is accessible under the FOIA provisions or some other statutory provision.[157] Records that are not otherwise disclosable, such as personnel or medical records, however, are still subject to the normal rules that subject such information to disclosure either by subpoena or through the rules of discovery. Thus for example, applications submitted to a paratransit agency are generally subject to disclosure unless they contain privileged medical information; however, that would not preclude their disclosure to other government agencies, insurance companies, or private litigants in the proper setting.

C. Privacy in the Public Workplace: Oral, Wire, and Electronic Communication

1. Introduction

The Fourth Amendment protects against unwarranted government intrusion into oral communications. Since the Fourth Amendment is applicable to and protects people rather than places, and its reach is not dependent upon whether or not there has been a physi-

[152] *See* for example 5 U.S.C.S. § 552(b) and *inter alia*, § III.B.2.

[153] "Personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."

[154] Julian v. United States Dept. of Justice, 806 F.2d 1411 (9th Cir. 1986), *aff*.'d 486 U.S. 1 (1988).

[155] United Technologies Corp. v. F.A.A., 102 F.3d 688, at 692 (2d Cir. 1996).

[156] *Id*.; *Also see* United States Dept. of Defense v. Federal Labor Rel. Auth., 510 U.S. 487 (1994).

[157] For example, under 18 U.S.C.S. § 2721, the release of motor vehicle records is prohibited, except as otherwise permitted under the numerous exceptions contained in the statute, such as to law enforcement officials or to any governmental authority in a civil or criminal proceeding.

cal intrusion into a given enclosure,[158] intrusions into oral, wire, and electronic communication also invoke Fourth Amendment protections.[159] All such communications are protected from interference or interception by others, unless made specifically exempt by statute, thereby making them subject to interception consistent with the terms of the exemption.[160]

2. The Electronic Communication Privacy Act[161]

The United States Congress has long recognized the benefits of wiretapping for national security purposes and the prevention of illegal activities, but it has also recognized the potential for abuse. In adopting Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Congress expressed its concern regarding privacy:

> To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused.[162]

In 1986, Congress adopted the Electronic Communications Privacy Act of 1986 (ECPA), which amended the existing wiretap law to broaden the coverage of the Act to include most types of wire and electronic communications, in addition to oral and wire communication, including the telephone, and to prohibit unauthorized eavesdropping by all persons (not only government).[163] The last major amendment appears to cover all manner of electronic communication, which would include email, voice mail, fax transmissions, and the Internet. As an example, electronic communication is defined as "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce...."[164]

As a general rule, the legislative history of the Act and its various amendments, even prior to 1986, indicates that it was intended to protect the privacy of individuals engaged in lawful activity who had a reasonable expectation of privacy. As the cases indicate, not all persons using a telephone to conduct business have a reasonable expectation of privacy. Thus a person making a telephone call within 4 feet of another who is close enough for the conversation to be overheard does not have a real expectation of privacy.[165] Nor would an employee misusing a private telephone system be entitled to assume any reasonable expectation that the communication was not subject to interception.[166]

A person's "reasonable expectation of privacy" must be decided on a case by case basis, taking each case's unique facts and circumstances into account.[167] As noted in the *Benford* case, "[g]enerally, the test applied is two-part: (1) Did the person involved have a subjective expectation of privacy; and (2) Was that expectation objectively reasonable?"[168]

Of equal importance are two exceptions contained within the Act that have traditionally been utilized in telephone interception cases. The first is the "prior consent exception" in which prior consent of one of the parties to the communication is either given directly or is implied. The second is the "business use exception," which exempts communication to or from a business facility from the interception prohibitions in the ECPA. It would appear that these provisions cover the entire spectrum of oral, wire, and electronic communication, such that they apply to telephonic communication, facsimile transmissions, email, voice mail, Internet usage, and the like.

The public employment issue with regard to the "prior consent exception" is whether by providing notice to its employees that the communication of whatever nature may be monitored, does the public employers' interception of such communication fall within this recognized exception to the ECPA? While examination of the prior consent rule may be somewhat of an academic exercise in light of the "business use exception," the ultimate determination, certainly for these two exceptions and perhaps in all cases, will depend upon the employees' reasonable expectation of privacy based upon the surrounding facts and circumstances. As a general rule, however, it is probably safe to assume that most types of communication undertaken at the work site are subject to the exclusionary provisions of

---

[158] Katz v. United States, 389 U.S. 347 (1967); Roberts v. Houston Indep. School Dist., 788 S.W.2d 107 (Tex. App., Hous., 1st Dist. 1990).

[159] It is a well-established federal rule that where one of the parties to a communication has provided his or her consent to be monitored, it is a recognized exclusion to the Electronic Communications Privacy Act and not prohibited by the Fourth Amendment. United States v. Hodge, 539 F.2d 898 (7th Circuit 1976) *cert. den*., 429 U.S. 1091 (1977); United States v. Puchi, 441 F.2d 697 (9th Cir. 1971) *cert. den*., 401 U.S. 853 (1971).

[160] The Electronic Communications Privacy Act of 1986, P.L. 99-508 (Oct. 21, 1986) 100 Stat. 1848; codified at 18 U.S.C. § 2510 *et. seq*. and 18 U.S.C. § 2701 *et. seq*.

[161] *Id*.

[162] P.L. 90-351, Title III, Sec. 801(d) (June 19, 1968) 82 Stat. 211.

[163] *See* note 161, *supra.*

[164] 18 U.S.C. § 2510(12).

[165] United States v. McLeod, 493 F.2d 1186 (7th Cir. 1974).

[166] United States v Christman, 375 F. Supp. 1354 (ND Cal. 1974).

[167] O'Connor v. Ortega, 480 U.S. 709 (1987); Benford v. American Broadcasting Cos., Inc., 554 F. Supp. 145 (Md. 1982) *cert. den.*, 464 U.S. 830 (1983).

[168] 554 F. Supp. at 154, citing United States v. McIntyre, 582 F.2d at 1223.

the ECPA, thereby permitting the employer to monitor most types of communications.

(A) THE PRIOR CONSENT EXCEPTION

The "prior consent exception" reads:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.[169]

In a case that predated adoption of the Electronic Communications Privacy Act, the court determined that an employee's knowledge of the employer's capabilities to monitor private telephone conversations did not constitute implied prior consent to be monitored.[170] The decision in this case walked a fine line and tried to dichotomize what might be subject to interception and what was private information not subject to interception by the employer and held that consent, per se, was not an all or nothing proposition and that it could be limited in scope. Relying more on the "business use exception," the court concluded that a personal call could be intercepted in the ordinary course of business as an allowable interception under the Act. However, in this case the court concluded that it was an issue for the trier of fact to determine when such consent terminated by virtue of the nature of the conversation and that once the conversation turned to a matter of personal nature, an employer may no longer listen.

Another case within the context under which the ECPA was adopted involved a routine, nonsurreptitious recording of a police telephone line, which was normally recorded and was used by a police officer for a private purpose.[171] The police officer had knowledge of the line's purpose and therefore the court held that it constituted an exception under existing law on the basis that it amounted to prior consent. Although the case was dismissed based upon its facts, the court did note that Congress did not intend the Act to apply to the recording of emergency and investigative calls, which were part of the routine police function. When considering whether there has been prior consent, there must be a close examination of facts, but normally the exceptions will be narrowly construed.

(B) THE BUSINESS USE EXCEPTION

A much broader exception under the statute is the "business use exception."[172] The "business use exception," sometimes formerly referred to as the "business" or "telephone extension exception" to the ECPA is contained in the definition section of the Act, which defines an electronic, mechanical, or other device as any device or apparatus that can be used to intercept a wire, oral, or electronic communication other than:

> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (I) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business, or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business.....[173]

The rationale for the "business use exception" was discussed in a 1980 case when the exception was referred to as the "telephone extension exception."[174] Plaintiff Briggs was a former employee of American Air Filter who was now employed by a competitor of the company. Roby, a salesman for American, kept in contact with Briggs and spoke to him often. A manager for American Air Filter who knew of the relationship had cautioned Roby and another employee not to discuss business with Briggs. The manager had been subsequently advised at some point that Briggs and Roby were working together. The court held that the manager's taping of a conversation between the two was within the ordinary course of business for the manager because the manager had reasonable suspicions that business was being discussed, and in fact the call did concern corporate business.[175]

While the "business use exception" is rather broad in its scope, it is not without limitation.[176] The fact that monitoring and recording of telephone calls can be justified for a legitimate business purpose is not sufficient alone to be used as an exception under the Act, unless the interception occurs during the normal course of business.[177]

Indiscriminate recording of all calls, whether business or personal, does not constitute conduct during the ordinary or normal course of business.[178] Personal calls may never be intercepted, except to the extent that it is necessary to determine whether there has been an authorized use of the telephone or to determine whether the call is personal or not.[179] Although a per-

---

[169] 18 U.S.C. § 2511(2)(d).

[170] Watkins v. L.M. Berry and Co., 704 F.2d 577 (11th Cir. 1983).

[171] Jandik v. Village of Brookfield, 520 F. Supp. 815 (ND Ill. 1981).

[172] This exception, discussed in Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412 (11th Cir. 1986), was read more broadly than the court did in the Jandik case.

[173] 18 U.S.C. § 2510(5).

[174] Briggs v. American Air Filter Co., Inc., 630 F.2d 414 (5th Cir. 1980).

[175] *Also see* James v. Newspaper Agency Corp., 591 F.2d 579 (10th Cir. 1979); Burnett v. State of Tex., 789 S.W.2d 376 (Tex. App. 1990).

[176] Ali v. Douglas Cable Communications, Inc., 929 F. Supp. 1362 (D. Kan. 1996).

[177] *Id*.

[178] Sanders v. Robert Borsch Corp., 38 F.3d 736 (4th Cir. 1994).

[179] Ali v. Douglas Cable Communications, Inc., *supra* note 176; Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983).

sonal call may be intercepted to determine its nature, interception can never be used to determine its content.[180]

3.Email/The Internet

While the ECPA language appears to cover all types of electronic communication, including email specifically, a limited number of authorities have addressed email transmissions and interceptions in case law and in law review and journal articles. A 1992 issue of *The Labor Lawyer* includes an article that provides an analysis of the Electronic Communications Privacy Act of 1986 and how it was extended to cover email communications, where it is noted that[181]"[t]he Senate Report on the ECPA underscores individual privacy concerns as the primary reason for including E-mail and similar forms of electronic surveillance within the purview of the statute."[182]

This article explores the language of the Act, attempts to ascertain the will of Congress in adopting the law, and attempts to anticipate how the courts will decide certain issues. The author notes that while the Act also contains a property protection exemption, which allows employers to monitor employees calls in certain instances, that section appears to generally apply to communications companies. According to the author's analysis, the "business use exception" is more applicable in the case of email interception.[183]

While employers appear to have broad discretion based upon the statutory exceptions, employer intrusions are not without limits. One set of authors set forth the parameters of such employee rights:[184]

> Although an employer's right to engage in service observation, computerized work measurement, and other electronic surveillance of employees is largely unrestricted, it is not entirely without limits. Employees have a protected zone of privacy—albeit relatively narrow—even inside the workplace. Monitoring employees' personal calls, eavesdropping on their private conversations, videotaping employees in highly private areas, or otherwise exceeding reasonable substantive and temporal limitations on the scope of the monitoring may well subject employers to liability under existing constitutional, common law, or statutory prohibitions. Furthermore, the protection afforded to employees' privacy rights' necessarily increases as the employer's monitoring extends beyond purely work-related matters or moves outside the workplace.[185]

The authors further emphasize that this is a relatively new area of law, which is still under development. Just as in the old axiom, "bad facts make bad law," egregious situations and unreasonable conduct on the part of employers wanting "to push the envelope" will most likely lead courts to carve out exceptions favoring individual privacy protections and create further balancing tests as this body of law develops.

(A) RATIONALE FOR BUSINESS USE EXCEPTION

A Pennsylvania court explained the rationale for the "business use exception" arising from the use of corporate email.[186] A wrongful discharge tort complaint of an at-will employee was dismissed for failure to state a claim after the court discussed the public policy implications of email interceptions. Plaintiff had alleged an invasion of his right to privacy, claiming it constituted a breach of public policy.

As alleged in the complaint, the defendant company maintained an email system to encourage internal corporate communications between their employees. The company repeatedly assured users of the system that email communication would remain confidential and privileged and that such communication could not be used to reprimand or terminate its employees.

The plaintiff, an at-will employee, received an email message at his home from his supervisor to which he responded. In the course of his response, he allegedly made derogatory remarks about the company and some of its employees. The company subsequently intercepted the plaintiff"s email and terminated his employment for transmitting what the company deemed to be inappropriate and unprofessional comments. Ruling initially that Pennsylvania law provided no cause of action for wrongful discharge of an at-will employee, the court took up the issue as to whether the conduct of the defendant company violated public policy. At the time of this decision, Pennsylvania courts had established a rule that in order to constitute a public policy exception, the company's actions must violate a "clear mandate" of public policy, which it defined as "of a type that 'strikes at the heart of a citizen's social responsibilities.'"[187]

In reaching its decision the district court said, "we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company's e-mail system, notwithstanding any assurances that such communications would not be intercepted by management."[188]

The court went on to say that even if the employee was found to have a reasonable expectation of privacy, it did not find that a reasonable person would consider the company's interception of email on its system to be

---

[180] Ali v. Douglas Cable Communications, Inc., *supra*.

[181] Julia Baumhart, *The Employer's Right to Read Employee E-Mail: Protecting Property or Personal Prying*, 8 LAB. LAWYER at 923 (1992).

[182] *Id*. at 925.

[183] 18 U.S.C. § 2510(5). The rationale is based upon the line of cases relating to telephonic interceptions; Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983); Epps v. St. Mary's Hosp. of Athens, Inc. 802 F.2d 412 (11th Cir. 1986).

[184] Kenneth Jenero and Lynne D. Maples-Riordan, *Electronic Monitoring of Employees and the Elusive "Right to Privacy*," 18 EMPLOYEE RELATIONS L.J. at 71 (1992-93).

[185] *Id*. at 97.

[186] Smyth v. Pillsbury, 914 F. Supp. 97 (E.D. Pa. 1996).

[187] 914 F. Supp. at 99, cite omit.

[188] 914 F. Supp. at 101.

a "substantial and highly offensive invasion of his privacy."[189] Finally, the court concluded by saying that "the company's interest in preventing inappropriate and unprofessional comments, or even illegal activity over its e-mail system outweighs any privacy interests the employee may have in those comments."[190]

(B) OTHER CASES

In the well-publicized case involving an email interception of a 17-year U.S. Navy veteran, the Navy was enjoined from dismissing the serviceman on the basis that the latter's suit had a reasonable probability of success and met all of the other requisite grounds for issuance of an injunction.[191] The suit alleged that the Navy had violated its "Don't ask, Don't tell, Don't pursue" policy by obtaining the plaintiff"s identity and sexual orientation from America Online (AOL), his Internet on-line service provider.

In this case, initially a civilian Navy volunteer inadvertently came across the information that a serviceman aboard the USS Chicago corresponded over the Internet via homosexual Web sites. She then pursued it further to ascertain the identity of the individual from AOL, that it was McVeigh, and then passed that information on to the command of the USS Chicago. After conducting an administrative discharge hearing, it was determined that McVeigh would be dismissed from the service based upon this information. This action was enjoined by the court.

The district court in Nevada held that police officers had no reasonable expectation of privacy in a computerized paging system that automatically stored messages transmitted through the system.[192] The case involved a paging system used by the City of Reno Police Department for purposes of communication, primarily to the media, but also between officers. A standing order for the pagers and their use included a warning that all messages were stored by the department. As a result of certain communications between the plaintiff police officers, an internal affairs investigation was instituted.

The plaintiffs filed suit alleging a violation of their right to privacy under the Fourth Amendment and the ECPA. The court in *Bohach* held that because of the nature of the paging system, the use to which it was put, and the "standing order," plaintiffs could only have had a diminished expectation of privacy in their communications and therefore there was no Fourth Amendment violation. On the allegation that the city used illegal "wiretaps" to collect the information, the court held that the city did not "intercept" the transmission in violation of 18 U.S.C. Section 2510 et. seq., but rather that it correctly retrieved such messages from storage pursuant to 18 U.S.C. Section 2701 et seq.

A New York court held that the ECPA only prohibits intentional interception of electronic communication without a court order (unless exigent circumstances exist), not access to stored messages, which only requires a warrant.[193] In this case, federal agents seized three pagers from the defendants, two of which were incident to their lawful arrest. However, information obtained from the third pager was stored information and its retrieval resulted from an illegal search, since exigent circumstances did not exist. The court determined that retrieval of information from two of the pagers was warranted under the circumstances, but with regard to the third pager, the information retrieved required a warrant since such exigent circumstances did not exist.

The defendant argued for exclusion of the evidence based upon the Fourth Amendment and the ECPA. The case was decided on the basis of what constitutes "interception" and what constitutes "stored" information within the meaning of the Act, since different standards apply.

The court in *Reyes* cited a Fifth Circuit decision that held that a seizure of a computer used to operate an electronic bulletin board system and containing private electronic mail that had been sent to the bulletin board, but not read by intended recipients, was not unlawfully intercepted under the Federal Wiretap Act, which would require issuance of a court order.[194]

Although 18 U.S.C. Section 2511(1)(a) prohibits interception of "any wire, oral, or electronic communication" under the holding in *Steve Jackson Games, Inc*., supra, that section was not applicable in this case, since the actions did not constitute an "interception." The section of the Act referencing stored electronic communications would apply, and in this case a search warrant was justified to access the information.[195]

Unless and until Congress adopts a statute that more specifically is addressed to the question of the privacy of email in the workplace, it will most likely be determined on a case by case basis. Using the analogy contained in the *Ortega* line of cases, does an employee using the company email have a reasonable expectation of privacy or does the fact that the system belongs to the government make all communications subject to review? If the government employer posts a notice that all email received or sent on government-owned computers during or after normal work hours is subject to review and inspection by the employer, the employees' right to privacy is correspondingly diminished since whatever expectation of privacy they may have had would be diminished as a result of the notice.[196]

---

[189] This rationale appears to be contra to that espoused in the telephone cases: Ali v. Douglas Cable Communications; Sanders v. Robert Borsch Corp, *supra.*

[190] *Supra*, at 101.

[191] McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998).

[192] Bonach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996).

[193] United States v. Reyes, 922 F. Supp. 818 (SD NY 1996).

[194] Steve Jackson Games v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994).

[195] 18 U.S.C. § 2701 *et seq*. (*See* 922 F. Supp. 818, 837).

[196] American Postal Workers Union v. United States Postal Serv., 871 F.2d 556 (6th Cir. 1989).

Does this mean that the government employer has the right to randomly access employee email? Or would it be necessary to apply the rule unless there is a case of individualized suspicion of an employee? Or in the alternative, following the logic of *Ortega*, must a search of employee email be justified at its inception and must the scope of the search be reasonably related to the circumstances that originally justified the interference with the employee's reasonable expectation of privacy?

The third possibility is that the email would fall into one of the categorical exceptions under the ECPA. In the absence of written notification, in all likelihood this would be the "business use exception." In *Ortega*, the Court required a balancing of public employees' privacy expectations against reasonableness of the search or the government's requirement for supervision control and efficiency as an employer.

4. Voice Mail

In one of the few cases involving voice mail, the plaintiff was discharged from his position as collection manager at Norwest Bank, Billings, for alleged insubordination.[197] When he sued, the bank counterclaimed on the grounds that he taped telephone conversations of bank customers and employees. The plaintiff was alleged to have used a handheld recorder to tape phone messages left on his voice mail and also to have recorded conversations between customers and the bank president.

With regard to the voice mail messages, the court determined that, for an illegal wiretap to have taken place under the wiretap statute, it was necessary that an interception of the conversation occur and that such interception occur during the initial use of the recording device contemporaneous with the transmittal or preservation of the communication.[198] Since use of the handheld recorder to record voice mail messages did not occur at the same time as the leaving of the messages, and the persons leaving the messages consented to the recording of the messages by the fact that they left them, the court concluded that no interception within the meaning of 18 U.S.C. Section 2510 et. seq. occurred. The court went on to hold that the recording of telephone conversations between the bank customer and the president of another bank without consent or knowledge of the parties to the conversation did not violate the statute, absent evidence that the employee was motivated by a criminal or tortious purpose when he recorded the conversations.

5. Intercepted Information

It would appear that any information acquired from a lawful interception of an electronic communication or even information acquired by accident or non-intentionally may be properly disclosed. The ECPA[199] provides specifically that any person who has received information pursuant to the Act may disclose it in "any proceeding held under the authority of the United States or any State or any political subdivision thereof."[200]

In the case of unauthorized interception of such communication, its disclosure is only prevented when such interception was intentional.[201]

While it is clear that properly intercepted information *may* be disclosed in a proper manner, it begs the question of whether the acquisition of such information may give rise to a duty to disclose, particularly if failure to disclose might aid in the commission of a crime or cause injury to others. One example might be the interception of an email or telephone conversation that discloses a terrorist act.

While transmittal of such information to a law enforcement agency is allowed by statute,[202] mere knowledge of a crime to be committed would not be sufficient to create a duty subject to criminal liability for failure to report the incident.[203] However, depending upon the degree of knowledge, systematic tracking, and review of such communication and all other factual circumstances, failure to report criminal activity obtained through the interception of electronic communication may give rise to an actionable duty to prevent the threatened harm.[204]

D. Supervisor's Responsibilities

1. Introduction

As noted above, a distinct body of law has developed in the area of privacy in the public workplace. Additionally, public employees also have responsibilities to their superiors, fellow employees, and members of the public involving related privacy issues. As with many of the other sections, a large body of law has developed on several of these issues as well. This paper only touches upon a couple of cases to provide the general direction of the law in this area.

The Civil Rights Act of 1871[205] provides a broad range of redress for one who has had their constitutional rights endangered by actions or threatened actions of the government or government officials. In order to have an actionable civil rights claim, two elements are essential: "that the challenged conduct was attributable at least in part to a person acting under color of state

---

[197] Payne v. Norwest Corp., 911 F. Supp. 1299 (D. Mont. 1995).

[198] *Id*. at 1303, citing to United States v. Turk 526 F.2d 654 (5th Cir. 1976), *cert. den*. 429 U.S. 823 (1976).

[199] P.L. 99-508, (October 21, 1986) 100 Stat. 1848.

[200] 18 U.S.C.S. § 2517(3).

[201] Bayges v. Southeastern Pa. Transp. Auth., 144 F.R.D. 269 (E.D. Pa. 1992).

[202] 18 U.S.C.S. § 2702(b)(6).

[203] For standards applied, see United States v. Greer, 467 F.2d 1064 (7th Cir. 1972), *cert. den*., 410 U.S. 929 (1973); Pinkerton v. United States, 328 U.S. 640 (1945).

[204] *See,* for example, *Negligence,* 57A AM. JUR. 2D, at 6-16.

[205] 42 U.S.C. § 1983.

law, and...that such conduct deprived the plaintiff of a right, privilege or immunity secured by the Constitution or laws of the United States.…"[206]

2. 1983 Actions

As an officer, employer, or employee of a public transportation agency, one has a dual role to play with respect to a potential violation of 42 U.S.C.S. Section 1983.[207] Any such officer, employer, or employee must be mindful of his or her personal rights and responsibilities as they may be affected either by some action of the public transportation agency or the actions of another officer, employer, or employee acting on behalf of the public transportation agency, or conversely, acting outside the scope of their responsibilities. Public employees, as supervisors, also have rights and responsibilities toward subordinate employees. These issues are all the more pointed in the area of personal privacy and how they impact each employee's "zone of privacy."

The Civil Rights Act of 1871, 42 U.S.C. Section 1983, prohibits interference with the constitutional or statutory rights of another under penalty of law and potential liability.[208] The language is sweeping in scope, and the annotations to this relatively brief statute literally cover volumes. As an officer, employer, or employee in the public transportation industry, one must be mindful of which activities are permitted and which are not.

It is important to note at the outset that 42 U.S.C.S. Section 1983 carries with it an implied qualified immunity for official actions undertaken in good faith.[209] To be shielded by qualified immunity, the government official must operate within the bounds of his or her official responsibility. Conversely, if a federal official commits an unconstitutional act, he or she is necessarily operating outside of his or her official capacity and the doctrine of sovereign (and presumably qualified or governmental) immunity would not apply.[210]

In *Strathie v. Dept. of Transportation, Commonwealth of Pennsylvania*,[211] a class action suit, the court explained that:

> Executive officials must be guided by the public interest in making decisions and authorizing actions of their subordinates. Implicit in the concept of a qualified immunity for certain official acts, is a recognition that officials may err. The rationale for the immunity protection is that unless an official is protected from personal liability he may refrain from decision-making, or be guided by factors other than the best interest of the public.[212]

Qualified immunity has been broadly applied to protect public officials for good faith actions undertaken in their official capacity. In a case involving the release by a prison official of medical records of a rape victim to a prison inmate (the victim's father), the Sixth Circuit held that the release of such records "does not rise to the level of breach of a right recognized as fundamental under the Constitution."[213] The court expounded upon the doctrine and said that "[g]overnmental officials who perform discretionary functions, such as the defendants in this case, generally are shielded from civil liability insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known."[214]

In another case involving a search incident to an internal affairs police investigation, the Seventh Circuit, in commenting on the rights that may be violated before an official would lose qualified immunity, stated that "[f]or a right to be 'clearly established', the right's contours must be sufficiently clear so that the officials could have reasonably believed that their actions were lawful."[215]

The court went on to say that conversely, for an official act to breach qualified immunity, its unlawfulness must be apparent based upon existing law.

Under the facts in *Jarvis v. Wellman*, supra, a medical record was found to not be constitutionally protected; however, the Third Circuit, in *Doe v. Southeastern Pennsylvania Transportation Authority*,[216] held that the privacy of individual medical records is a constitutionally protected right.[217] In this case, SEPTA instituted a program to monitor its medical costs by requiring the pharmacy that filled prescriptions for SEPTA employees to report when prescriptions totaling in excess of $100 per month were being filled by its employees. Through the information received from the pharmacy, SEPTA was able to learn that one of its employees was HIV positive. This information was shared with other managers within SEPTA. In reaching its determination, the court said, "When the underlying claim is one of invasion of privacy, the complaint must be 'limited to those (rights of privacy) which are 'fundamental' or 'implicit' in the concept of ordered liberty'.…"[218]

---

[206] New York Magazine v. Metropolitan Transp. Auth., 136 F.3d 123, 128 (2d Cir. 1998) (citation omitted).

[207] *See Selected Studies in Highway Law*, *IV*: *Impact of 42 U.S.C. § 1983 on Highway Departments, Personnel, and Officials*, 2018-N119.

[208] *See*, for example, New York Magazine v. Metropolitan Transp. Authority, 136 F.3d 123 (1998).

[209] Wood v. Strickland, 420 U.S. 308 (1975); Scheuer v. Rhodes, 416 U.S. 232 (1974).

[210] Schowengerdt v. General Dynamics Corp., 823 F.2d 1328 (9th Cir. 1987).

[211] Strathie v. Dept. of Transp., Commonwealth of Pa., 547 F. Supp. 1367 (E.D. Pa. 1982), vacated on other grounds, 716 F.2d 227 (3d Cir. 1983).

[212] *Id*. at 1375.

[213] Jarvis v. Wellman, 52 F.3d 125, 126 (6th Cir. 1995).

[214] *Id.*

[215] Shields v. Burge, 874 F.2d 1201 (7th Cir. 1989).

[216] *Id*. at 1205.

[217] 72 F.3d 1133 (3d Cir.); *cert. den*.____US____, 117 S. Ct. 51 (1996).

[218] *Id*., at 1137.

Citing *Whalen v. Roe*,[219] the court noted that the right to privacy involves at least two separate interests: (1) the personal interest in avoiding disclosure of personal information, and (2) interest in independence in making certain types of important decisions. In reaching its decision the court determined that indeed medical records fall within the first category.

In the SEPTA case, however, the court balanced the individuals' privacy interest against the interest of the employer in obtaining the information. The court found that the constitutional right of the individual was superseded by SEPTA's need to have access to the prescription records in order to monitor costs of the program.

A Philadelphia police officer was fired for refusing to respond to questions about his sexual activities that bore no relationship to his job, and he filed a 1983 action alleging violation of his rights under the First, Fourth, and Fourteenth Amendments to the Constitution.[220] The district court held that a person's private sexual activities (unrelated to job performance) are within the "zone of privacy" protected from unwarranted government intrusion.[221] In reaching its decision in *Shuman*, the court referred to the subject of the inquiry as being one of those private matters of which Justice Brandeis characterized as the right to be left alone.[222]

Disabled school children's claims for invasion of their constitutional right of privacy against a bus driver for physical and mental abuse were permitted in *Jane Doe A. v. Special School District of St. Louis City*.[223] The district and district officials were dismissed as defendants since evidence did not support a consistent pattern of constitutional violations, nor did it depict indifference to such violations. Failure to prove these facts provided the district and district officials with qualified or discretionary immunity.

Courts have uniformly held that any activities conducted in public view are not protected by the Constitution. A bus passenger who sued SEPTA for alleged injuries from a bus accident brought a subsequent civil rights action pursuant to 42 U.S.C.S. Section 1983 against the authority, in which she claimed a violation of her civil rights for personal surveillance undertaken by the authority to determine the extent of her injuries.[224] The district court dismissed the case on the basis that the surveillance did not deny plaintiff access to the courts, nor did it invade her right to privacy since all of the surveillance occurred in public locations.

In a somewhat unusual seven page dissent, Justice Marshall strenuously disagreed with the court's failure to grant certiorari in a suit brought by an unmarried couple pursuant to 42 U.S.C. S. Section 1983 on the basis that they were fired from their positions at the state-maintained Carnegie Free Library because of their relationship.[225] Despite the holding that the Carnegie Free Library was not acting under the code of any state law or regulation, but only within its discretion, its actions were allowed to stand because the plaintiffs failed to "normalize" their relationship. Acts arising even partially under the color of state law can give rise to a 1983 claim.[226]

In perhaps the seminal case dealing with electronic intrusions into personal privacy,[227] Justice Harlan, in his concurring opinion, raised the issue regarding the consequences of innovative technologies and their impact upon privacy rights. Presaging the pending dilemma, Justice Harlan stated that "[i]ts limitation on Fourth Amendment protection is, in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[228]

3. Public Transportation Managers

With regard to privacy issues, transportation managers need to be aware of the rights and responsibilities of employees and members of the general public summarized in this paper. There are general principles of privacy law that have been held to be the appropriate standard in most cases that are dependent on the given factual situation.

To reiterate briefly, public employees do enjoy a reasonable expectation of privacy in their workplace and do retain their Fourth Amendment privacy rights; however, these are subject to the "operational realities" of the work setting.[229] Within the context of the *Ortega* decision, as a general rule only areas reserved for the exclusive use of an individual employee enjoy some degree of privacy. These areas may be invaded if there are reasonable grounds to believe that improper conduct has occurred and the scope of the actions taken is reasonably related to the basis for the action in the first instance.[230]

The use and release of records are generally controlled by statute, such as the FOIA.[231] As a general rule, all such records are subject to public inspection,

---

[219] 429 U.S. 589 (1977).

[220] Shuman v. City of Philadelphia, 470 F. Supp 449 (E.D. Pa. 1979).

[221] 470 F. Supp. at 459, citing Roe v. Wade, 410 U.S. 113 (1973; Griswold v. Connecticut, 381 U.S. 479 (1965), and other cases).

[222] *Id.* quoting dissenting opinion in Olmstead v. United States, 227 U.S. 438 (1928).

[223] 682 Fed. Supp. 451 (E.D. Mo., 1988), a*ff'd* 901 F.2d 642 (8th Cir. 1990).

[224] Frazier v. Southeastern Pa. Transp. Auth., 907 F. Supp. 116 (E.D. Pa. 1995).

[225] Hollenbaugh v. Carnegie Free Library, 439 U.S. 1052 (1978).

[226] New York Magazine v. Metropolitan Transp. Authority, 136 F.3d 123 (1998).

[227] Katz v. United States, 389 U.S. 347 (1967).

[228] *Id*. at 362.

[229] O'Connor v. Ortega, 480 U.S. 709 (1987).

[230] *Id*. at 724-26.

[231] 5 U.S.C.S. § 552.

except as otherwise listed in the statute. Some types of tests and medical information are regulated by statute and in some cases held to be constitutionally protected.[232] Blood and alcohol testing of public employees is generally permissible, particularly where such employees hold sensitive positions involving security or public safety.[233]

Surveillance of public employees at work is generally a permissible activity, unless it involves a situation in which the employee enjoys a justifiable and reasonable expectation of privacy.[234] Based upon the Supreme Court's decision in *O'Connor v. Ortega*, public employees enjoy a very limited expectation of privacy within the workplace.[235] The ECPA protects privacy in most types of electronic communication; however, only the most personal of communication in the workplace is protected.[236] Based upon the "prior consent" and "business use" exceptions, most types of electronic communication, including the telephone, email, voice mail, and the Internet are subject to scrutiny by management.[237]

Activities of public transportation operators as they relate to privacy interests of the general public must adhere to similar broad legal principles. In a long line of cases, the courts have determined that activities conducted outside a permanent residence and in the open are in plain view and subject to public scrutiny.[238] This rule has been extended in application to persons traveling on public transit to the extent such persons have no protected privacy interest. By exposing oneself to the public within a transit facility or on a transit vehicle, one loses any reasonable expectation of privacy.[239] Reasonable use of cameras in transit facilities and vehicles does not violate privacy interests of the patrons. Likewise, it would appear that information generated as part of transit operations, such as origin-destination data, use pattern data, information contained on various applications for motor vehicle registrations, information on paratransit and transit use, etc., enjoy no special protection, unless it contains medical or other protected information. For further information as to what public employees and public transportation managers should know about their privacy rights and obligations, see Appendix B.

[232] Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260 (9th Cir. 1998).

[233] Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989).

[234] O'Connor v. Ortega, 480 U.S. 709 (1987).

[235] *Supra.*

[236] 18 U.S.C. § 2510 *et. seq*. and 18 U.S.C. § 2701 *et. seq*.

[237] Ali v. Douglas Cable Communications, Inc., 929 F. Supp. 1362 (D. Kan. 1996).

[238] New York v. Class, 475 U.S. 106 (1986).

[239] U.S. v. McDonald, 100 F.3d 1320 (7th Cir. 1996); Hoffman v. City of New York, 1998 W.L. 212894 (E.D. N.Y.); Katz v. United States, 389 U.S. 347 (1967).

IV. CONCLUSION

The American concept of privacy as defined by the Constitution and interpreted by Congress and the courts is being overwhelmed by technological advances that have altered the factual framework that constituted the background for those earlier decisions. In the past the standard test has involved a balancing of individual privacy rights versus the needs of society in general, generally characterized as a "compelling state need." This test may no longer be sufficient, since technology provides the capability to intrude upon individual privacy rights but may still meet at least several aspects of the traditional test of what constitutes a reasonable intrusion into personal rights of privacy (see Appendix A).

A. Reasonable Expectation of Privacy

Employees in the public sector are entitled to a "reasonable expectation of privacy" in their workplace. For instance, any search of the premises on which the employee is located must be made upon grounds that are reasonable at the outset, reasonably conducted, and related to the circumstances that led to the search in the first instance. Any expectation of privacy in the public workplace is also conditioned upon the nature and circumstances of such employment. A "diminished expectation of privacy" may arise, for example, in a case where notice of a possible search has been provided or where, because of the nature of the work being performed, it would be reasonable to anticipate such an intrusion.

With regard to public records as they relate to the public employee and such records over which the public employee may have custody or control, access to and release thereof are generally controlled by state and Federal FOIAs. All such records are generally accessible unless otherwise protected by a privilege. Most FOIAs contain a proviso that prohibits disclosure of "personnel and medical and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." Case law is replete with pertinent examples of what is and is not subject to disclosure.

Access to medical records and testing results has traditionally been denied on the basis of a protected personal privacy interest. Numerous exceptions have evolved, particularly as they are applied to employees in public service. Mandatory drug and alcohol testing of public employees in safety sensitive positions or security sensitive positions has been permitted generally on the basis that such employees have a "diminished expectation of privacy" by the nature of their job. Although courts have been loathe to accept polygraph and psychological testing results into evidence because of their inherent unreliability, federal law allows the use of the polygraph as a precondition or condition of continued government employment.

B. Electronic Communication

The interception and dissemination of information from any electronic communication by a third party or organization is illegal. However, with minor exception for the most personal situations, virtually all electronic communication within the workplace is subject to some form of monitoring by the employer as one or more exclusions under the ECPA adopted by Congress. This is true whether such communication is by telephone, facsimile, email, voice mail, or electronic means.

The two most notable exceptions under the Act are the "prior consent exception" and the "business use exception," which together would encompass essentially all communication to and from the work site. By virtue of being in the work setting, employees have a "diminished expectation of privacy" and no reason to expect any great degree of privacy. From a management perspective, providing notice of the agency's monitoring policy is not only a good management practice, but also provides an extra level of protection to the employer.

C. Public Transportation

The Fourth Amendment protects against governmental intrusions into activities for which persons have a justifiable (as determined by societal norms) and "reasonable expectation of privacy" (as determined subjectively). Activities conducted in the open have been determined not to give rise to a constitutionally protected interest under the Fourth Amendment. Case law suggests that virtually any activity conducted in a public location, including those conducted in public transportation facilities or on transit vehicles, is subject to public scrutiny. This includes any reasonable surveillance of such activities, whether conducted in person or by use of a television or video camera.

Persons traveling on public transportation have been held to have a diminished or reduced expectation of privacy. The use of cameras for traffic law enforcement, for security in public transportation facilities, or on public conveyances has been permitted on the same basis. It has been generally held that discrete and reasonable surveillance of any activity open to the public enjoys no constitutional privacy protection.

While there has yet to be a dispositive case on the issue, it is reasonable to presume that information gathered from public transportation activities, such as origin-destination studies, passenger surveys, the use of smart cards or farecards, or other planning or operational techniques enjoys no particular protection. In all likelihood it will depend more upon the nature of the request, or the reasonableness to which such information will be used, in determining its accessibility.

D. Rights and Obligations of Public Transportation Managers

Public transportation managers have to be aware of their rights and obligations both as employees and supervisors of other employees and with regard to the unique relationship that they have with members of the general public. The Civil Rights Act prohibits interference with the constitutional rights of others. As it relates to issues of privacy, the public transportation manager has to be mindful of the principles expressed in this paper.

While the public transportation manager does enjoy a qualified immunity for official actions that he or she undertakes in good faith, to undertake actions outside of those parameters may incur significant and severe repercussions. The manager does have the right to monitor the movement and work being performed at the work site by all reasonable means. These include monitoring of nonpersonal communication by telephone and email, etc., and surveillance through TV and video equipment. The critical watch word is whether the activity being monitored is entitled to a "reasonable expectation of privacy" or whether by the nature of the work being performed or notices provided to the employee, the activity carries with it a "diminished expectation of privacy."

The relationship that the public transportation manager has with members of the public always involves a matter of public trust. By the same token, unless otherwise excepted by statute, most records held by the public manager are subject to disclosure. The FOIA generally controls which documents are protected. The public has a right to know that public transportation is being operated in a safe and reasonable manner, and the courts have permitted drug and alcohol testing by management to insure that this is taking place.

Riding on public transportation provides no special privacy interests to the users. In fact, by exposing oneself to the public, one is therefore exposed to scrutiny by all. Public agencies have the right to reasonably monitor the activities of individuals in public transportation facilities, on the roads, and on transit vehicles.

APPENDIX A—POSSIBLE SOLUTIONS: FAIR INFORMATION STANDARDS

The United States Congress has developed a set of standards that it uses in drafting legislation related to privacy issues. These standards, known as the Fair Information Principles, were developed in the 1970s specifically to address the question of protecting privacy in a world where access to personal information becomes easier every day.[240] These principles, although they have not been codified to date, have been used by Congress as the framework for privacy-related legislation,[241] such as the Privacy Act of 1974,[242] the Fair Credit Reporting Act,[243] the Right to Financial Privacy Act,[244] the Electronic Communications Privacy Act,[245] and the Video Privacy Protection Act.[246]

These principles have been stated in various ways, but in essence they turn on providing a measure of fairness and protection to individual privacy in a rapidly "shrinking" world. One version of the principles has been stated thusly,[247]

> The first principle is that only *relevant* personal information should be collected. In other words, if our purpose is to improve traffic management, we should collect only the information necessary to achieve that goal and nothing else.
>
> Second, individuals should be informed what information is to be collected and how it will be used. We may not be able to guarantee that every IVHS application will be used.
>
> Third, individuals should be able, and with relative ease, to inspect their records for accuracy, completeness, and appropriateness. For example, if tolls are collected electronically, drivers should have access to the records of their toll road use, and should have the means to correct any errors.
>
> Fourth, personal information should be available within the collecting organization only to those with a legitimate need to know. This would apply to public and private operators alike.
>
> Fifth, disclosures of personal information to third parties outside of the original operator should not be made without the individual's agreement or appropriate legal process.
>
> And sixth, security measures must be in place to ensure that pledges of confidentiality are meaningful.

It is axiomatic that these principles must be an inherent and underlying feature of all ITS development. It has been observed that if people do not believe that their privacy is being protected, they will resist adoption of ITS technology, including all of the good features designed to improve the Nation's mobility.[248]

---

[240] *A Review of the Fair Information Principles: The Foundation of Privacy Public Policy,* Privacy Rights Clearinghouse (www.privacyrights.org/ar/fairinfo).

[241] *Id*.

[242] 5 U.S.C.S. § 552a.

[243] 15 U.S.C.S. § 1681 *et. seq*.

[244] 12 U.S.C.S. § 3401 *et seq*.

[245] 18 U.S.C.S. § 2710.

[246] 18 U.S.C.S. § 2710.

[247] 11 SANTA CLARA COMPUTER AND HIGH TECHNOLOGY LAW JOURNAL (1995). This publication is strongly recommended reading on the subject of the danger to privacy from ITS developments.

[248] *Id*.

APPENDIX B—RIGHTS AND OBLIGATIONS OF PUBLIC EMPLOYERS AND EMPLOYEES

Suggestions for Public Employers

Public employees, like their counterparts in private industry, generally wear many hats in the workplace. While in one sense they are always public employees, regardless of their position, they may also be in supervisory or managerial roles, which require them to act on behalf of the governmental entity as the public employer. Reviewing the case law and authority cited above and borrowing liberally from certain selected sources, the following is a list of suggested actions to be taken by the public employer to not only protect the interests of the governmental entity but also to make themselves and all employees within the public sector aware that certain rights and obligations are applicable in the public workplace and that their own privacy interests, while limited, are of extreme importance.

The following is a list of suggested actions for the employer to take, taken in large measure from Jenero and Maples-Riordan, *The Electronic Monitoring of Employees and the Elusive Right to Privacy*, 18 EMPLOYEE RELATIONS LAW JOURNAL 71, 98-100:

•Determine and understand the applicable federal and state laws.

•Develop written and posted policies, or include in an employee handbook policies related to privacy in the workplace, including, access and usage of telephones, fax machines, the Internet, office searches, drug and alcohol testing, personnel records, access to records, etc.

•Establish reasonable standards with the benefit of employee input into the use and content of email and Internet usage.

•Provide employees with prior written notice of the nature and extent of the applicable monitoring practices.

•Be prepared to justify employee monitoring from its inception.

•Observe reasonable temporal and geographical limitations on the scope of monitoring.

•Be sensitive to employee privacy rights.

•Reserve your rights but limit telephone monitoring and similar forms of electronic surveillance as necessary to preserve the "business use exception."

•Do not "bug" employee's offices or otherwise surreptitiously intercept their oral communications.

•Adopt reasonable procedural safeguards concerning the use of disclosure information gathered through monitoring.

•Conduct frequent, open, and informal sessions with employees to discuss, question, and provide input into the formulation and adoption of employment practices.

•Work with employees whenever possible to establish reasonable criteria and guidelines for standardized policies and practices. Train supervisors, managers, and security personnel regarding the applicable legal restrictions.

•Allow employees access to their personnel files, if this is not already a standard practice.

•Establish standards for the release of information from employees with input from employees (i.e., execution of a formal release from employee).

•Understand that in order to develop and implement ITS technologies, the public is going to have to understand not only the technology but also the ramifications to personal privacy that are involved. A public education plan will be required to explain such programs and to allay fears about their personal privacy being threatened. If such concerns cannot be adequately addressed, ITS programs will ultimately have minimal application.

Suggestions for Employees:

•Determine and understand applicable federal and state laws.

•Understand the concepts of "reasonable expectation of privacy," "diminished expectation of privacy," and "zone of privacy," as well as particular applications such as office search parameters, personnel records, drug and alcohol testing, etc.

•Work with employers whenever possible to establish reasonable criteria and guidelines for standardized policies and practices.

•Work with employers whenever possible to establish standardized personnel practices, access to records, etc.

•Work with employers to establish criteria for email use and content (inappropriate content can come back to haunt you).

•Work with employers to establish criteria for Internet usage.

•Seek advice of counsel whenever possible.

•Understand your rights and obligations as an employer and an employee.

•Become an active participant in a public education plan for development and implementation of ITS.

ACKNOWLEDGMENTS

This study was performed under the overall guidance of TCRP Project Committee J-5. The Committee is chaired by RICHARD J. BACIGALUPO, N.E. Illinois Regional Transit Authority. Members are ARTHUR P. BERG, Port Authority of New York and New Jersey; RICHARD W. BOWER, California Department of Transportation; SHELLY R. BROWN, Federal Transit Administration—Region 10; DORVAL RONALD CARTER, JR., Federal Transit Administration—Region 5; PAUL STEPHEN DEMPSEY, University of Denver; DENNIS C. GARDNER, Ogletree, Deakins, Nash, Smoak & Stewart, Houston, Texas; EDWARD J. GILL, JR., Eckert, Seamans, Cherin & Mellott; BRIGID HYNES-CHERIN, BHC Trans, Arlington, Virginia; CLARK JORDAN-HOLMES of Stewart, Joyner, Jordan-Holmes, Holmes, P.A.; and JEANETTE J. CLARK, Washington Metropolitan Transit Authority. NANCY ZACZEK provided liaison with the Federal Transit Administration during the preparation of this study, and GWEN CHISHOLM SMITH represents the TCRP staff.

TRANSPORTATION RESEARCH BOARD
National Research Council
2101 Constitution Avenue, N.W.
Washington, DC 20418

NON-PROFIT
U.S. POSTAGE
PAID
WASHINGTON, DC
PERMIT NO. 8970