3 Va. J.L. & Tech. 7 (Fall 1998) <http://vjolt.student.virginia.edu>
1522-1687 / © 1998 Virginia Journal of Law and Technology Association

VIRGINIA JOURNAL of LAW and TECHNOLOGY

UNIVERSITY OF VIRGINIA	FALL 1998	3 VA. J.L. & TECH. 7

"Don't Ask, Don't Tell;" A Discussion of Employee Privacy in Cyberspace in Light of *McVeigh v. Cohen, et al.*

by Clifford T. Karafin, Esq.[*]

I. Introduction

1. Did you think you could leave your home without the risk of having your secrets known to your employer, your loved ones, or the public at large? Do you believe that there are still any vestiges of privacy to be coveted when the door of your home closes behind you? The answer to both questions, I'm sorry to say, is no. It did not happen because of an act of Congress; the courts did not provide the government with a new window to see inside of our homes. What happened was that a purveyor of the right of passage into the communications frontier of the 90's, a.k.a. the World Wide Web, unmasked an unwary traveler cloaked in a thin veil of anonymity.

2. Earlier this year, it became known that a Navy Chief Petty Officer, who has the misfortune of bearing the same name as the Oklahoma City bomber Timothy McVeigh, was approved for discharge from the Navy by the Chief of Naval Personnel, presumably for openly acknowledging his homosexuality. The District Court of D.C. interceded on a motion by the sailor and issued a

preliminary injunction enjoining his discharge.[1] Discharge proceedings against the sailor were precipitated by the Navy's initiation of an investigation into the sailor's activities as a result of the Navy's discovery that he was using a "screen name"[2] of "boysrch" to access the services of an Internet service provider ("ISP"), America On Line ("AOL"), and to send e-mail. In the McVeigh incident, the sailor's AOL "profile," an AOL listing associated with an individual screen name and available to all AOL members, listed his name as "Tim" and his marital status as "gay." A Navy spouse, serving as an onshore ombudsman, was a recipient of e-mail from McVeigh and became suspicious when she noticed that the e-mail listed the sender's screen name as "boysrch." Upon reviewing the AOL profile for "boysrch," the woman gave the information to the Navy. A Navy paralegal, on orders from a Navy officer, telephoned AOL and requested the name associated with the profile. A customer service representative of AOL provided the sailor's full name to the Navy paralegal, who identified himself as a friend of the sailor and did not reveal himself to be a Navy representative. By providing the sailor's name, AOL admitted subsequently in a letter to members dated January 23, 1998 that the representative violated AOL's own policies regarding members' privacy.[3]

3. AOL's disclosure did not simply expose an individual's voyeurism; instead, it revealed how vulnerable we are to prying eyes when we use an electronic medium for activity we might otherwise have regarded as private. Unfortunately for McVeigh, his use of the Internet (the "Net") was now open to scrutiny by a not-so-forgiving employer. More disconcerting is the fact that current laws may not be adequate to protect the privacy of information in the possession of an ISP.

II. The Electronic Communications and Privacy Act of 1986

4. AOL's actions indeed amounted to more than just a simple unmasking of an individual's anonymity. Privacy advocates will undoubtedly opine that a revelation of this kind further erodes the privacy we enjoy in our homes and in matters we may wish to shield from scrutiny by employers. Fortunately, the American public was afforded some protection against unwanted intrusions into their use of electronic communications media by virtue of the passage of The Electronic Communications Privacy Act of 1986 ("ECPA"),[4] which amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[5] The ECPA was enacted specifically to safeguard the privacy of wire[6] and electronic communications[7] affecting interstate or foreign commerce. Title II of the ECPA generally governs the unauthorized access and disclosure of stored wire or electronic communications.[8] An examination of Title II, in light of AOL's disclosure in *McVeigh*, reveals some shortcomings in the protection afforded to the public.

5. The potential liability of an ISP for an unauthorized disclosure begins with an inquiry into whether or not the information disclosed was *content*; it involves a characterization of the person or entity to whom the information was disclosed; and the inquiry ends with the state of mind of the person or entity making the disclosure. In *McVeigh*, the nature of the inquiry as to liability is whether or not an ISP's disclosure of a person's full name, associated with an individual's screen

name, to a person who fails to identify himself as a government employee is proscribed by the ECPA.

6. Title II of the ECPA proscribes the knowing or intentional divulging of the *contents* of any communication carried or maintained on a remote computing service.[9] "Contents" is defined in Title I of the ECPA as including "any information concerning the substance, purport, or meaning" of any wire, oral, or electronic communication.[10] However, disclosure to a government agency or representative may be compelled upon the government actor's obtainment of a warrant, court order, or administrative subpoena.[11]

7. Alternatively, a remote computing service "may disclose a *record* or *other information* pertaining to a subscriber to or customer of such service (not including the contents of communications . . .) to any person other than a governmental entity."[12] And in the event that a governmental entity obtains proper authorization, a remote computing service may disclose to such entity the "name, address, . . . telephone number . . . and the type of services the subscriber or customer utilized."[13]

8. However harmful a disclosure may be, an aggrieved party will have a difficult time asserting a cause of action directed against an ISP. This is due to the fact that even upon the disclosing of information that is termed "content," an ISP is afforded substantial protection against liability from lawsuits involving unauthorized disclosures of electronic communications.[14] The protection afforded an ISP applies to, but is not limited to, circumstances in which an ISP discloses the contents of a communication to an addressee, an intended recipient or an agent of the addressee or recipient;[15] or the disclosure is made with the lawful consent of the originator or addressee or intended recipient or the ISP subscriber.[16] Immunity is also given to ISP employees and others authorized to forward communications to their destination,[17] and it also attaches to all activities that are incident to the rendition of the computing service.[18]

9. Further complicating matters is the state of mind required for any actor to be liable under the ECPA. A cause of action is provided for "any provider of [an] electronic communication service, subscriber, or other person aggrieved by any violation . . . in which the conduct . . . is engaged in with a *knowing or intentional* state of mind."[19] Noticeably absent from the causes of action afforded an individual are actions that could inure to an individual as a result of negligence by a wrongful actor. In the *McVeigh* incident, the absence of negligence as a standard for culpability could serve to immunize AOL from liability. If the information revealed was content, AOL need only assert that the representative who revealed the information believed that the individual requesting the information was an intended recipient of a communication from McVeigh.[20] If the information disclosed in the McVeigh incident was not content, AOL would be absolved from liability due to the failure of the Navy paralegal to identify himself as a government representative. In summary, the absence of negligence as a standard for liability serves to make the privacy protection afforded individuals against unauthorized disclosures of information by an ISP inadequate.

10. Absent a successful assertion of sovereign immunity[21] or "qualified or official" immunity,[22] a government employer may not be as fortunate as AOL in escaping liability under the ECPA.[23] As previously indicated, a government entity may require disclosure of content or non-content information only upon the issuance of a warrant, an administrative subpoena, or a court order.[24] In *McVeigh*, the Navy officer initiating the inquiry into the identity of the person using the screen name of "boysrch" did not obtain a warrant, nor did he make the inquiry pursuant to a court order or subpoena. Moreover, the facts surrounding the case make it unlikely that the Navy would assert that McVeigh consented to the inquiry initiated by the Navy officer.

11. Alternatively, a person aggrieved by a "private" employer's inquiry into information being retained and stored by an ISP presently has no recourse against his employer under the ECPA. The ECPA contains no provision that proscribes unauthorized private party inquiries into information in the possession of a computing service provider. The onus of preventing disclosure falls upon the ISP, and by virtue of the liability exemptions that the ECPA provides to computing service providers, an ISP can wield a powerful shield against any assertion of liability based upon its actions or the actions of its employees.

12. In essence, the salvation of employee privacy in cyberspace under the ECPA is dependent upon the source of a person's paycheck. For the individual in government service, the home will continue to remain a place of solitude, foreclosed from the harmful agendas cloaked in policy considerations of an entity that influences much of an employee's life, namely his employer. And if wanting for additional privacy protection, the individual in government employment is also fortunate in that he enjoys protection against employment-related violations of his constitutional rights, namely those of the Fourth Amendment and the "right to privacy." In contrast, a person who derives his income from private employment enjoys little of the protection otherwise bestowed upon those in government service. The privately employed individual is subject to having his behavior, thoughts, attitudes, and interests, as expressed in cyberspace and within or outside of the physical confines of his home, scrutinized by anyone outside of government service, including his employer. The private employee's only recourse against unwarranted and unauthorized intrusions into his privacy is through state privacy laws.

III. Constitutional Protection Afforded Governmental Employees

A. The Fourth Amendment

13. Aside from potential ECPA liability, a government actor in the position of the Department of the Navy in the McVeigh incident could face liability pursuant to a violation of the employee's rights under the Fourth Amendment to the Constitution[25] The Fourth Amendment to the United States Constitution protects persons against unreasonable searches and seizures.[26] "A search occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[27] In *Katz v. United States*, the Supreme Court recognized that a "physical intrusion" is not necessary

for an action taken to be termed a search, stating that "the Fourth Amendment protects people, not places."[28] And in *United States v. Knotts*, the Supreme Court further emphasized the Fourth Amendment's protection of the individual, saying that its "application . . . 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."[29]

14. In *O'Connor v. Ortega*, the U.S. Supreme Court, in a plurality opinion, set forth criteria to be employed in determining the *reasonableness* of a search conducted in the workplace context.[30] To be entitled to Fourth Amendment protection, an aggrieved party must have an expectation of privacy that society is prepared to recognize as "reasonable."[31] To determine the standard of reasonableness that applies "in the case of searches conducted by a public employer, [the courts] must balance the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and efficient operation of the workplace."[32] The Court indicated that the context in which a search takes place should be also factored into a determination of reasonableness, stating that "the workplace context includes those areas and items that are related to work and are generally within the employer's control."[33] Furthermore, the *Ortega* court set forth a twofold inquiry to be used to determine the "reasonableness" of any search by a government employer, involving a government employee, in which the search is conducted for "noninvestigatory, *work-related* purposes" or for investigations involving "*work-related* misconduct."[34] Essentially, to determine whether or not a search was reasonable, the Court stated that the first inquiry must consider "whether the [employer's] action was justified at its inception," and secondly, "whether the search as actually conducted was reasonably related in scope to the circumstances which justified the interference in the first place."[35]

15. In *McVeigh*, it is not entirely clear whether or not an attempt to obtain information from a third party, via a telephone call, for the purpose of identifying an individual would constitute a "search" pursuant to the Fourth Amendment. The issue as to whether an individual can claim a constitutionally protected Fourth Amendment interest in a telephone conversation to which he is not a party has not been decided in the federal arena.[36]

16. Also, in *McVeigh*, no physical intrusion into the sailor's privacy was affected. However, the Navy did attempt to solicit from a third party what may be considered private or personal information, and the action taken to obtain the information was arguably in violation of the armed forces "Don't ask; Don't tell" policy.[37] In *United States v. Attson*, the Ninth Circuit stated that in order "to determine whether a given governmental activity is of the kind that is prohibited by the Fourth Amendment, [one] must first ask whether the action is a 'search'."[38] The *Attson* court further opined upon the types of non-law enforcement conduct that it had historically considered to be a search within the scope of the Fourth Amendment, saying that such conduct that was "motivated by some sort of investigatory or administrative purpose designed to elicit a benefit for the government" was entitled to the protection of the Amendment.[39] And "whether the challenged governmental conduct is the type of conduct proscribed by the fourth amendment analytically *precedes* the question of whether there is a privacy interest at stake."[40]

17. An examination of case law relating to the telephone call to AOL in *McVeigh* suggests that a telephone call to a third party could very well be deemed a "search." In *People v. Chapman*, the court was confronted with the issue as to whether the obtainment by law enforcement personnel of a telephone subscriber's name and address from the telephone company violated a criminal defendant's constitutionally protected expectation of privacy pursuant to the state's constitution.[41] What is troubling about the *Chapman* decision and other state court decisions, which have addressed whether the warrantless obtainment of name and address information from a third party is violative of an individual's privacy, is that the courts never explicitly state how the information in question was obtained.[42] Thus, the omission of an explanation as to the manner in which the information was obtained could be interpreted to mean that the courts did not see this as material to their decisions. Should federal courts choose to follow a parallel course to state court decisions if called upon to determine whether a telephone call to a third party could constitute a search, it is likely that they would align themselves with state court precedents.[43]

18. In *McVeigh*, the Navy officer initiated contact with AOL in order to "connect" the screen name "boysrch" and the user profile, provided by the ombudsman, to McVeigh.[44] Thus, a great leap of faith is probably not required in order to conclude that one possible (and likely) motivation of the Navy's actions was premised upon an identification of McVeigh as the owner of the screen name. Pursuant to the reasoning of the *Asston* court, the question that presents itself is whether or not the Navy's actions were motivated by an investigatory or administrative purpose. In *McVeigh*, the court's recitation of the facts indicated that the ombudsman's forwarding of the e-mail to the Navy resulted in the contacting of the Navy's JAG Corps in order to "investigate" the matter.[45] Thus, under the *Asston* rationale, the Navy's placement of a telephone call to a third party could conceivably be termed a search when analyzed in a Fourth Amendment context.[46]

19. In the event that a governmental employer's obtainment of information from a third party via a telephone call would be held to constitute a search, a threshold inquiry, pursuant to *Ortega*, would be necessary to determine if the search initiated by the employer was for *work-related* purposes. Should the threshold inquiry fail, the Fourth Amendment analysis undertaken by the *Ortega* court would not be applicable. In this event, it is likely that a *probable cause* standard would apply, which would require the government actor to obtain a warrant prior to commencing a search.[47] When considering the existence of a government employer's policy, which purportedly limits government inquiries into the sexual preferences of its employees, a government actor in the position of the Navy in *McVeigh* would be forced to justify the AOL inquiry as being for a non-investigatory work-related purpose or work-related misconduct. Failure to justify the search as being for one of the aforementioned reasons could result in a determination that a government actor violated the aggrieved individual's Fourth Amendment rights.[48]

20. If a government employer's conduct amounts to a search, and the search at its inception is justified, the inquiry under *Ortega* proceeds to a determination as to whether the scope of the search was reasonable, taking into consideration the context in which it took place. When looking to the reasonableness of the search, a determination is required as to whether or not the affected

employee had a reasonable expectation of privacy in the area or items searched. It has become an axiom of workplace Fourth Amendment jurisprudence that office practices, procedures, and legitimate employer regulations are to be considered when assessing the context of a workplace search in order to determine its "reasonableness."[49] Additionally, a contract between an employer and an employee can, "under appropriate circumstances, diminish (if not extinguish) [an employee's] legitimate expectations of privacy."[50]

21. A defense available to government actors upon an individual's assertion of his Fourth Amendment rights, and one that would be available to an actor in a like position to that of the Navy in *McVeigh*, would be to assert that the information obtained had already received public exposure. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[51] The public exposure doctrine has been the center of analysis in various state court decisions in which courts were faced with the issue as to whether a person can have a reasonable expectation of privacy in his name and address. For example, in *State v. Chryst*, the court held that a person's name and address, by themselves, do not constitute information about which a person can have a reasonable expectation of privacy.[52] The court's rationale centered upon the public exposure of one's address insofar as its appearance in public records and the like.[53] Alternatively, in *People v. Chapman*, the Supreme Court of California, sitting en banc, held that a criminal defendant, who had maintained an unlisted telephone number with the telephone company, had a reasonable expectation of privacy in his name and address.[54] The court reasoned that the defendant's disclosure of her name and address to the telephone company was not volitional and was for the limited purpose of billing. Additionally, the court also expressed a concern about the possibility that the warrantless disclosure of such information could provide a "missing link to make up a *virtual biography* about the subscriber."[55] Other state courts have also expressed opinions, with differing results, concerning an individual's expectation of privacy in his name and address.[56]

22. Faced with a possible violation of an employee's Fourth Amendment rights, a government actor in the position of the Navy in *McVeigh* would likely assert that the sailor's e-mail communications with the Navy ombudsman would reduce or eliminate any Fourth Amendment rights he might otherwise have enjoyed. "It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information."[57] "However strongly a defendant may trust an apparent colleague, his expectations . . . are not protected by the Fourth Amendment when it turns out that the colleague is . . . communicating with the authorities."[58] In *McVeigh*, the e-mail sent by McVeigh to the Navy ombudsman allegedly contained his screen name, and it's conceivable that the recipient may have had some idea as to the identity of the sender. Thus, a factfinder could determine that the Navy's telephone call to AOL did not result in the Navy's obtainment of any information not already in its possession. Moreover, should a court determine that a person has no Fourth Amendment right of privacy in his name and address, an individual in the position of McVeigh would undoubtedly find it difficult to prevail on a claimed Fourth Amendment violation.

23. Whether a court faced with an alleged Fourth Amendment violation emanating from a telephone call to a third party in an employment context would reach the issue of an employee's reasonable expectation of privacy is open to speculation. It is also open to debate as to the likelihood that the court would hold that an individual's name and address is subject to Fourth Amendment protection.[59] If a court were to rule in the affirmative, the issue that would then be addressed, presuming that the court chose to follow *Ortega*, is whether that expectation of privacy was diminished by any workplace practices, procedures, or policies in place. Conversely, if a court were to rule in the negative, the question that begs an answer is whether the absence of an objective expectation of privacy can ripen into an objectively reasonable expectation of privacy for Fourth Amendment purposes by virtue of an employer policy that limits the employer's own conduct. Although I could find no case that directly addressed this issue, I was able to locate two decisions outside of the employment context that address whether a person's "conduct" may transform a subjective expectation of privacy into one that is objectively reasonable. In *United States v. Watson*, the court held that a hotel guest's late pre-payment of his next day's room charges for three consecutive days manifested his intent to continue his stay, thus affording him a reasonable expectation of privacy in his hotel room subsequent to the hotel's normal check-out time.[60] And in *United States v. Owens*, the 10th Circuit held that a defendant that had paid for a week's rental of a hotel room in advance, but was not regarded by the hotel as a weekly tenant, was entitled to a reasonable expectation of privacy in his room by virtue of "prior conduct."[61] In *Owens*, the government claimed that the defendant was a daily (vs. a weekly) tenant, ending his expectation of privacy in his hotel room prior to the time the police conducted a warrantless search.[62] In summary, both *Watson* and *Owens* may suggest that a pattern or past practice established by an individual can cause an expectation of privacy, which is not objectively reasonable, to be transformed into one that is reasonable by societal standards. In this event, it is not entirely unthinkable that a court could use *Watson* and *Owens* as a basis for finding that an employee's expectation of privacy could be enhanced (rather than just diminished) by an employer's past practices or policies. Such a decision would undoubtedly draw praise from privacy advocates nationwide.

B. "Right to Privacy"

24. Although the assertion of one's Fourth Amendment rights gives rise to a constitutional-based cause of action in the case of a governmental inquiry into one's personal affairs, the assertion of an individual's "right to privacy" provides another potential source of relief. To be accorded relief based upon a right to privacy action, a person seeking relief must show governmental interference in his "fundamental rights" or rights "implicit in the concept of ordered liberty."[63] The rights traditionally accorded protection are those involving marriage, procreation, contraception, family relationships, child rearing, and education.[64] Perhaps pertinent to the plight of McVeigh, however, is the Supreme Court's refusal to extend privacy protection to homosexuals engaged in acts of consensual sodomy.[65]

25. In *Whalen v. Roe*, the Supreme Court extended the constitutional protection of individual privacy to encompass the disclosure of personal matters to the government.[66] When faced with a claim of an intrusion into personal matters in the employment context, the courts are inclined to employ a balancing test, weighing the public interest in disclosure against the individual's privacy interests.[67]

26. Given the factors in *McVeigh*, it is unlikely that a court faced with deciding whether or not an instrusion into a government employee's privacy occurred as a direct result of a telephone call to an ISP would find that such an invasion did in fact occur. In *McVeigh*, the telephone call made to AOL by the Navy representative was presumably made for the purpose of obtaining an identification; no information was purportedly obtained that would be encompassed by one of the protected categories. Alternatively, the launching of an investigation into a government employee's background, in total, could give rise to an invasion of privacy claim. Such a discussion, however, is beyond the scope of this article.[68]

C. Summary

27. The absence of adequate precedent regarding an employee's expectation of privacy in the workplace makes it difficult to speculate on the likelihood of success that an employee in a similar position to that of McVeigh might have in his assertion of a Fourth Amendment claim. A court might choose to analyze the claim by following the framework set forth in *Ortega*, with consideration possibly given to *Asston*, in which case it is questionable whether the court would reach the issue regarding the employee's reasonable expectation of privacy. Or the court might choose to analyze the claim by following *Katz*, whereby the issue regarding the employee's reasonable expectation of privacy would most likely be answered as a threshold question. Another alternative would be for the court to analyze the claim using a hybrid framework of analysis premised upon the holdings of both *Katz* and *Ortega*. In the latter event, it is possible that the court might reach the privacy issue twice: once as a threshold question to assist in a determination as to whether a search took place; and if a search was effected, the privacy issue might be analyzed again in terms of the employee's expectation of privacy in the context of the workplace. In summary, uncertainty in the framework of analysis breeds uncertainty in the predictability of the outcome.

28. The focus of Fourth Amendment protection in the workplace remains centered on the employer's tangible sphere of influence as opposed to the information that traverses that sphere. Perhaps a greater focus on the informational aspects of workplace privacy is needed to bring Fourth Amendment workplace jurisprudence into the information age of the 90's and beyond. Justice Douglas was arguably endowing us with his foresightedness when, in *United States v. White*, he stated that "electronic surveillance is the greatest leveler of human privacy ever known."[69] "To be sure, the Constitution and Bill of Rights are not to be read as covering only the technology known in the 18th century. Otherwise its concept of 'commerce' would be hopeless when it comes to management of modern affairs."[70] Should the Supreme Court choose to revisit the

issue of Fourth Amendment rights in the workplace, they might choose to consider the changes that have taken place in the handling of information in the workplace since *Ortega* was decided.

29. Focusing on the intangible, as opposed to the tangible, however, is fraught with problems of definition, not to mention the various approaches to understanding the embodiment of the words contained within the Constitution. Suppose, for example, the Navy officer in *McVeigh* had initiated an inquiry into the sailor's background by accessing, via computer, information held by another government agency to which the officer had privileged access.[71] Is there any difference between "information" gathered via a computer search as opposed to that gathered by searching the physical confines of an employee's workspace? If the Fourth Amendment protects the person, what are its boundaries when information resides in a place apart from the employer's physical sphere of influence? Should the Supreme Court eventually reconsider the *Ortega* criteria, it will be interesting to see whether the Court will choose to analogize computer aided information gathering techniques to those of the parochial workplace search or leave intact the traditional but perhaps outmoded notion of what constitutes the "workplace" for Fourth Amendment purposes.

30. For all practical purposes, a person's "right to privacy" is unlikely to be an Achilles heel for a government employer that probes into an employee's privacy on the Internet. The "right to privacy" is applicable only to select categories designated by the Supreme Court as deserving of protection. A government employer's traversing upon an employee's rights in any of the designated categories, with or without the aid of a computer, is likely to give rise to a cause of action for an invasion of privacy. The focus of the protection is categorical, it is based seemingly on the substantive information obtained versus the manner employed to obtain it. Consequently, it is unlikely that changes in the manner in which information, personal or otherwise, is used, communicated, or stored will weigh heavily into any expansion or alteration in scope of the constitutional "right to privacy" protection accorded any aggrieved party.[72]

IV. State Common Law Privacy Rights

31. In the event that an unwarranted and unwanted intrusion occurs into an individual's private affairs, and the intrusion is into a matter which society has said the person may keep to himself, the person who is aggrieved by the intrusion may be entitled to relief at common law.[73] For a prospective plaintiff to have a common law action for the tort of "intrusion upon seclusion," the plaintiff must be able to demonstrate that he had a "reasonable expectation of privacy" in the matter intruded upon and that the intrusion would be "highly offensive to a reasonable person."[74] A "defendant'[s] duty to refrain from [an] intrusion into another's private affairs is not absolute in nature, but rather is limited by those rights which arise from social conditions, including the business relationship of the parties."[75] When considering the offensiveness requirement, courts will generally consider the degree of the intrusion, the context in which the intrusion occurs, the intruder's motives and objectives, and the privacy expectations of those whose privacy is invaded.[76] Additionally, some courts have added an additional requirement, stating that the intruder's actions must "foreseeably result in extreme mental anguish,

embarrassment, humiliation, or mental suffering."[77]

32. In certain circumstances, the courts have held that the interest of the public demands that employees in certain professions acquiesce to what might otherwise constitute an invasion of an employee's privacy. For example, a police officer may be required to undergo random drug testing due to the fact that he is called upon to "exercise[] the most awesome and dangerous power that a democratic state possesses with respect to its residents - the power to use lawful force to arrest and detain them."[78] Similarly, railroad workers may be required to subject themselves to drug testing because of the risk of injury to the public arising from the discharge of their duties.[79] And in *National Treasury Employees Union et al. v. Von Raab*, the Court stated that the public's interest in ensuring the safety and integrity of our borders resulted in a diminished expectation of privacy on the part of certain customs employees with respect to tests that bare on their "fitness and probity."[80]

33. Other considerations also factor into an employee's reasonable expectation of privacy. Employer practices and procedures, announced workplace policies, and the signing of a notice and waiver of rights will, by law, reduce the expectation of privacy on the part of individuals in the workplace.[81] And with respect to private employers, their actions may be sanctioned at common law unless there is a "clear mandate of public policy" that weighs in favor of the employee's privacy rights.[82]

34. Alternatively, not all employer actions are insulated from common law liability under the tort of intrusion upon seclusion. An employer's persistent demands for information concerning an employee's "sexual proclivities and personality," regardless of whether any information was obtained, is to be considered an "examination" into an employee's private concerns and actionable at common law.[83] An employer's opening of an employee's "private mail" and reading it without authority may be deemed an invasion of an employee's privacy.[84] Also, the planting of a concealed listening device in an employee's office by an employer will give rise to the tort of intrusion upon seclusion.[85] In addition, it has been held that a former employer's obtainment of information communicated by employees in confidence to a third party may be sufficient to state a cause of action for intrusion upon seclusion.[86] Also, an employer's search of an employee's workplace when "done in such a way as to reveal matters unrelated to the workplace, may constitute [a] tortious invasion of the employee's privacy."[87]

35. The courts have also held that other employer actions will not support an invasion of privacy claim. For example, a telephone call to an employee's former employer to verify the accuracy of information on an employment application was held to be an inquiry into the employee's "business affairs" as opposed to her personal solitude or personal affairs and was therefore not actionable against the former employer.[88] And it has been held that an employee has no reasonable expectation of privacy in e-mail communications made voluntarily over a company e-mail system, despite assurance that such communications were confidential.[89] Also, an employer's attempts to inquire into information about an employee's injuries, occurring during

the course of employment, by sending a letter to the employee's private physician, was not an action that would be "objectionable to a reasonable person."[90] Furthermore, an employer's inquiry into the identity of any employee in a matter unrelated to the employee's employment is not conduct that would be "highly offensive" and is thus not an invasion of privacy.[91] Finally, an employer's possession of an employee's private financial information, without a showing by the employee that the information was obtained improperly or acted upon, would not be "highly offensive to a reasonable person." [92]

36. Should a plaintiff in a like position to that of McVeigh choose to assert a cause of action for a common law invasion of privacy, a court would undoubtedly look to any employer policies, procedures, or practices in place in order to ascertain the context in which the alleged invasion occurred. In a matter bearing material similarities to the circumstances portrayed in *McVeigh*, a court would most certainly undertake an examination into any actions taken by a government actor in light of any workplace policies set forth by the employer.[93] A court would also examine the employee's reasonable expectation of privacy while considering any public policies (constitutional, statutory, or common law) that would warrant a diminished expectation of privacy on the part of the employee; office practices and procedures that would likewise warrant a diminished expectation of privacy; the degree of the intrusiveness of the government actor's conduct; and common law precedent in the state whose law is applied to the action.[94] The placement of a telephone call alone would probably not be regarded as "highly offensive" in a common law context; nor is there a clear precedent which would suggest that a plaintiff finding himself in the position similar to that of McVeigh would have a reasonable expectation of privacy in the information obtained: his name and location. Alternatively, *any* inquiry that could be characterized as an investigation into a government employee's sexual proclivities could be contrary to established policy and may thus give rise to liability.

37. Alternatively, whether a non-government employee would be successful in asserting a common law privacy action against an employer should a private employee find himself in a situation baring some similarities to that of McVeigh, would depend on much the same factors as are used when considering a governmental employee's right to privacy. The factors include: the nature of the information acquired or solicited; the reasonableness of the employee's expectation of privacy; public policies favoring a diminished expectation of privacy on the part of the affected employee; announced employer policies, practices, or procedures; action (if any) taken by the employer which is deemed to be injurious to the employee, any countervailing interests on the part of the employer, and state law. A determination would then need to be made as to whether the employer's actions were violative of any public policy mandates. The main difference between an examination into a governmental employee's alleged invasion of privacy and a similar allegation on the part of a private employee is the nature of the public policy inquiry. As is evident in *McVeigh*, a governmental employee's assertion of an invasion of privacy is likely to be premised on an alleged violation of an articulated policy, having its basis in constitutional, statutory, or common law. Alleged invasions in the private employee arena are likely to involve more of a balancing of employee interests against public policy, with the weight favoring the employer.[95]

38. In summary, case law on employers' tortious invasions of employees' privacy rights does not appear generally favorable to any action that is not egregious and intolerable when looked upon from the viewpoint of society as a whole. Upon reviewing available case law involving the unauthorized access of employee electronic communications by an employer, I failed to unearth a case where the outcome was favorable to the employee.[96] Thus, an employer's obtainment of what may or may not be personal information about an employee, directly or indirectly from a third party ISP or from an employer owned and operated computer system, without more, is unlikely, under current law, to provide an employee with a meritorious cause of action against his employer for an invasion of privacy. Unless the courts change direction, plaintiffs are unlikely to succeed in seeking refuge from inquisitive employers under a common law right to privacy when wishing to maintain privacy in their communications involving the use of computing service providers.

V. Conclusion

39. "The Internet has emerged as an appliance of everyday life, accessible from almost every point on the planet." [97] This fact has most certainly spurned the growth in Internet commerce, which is expected to reach forty times its current volume--from $8 billion to approximately $327 billion in goods and services traded between companies--by the year 2002.[98] World trade involving computer software, entertainment products, information services, etc. now account for over $40 billion of U.S. exports.[99] However, the continued growth of the Internet's role in global commerce will depend upon a predictable legal environment, one that can provide assurances of personal privacy to the consuming public.

40. The results of a recent poll suggest that assurances of personal privacy may be critical to the Internet's continued growth. The poll results indicated that a majority of the respondents who chose to stay off the Net did so because of privacy concerns.[100] Use of the Net "can, if not managed carefully, diminish personal privacy. It is essential, therefore, to assure personal privacy . . . if people are to feel comfortable doing business [online]."[101] Moreover, in a June 1995 report entitled "Privacy and the National Information Infrastructure," issued by the Privacy Working Group ("Working Group") of the United States government's Information Infrastructure Task Force, the Working Group recommended a set of principles, referred to as the "Privacy Principles," to govern the collection, processing, storage, and re-use of personal data in the information age.[102] Standing prominent among the three values identified by the Privacy Principles, which the Working Group submits should be used to govern the way in which information is acquired, disclosed, and used online, is that "an individual's reasonable expectation of privacy regarding access to and use of his or her personal information should be assured."[103]

41. In the employment context, a survey of American businesses by *Macworld* magazine indicated that over twenty percent of respondents had conducted searches of employee computer, voice mail, e-mail, or other networking communications files.[104] And for companies with more than

1,000 employees, that figure rose to over thirty percent.[105] Additionally, the same study revealed that of those companies monitoring electronic communications, over forty percent had searched employee e-mail files.[106] If this and other surveys are indicative of a predisposition on the part of employers to monitor employee electronic communications, it does not appear that employees will enjoy privacy in their use of the Net for e-mail or other electronic communications in the workplace anytime soon.[107]

42. In this article, I identified four sources of legal protection afforded the public in its use of the Internet. Of the four sources, two are available to non-governmental employees who may choose to assert their right to privacy in their use of the Net, both within and outside of the workplace, against an employer's unauthorized access and use of information relating to the employee's use of the Net. The two sources referred to are the Electronic Communications Privacy Act of 1986, herein referred to as the "ECPA," and state common law. Two additional sources were identified as potential sources of legal redress for government employees--the Fourth Amendment guarantee against unreasonable searches by the government and the constitutional guarantee of an individual's "right to privacy."

43. Of the available sources, the most likely target for change would be the ECPA. Because the ECPA is a federal act, designed to affect the general populace, it is probably the most logical choice to provide uniform assurances of Internet privacy to most Americans. Excepting one, the remedial measures being recommended are not targeted specifically to address Internet privacy only in the workplace, but represent an approach to providing legal recourse to anyone who is aggrieved by an intrusion into his or her personal privacy as it relates to using the Net. Targeting just the employer-employee relationship would ignore other possible third party infringements of a person's privacy on the Net, and would run the risk of exceeding Congress' constitutional law-making authority.

44. The first change to the ECPA, which would have a profound effect on assuring privacy in an individual's use of the Net, would be to change the standard of liability for unauthorized disclosures of content and non-content information to a "negligence" standard. The doctrine of negligence "rests on [the] duty of every person to exercise due care in his conduct towards others from which injury may result."[108] Negligence is the "failure to do what a person of ordinary prudence would have done under similar circumstances."[109] The enactment of such a change would presumably force remote computing services, e.g. ISPs, to adopt and enforce internal policies to ensure that information is not divulged without proper authorization. In *McVeigh*, had the AOL employee sought to adduce proof from the Navy paralegal of his authority to receive information on McVeigh's behalf, the AOL employee would likely never have revealed the user's identity to the Navy.

45. Another congressional amendment, one which would serve well the objectives of achieving internet privacy, would clarify the liability of a government actor that solicits information from an ISP without properly identifying himself to the communications provider.[110] In *McVeigh*, the government argued that the substantive provision of the ECPA statute in question puts the

obligation on the ISP to withhold information from the government, and not vice versa.[111] The government failed to win its argument in the district court's ruling; however, should use of the Internet continue to grow as projected, it is likely that this issue will be revisited by the courts. More generally, the implication of the confusion encompassing the statute is that it might not be unlawful for a government actor to obtain non-content information about any individual without a court's authority. Absent judicial oversight, personal privacy on the Net is in jeopardy.

46. Although the ECPA proscribes the unauthorized disclosure of content and non-content information on the part of a remote computing service, it does not address requests for content and non-content information from persons or entities other than those in government service. In essence, the onus is on the service provider to ensure that personal information does not find its way into nefarious hands. The lack of a provision addressing non-government actors leaves open the possibility that an ISP may be duped into providing information to a party not authorized to receive it. This is presumably what happened in the *McVeigh* incident. And as noted, without a negligence standard for liability, an ISP may be exempt from liability under the current ECPA. Moreover, should a private actor request information that is deemed "content," and should the ISP so provide it, the private actor would not have committed any unlawful conduct. Thus, a companion statute proscribing the unauthorized obtainment of any information from a remote computing service would serve to ensure individual privacy in cyberspace.

47. At a minimum, one last amendment would be needed to ensure individual privacy on the Net. Unlike previously articulated addendums, the final recommendation is targeted specifically towards the employer-employee relationship. This recommendation calls for Congress to enact legislation making it mandatory for companies exceeding a pre-determined size to develop and distribute a policy concerning the use of computer networking equipment employed in the workplace and made available for use by the employees.[112] Such an enactment would serve multiple purposes: 1) it would lay to rest the question whether the ECPA governs the actions of private employers who use "electronic communications" as defined under the ECPA, and 2) it would put employees on notice as to any actions that are proscribed in the employees' use of the employer's equipment. Such a provision would be equitable to both employer interests and employee interests. Employer interests, consisting primarily of maintaining supervision of, control over, and efficiency in the workplace, [113] would be served by alerting employees as to the proper use of the informational tools provided by the employer. Moreover, by expressly bringing private employers that provide their own Internet gateway under the umbrella of the ECPA, they would be shielded from liability pursuant to the provider exemptions of the ECPA. Finally, employee interests would be served because employees would have legal recourse under the ECPA against an employer that was not compliant with federal law governing the use, facilitation, and access to electronic communications.

48. In conclusion, it is only through the acts of our legislative bodies and courts that we can be assured of maintaining the dignity of our private spheres. Perhaps we, as individuals, in our private existence and in our existence outside of the sanctity of our homes, should pay homage to the words of Samuel D. Warren and Louis D. Brandeis, echoed more than a century ago: [114]

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasion upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.

Footnotes

[*] J.D., 1995, Temple University School of Law; 1995-96, Law Intern to the Honorable David A. Scholl, Chief Judge of United States Bankruptcy Court for the E.D. of Pennsylvania; 1991, M.B.A. Drexel University; 1986-98, Information Technology Consultant for John Hancock Insurance Co., Honeywell, Inc., General Electric, Inc., Lockheed Martin, Inc., Rohm and Haas, Inc.

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

[2] A screen name is comprised of a combination of characters (usually letters and numbers) used by a subscriber to access the services of an internet service provider. A screen name is normally chosen by the subscriber of the service provider and is unique to each subscriber. Its primary purpose is to serve as an identifier for access to the provider's services.

[3] It should be noted that the letter was available on-line and accessible only to AOL customers. Also worthy of note is AOL's refusal to supply any written commitment to maintaining the privacy of member information to prospective customers. I twice requested such a commitment in writing and was informed both times that any information concerning the company's commitment to member privacy was available only to members.

[4] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

[5] Omnibus Crime Control and Safe Streets Act of 1986, Pub. L. No. 90-351, 82 Stat. 211 (codified as amended at 18 U.S.C. §§ 2510-2520 (1997)).

[6] A "wire communication," as defined under the ECPA, is "any aural transfer made . . . through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication." 18 U.S.C. § 2510(1) (1997).

[7] An "electronic communication" under the ECPA is "any transfer of signs, signals, writings, images, sounds, data, or intelligence . . . transmitted . . . by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does *not* include . . . (A) any wire or oral communication." 18 U.S.C. § 2510(12) (emphasis added).

[8] 18 U.S.C. §§ 2701-2710 (1997); s*ee also Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 464 (5th Cir. 1994).

[9] 18 U.S.C. § 2702(a)(2) (emphasis added).

[10] 18 U.S.C. § 2510(8).

[11] Under 18 U.S.C. § 2703(a), the government can compel disclosure for any electronic communication in storage for 180 days or less only upon obtaining a warrant. For a communication in storage for *more than* 180 days, a governmental entity must obtain a warrant, *id.* at § 2703(b)(2)(A), or an administrative subpoena, *id*. at § 2703(b)(2)(B)(i), or a court order, *id*. at § 2703(b)(2)(B)(ii).

[12] 18 U.S.C. § 2703(c)(1)(A) (1997) (emphasis added).

[13] 18 U.S.C. § 2703(c)(1)(B), (C).

[14] Many commentators have suggested that the provider exception is to be read broadly. More specifically, commentators have suggested that employers that provide their own e-mail systems on employer owned and operated computers may be exempt from liability for perusing and disclosing e-mail communications transmitted through the employer's system. Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J. L. & TECH. 345, 359 (1995). And in *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996), the court applied the ECPA's provider exception relating to unlawful *access* to electronic communications to a city owned and operated paging system absent evidence that the system was used in interstate commerce).

Congress may indeed have intended the ECPA to apply to "wire communications" used for interstate as well as *intrastate* communications. The legislative history of the ECPA states that the language used in the definition of a wire communication "recognizes that private networks and intra-company communications systems are common today and brings them within the protection of the statute." Act of October 21, 1986, Pub. L. 99-508, 1986 U.S.C.C.A.N. (100 Stat. 1848) 3566. However, wire communications are explicitly excluded from the definition of an "electronic communication." See § 2510, *supra* note 7. And it has been held that e-mail is an electronic communication. *Steve Jackson Games*, 36 F.3d at 458. Furthermore, the ECPA states explicitly that it applies to electronic communications that affect *interstate* commerce. 18 U.S.C. § 2510 (emphasis added). Moreover, in *Andersen Consulting LLP v. UOP*, No. 97 C 5501 (N.D. Ill. Jan. 23, 1998), the court held that a company that provided an e-mail service, accessible to contractors, company personnel, and other third parties,

was not a provider of an electronic communications service pursuant to the ECPA. Should future judicial interpretations prove consistent with *Andersen,* employees and other aggrieved parties will be foreclosed from asserting a cause of action against employers under the ECPA for the unauthorized disclosure of the contents of electronic communications.

[15] 18 U.S.C. § 2702(b)(1) (1986).

[16] 18 U.S.C. § 2702(b)(3).

[17] 18 U.S.C. § 2702(b)(4).

[18] 18 U.S.C. § 2702(b)(5).

[19] 18 U.S.C. § 2707(a) (1986) (emphasis added). The statute, on its face, does little to elucidate the actions to which the state of mind requirement may apply.

[20] Given the absence of a negligence standard, the belief on the part of the AOL representative that he was disclosing the information to an intended recipient may not even be judged by a standard of reasonableness. However, the statute does little to suggest whether it was Congress' intent that the state of mind requirement apply to an actor's knowledge as to the identity of the recipient of the disclosure or to the actual disclosure itself.

[21] Sovereign immunity is a doctrine that "precludes [a] litigant from asserting an otherwise meritorious cause of action against a sovereign . . . unless [the] sovereign consents to suit." BLACK'S LAW DICTIONARY 1252 (5th ed. 1979). Pursuant to Congress' enactment of the "Tort Claims Act," the United States is precluded from asserting sovereign immunity in a tort action by an injured party, unless the injury to the aggrieved party results from conduct by a federal official acting within the scope of his official duties and the conduct is discretionary in nature. 28 U.S.C. §§ 2671-2680 (1996); 28 U.S.C. § 1346(b) (1996). *See also Westfall v. Erwin*, 484 U.S. 292, 297-298 (1988) ("absolute immunity from state-law tort actions should be available only when the conduct of federal officials is within the scope of their official duties and the conduct is discretionary in nature.").

Alternatively, the circumstances under which a state can invoke sovereign immunity for the tortious acts of a state government actor is left to the discretion of the individual states. *Seminole Tribe of Florida v. Florida*, 517 U.S. 44, 70 nn.12-13 (1996). "Under the doctrine of sovereign immunity, the state is not liable for the torts of its agents or officers unless there is a constitutional or statutory waiver of immunity." *State v. McGeorge*, 925 S.W.2d 105, 107 (Tex. App. 1996). The immunity enjoyed by a state may also extend to a municipality as a political subdivision of the state. *See, e.g., Hill v. Dekalb Reg'l Youth Detention Ctr.*, 40 F.3d 1176, 1197 n.36 (11th Cir. 1994). However, under certain circumstances, a municipality will not enjoy immunity for an action premised upon a violation of federal law and asserted pursuant to 42 U.S.C. § 1983. *Leatherman v. Tarrant County NICU*, 507 U.S. 163, 166 (1993).

[22] Official or qualified immunity protects individual governmental employees from liability "when they perform discretionary functions in good faith and within their authority." *McGeorge*, 925 S.W.2d at 108. And where a governmental employee has no liability because of official immunity, the governmental entity by which he is employed is not liable. *Id.* However, when the government employee's acts do not call for deliberation, discretion, judgment, or a policy choice, the defense of sovereign immunity will not be available. *Tilton v. Dougherty*, 493 A.2d 442, 446 (N.H. 1985).

[23] *See Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 816 F. Supp. 432, 442-443 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457, 464 (5th Cir. 1994).

[24] A governmental entity's liability with respect to unauthorized access to the *contents* of stored electronic communications was established in *Steve Jackson Games*, 36 F.3d. at 464. However, whether or not a governmental entity may be liable for the unauthorized access of a *record or other information* involving stored electronic communications is questionable. In *Steve Jackson Games*, the court stated that "Section 2703 [of the ECPA] sets forth the requirements for governmental access to the contents of *electronic* (but not wire) communications." *Id.* at 464, n.10 (emphasis added). The court upheld the district court's finding of governmental liability for unauthorized access to the contents of the plaintiff's e-mail communications pursuant to 18 U.S.C. § 2703(a) & (b) *Id*. at 464. However, in *Tucker v. Waddell*, 83 F.3d 688, 693 (4th Cir. 1996), the court held that 18 U.S.C. § 2703(c) does not prohibit governmental accession of non-content information, unless the governmental entity aids and abets or conspires in a provider's violation of the same section.

In the case on which this article is based, *McVeigh v. Cohen*, the court refuted the government's contention that § 2703(c)(1)(B) pertained only to provider disclosures, saying that the aforesaid section must be read in the context of the statute as a whole. *McVeigh*, at 220. The court further stated that "all of the subsections of § 2703 were intended to work in tandem to protect consumer privacy." *Id.*

[25] It should be noted that a private employer is *not* subject to any Fourth Amendment constraints on searches and seizures. *United States v. Jacobsen*, 466 U.S. 109, 115 (1984).

[26] The Fourth Amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. CONST. amend. IV.

[27] *Jacobsen*, 466 U.S. at 113.

[28] 389 U.S. 347, 351 (1967). In *Katz*, the Court held that attaching a listening device to the outside of a telephone booth used to place calls, without a warrant, violated the individual's Fourth Amendment rights.

[29] 460 U.S. 276, 280 (1983) (citing *Smith v. Maryland*, 442 U.S. 735, 740-741 (1976)). In *Knotts*, the Court held that the monitoring of beeper signals served to augment the visual surveillance of individuals

from public places and did not therefore invade the individuals' legitimate expectation of privacy so as to constitute a search pursuant to the Fourth Amendment.

[30] 480 U.S. 709 (1987).

[31] *Id.* at 716.

[32] *Id.* at 719-20.

[33] *Id.* at 715. The *Ortega* Court provided examples of items which may be outside of the workplace context, such as "closed personal luggage, a handbag, or a briefcase." *Id.* at 716. Worthy of note is the Court's focus on physical items or belongings as opposed to what may lie inside or otherwise be associated with the items, namely "information."

[34] *Id.* at 725-726 (emphasis added).

[35] *Id.* at 726.

[36] The Supreme Court has, however, held that an individual that is a party to a telephone conversation can assert a Fourth Amendment interest in the conversation. *See Katz*, 389 U.S. at 352 (1967).

[37] The policy was adopted by the armed services pursuant to Congress' enactment and codification of 10 U.S.C. § 654 (1994).

[38] 900 F.2d 1427, 1429-30, (9th Cir. 1990) (quoting *Jones v. McKenzie*, 833 F.2d 335, 338 (D.C. Cir. 1987), *amended in part*, 878 F.2d 1476 (D.C. Cir. 1989)). In *Attson*, a criminal defendant challenged the taking of his blood by a government doctor on Fourth Amendment grounds.

[39] *Attson*, 900 F.2d at 1430-31. Conversely, the *Attson* court also stated that "governmental conduct which is not actuated by an investigative or administrative purpose will not be considered a 'search' . . . for purposes of the fourth amendment." *Id.* at 1431.

[40] *Id.* (emphasis added). In *Katz*, Justice Harlan, in his concurring opinion, stated that the expectation of privacy articulated by the Court actually entails a twofold requirement; the "first [one being] that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* at 361 (Harlan, J., concurring). Although it is tempting to say that no search was effected because a defendant did not actually expect privacy, such reasoning, according to Professor LaFave, "is to be avoided." W. R. LAFAVE, SEARCH AND SEIZURE § 2.1(c), at 386-87 (3d ed. 1996). Even though it may "lead to the correct result, [such an analysis] distorts and unduly limits the rule of the *Katz* case." *Id.* Thus, it would appear that Professor LaFave, who relies

heavily on Justice Harlan's concurrence in *Katz*, would agree with the *Attson* court's analysis. It is important to note, however, that the Supreme Court has not provided a framework of analysis for determining whether or not a "search" was actually effected in a workplace context.

[41] 679 P.2d 62, 71 (Cal. 1984).

[42] *Chapman*, 679 P.2d at 65. *See also State v. Faydo*, 846 P.2d 539 (Wash. App. 1993) (detective *contacted* telephone company to locate defendant's residence); *State v. Chryst*, 793 P.2d 538, 539 (Alaska App. 1990) (state trooper *contacted* utility company to obtain address and consumption information of criminal defendant). *State v. Smith*, 367 N.W. 497, 503 (Minn. 1985) (police *obtained* defendant's address from the county social services agency).

[43] The *Chapman* decision and its progeny involved state law challenges as opposed to Fourth Amendment challenges. However, lacking an appropriate federal case law precedent, I believe proceeding to the next level of analysis is the only logical choice to determine whether the conduct of an actor in the position of the Navy in *McVeigh* could be proscribed under the Fourth Amendment.

[44] *McVeigh*, 983 F. Supp. at 217. The district court's opinion also stated that the Navy's actions resulted in a "verification." *Id.* However, whether this term was used to indicate a verification of McVeigh's identity or his homosexuality is not known.

[45] *Id.* It is presumed that the Navy' motivation was to identify a homosexual in active military service. Although unlikely, it is acknowledged that the Navy might have possessed a less deleterious motive when launching the investigation. For example, the Navy could assert that its investigation was premised upon a concern for the well-being of the ombudsman in receipt of the e-mail from McVeigh. Such an argument would undoubtedly focus upon the suggestive nature of the screen name found on the e-mail, and the possibility that additional communiqués would be received coupled with an increase in the suggestive nature of their content. However, since the Navy's inquiry was pursuant to an investigation, it is unlikely that such an assertion would deter the application of the *Asston* rationale.

[46] In the federal arena, at least one court has held that obtaining information solely for the purpose of identifying ownership may constitute a "search." *See United States v. Concepcion*, 942 F.2d 1170 (7th Cir. 1991). In *Concepcion*, government agents arrested a criminal suspect, seized his keys, and used them to unlock an apartment in order to determine whether the residence belonged to the defendant. The defendant contested the agents' actions as being an unlawful search, and the court held that the agents' actions constituted a lawful warrantless "search." In so holding, the court reasoned that by inserting and turning the key in the lock, the agents obtained information from inside the lock, i.e. the tumblers, which was not open to public view. *Id.* at 1172. *But see United States v. Lyons*, 898 F.2d 210 (1st Cir. 1990), (insertion of a key into a lock solely for the purposes of identifying ownership did not constitute a search).

[47] In discussing the Fourth Amendment standard to apply to employer searches, the *Ortega* court made reference to *Gillard v. Schmidt*, 579 F.2d 825, 829 n.1 (3d Cir. 1978), which the Court interpreted as implying that a warrant would be required for an employer search that was not work-related. *Ortega*, 480 U.S. at 738 n.5. *See also United States v. Taketa*, 923 F.2d 665, 675 (9th Cir. 1991) (court held that federal employer's warrantless search of a federal employee's office without a warrant was "reasonable," but the installation of a video camera without a warrant did not amount to an investigation of work-related employee misconduct and thus violated the employee's privacy interests).

[48] *See McGregor v. Greer*, 748 F. Supp. 881, 888-89 (D.D.C. 1990). In *McGregor*, the court refused to dismiss a complaint asserting a Fourth Amendment violation whereby the plaintiff's public employer conducted a warrantless search of the plaintiff's office, during which the plaintiff alleged that her employer read every word of her private letters and records. Plaintiff disputed employer's assertion that the search was for a noninvestigatory, work-related purpose and that it was reasonable in scope. *But see Williams v. Philadelphia Hous. Auth.*, 826 F. Supp. 952, 954 (E.D. Pa. 1993) (court denied plaintiff's motion to amend complaint with Fourth Amendment claim, which asserted that plaintiff's employer removed a computer disk containing personal and business items from plaintiff's desk, stating that plaintiff failed to allege that the search was unreasonable at its inception or was associated with misconduct).

[49] *Ortega*, 480 U.S. at 717. *See also Schowengerdt v. United States*, 944 F.2d 483, 488 (9th Cir. 1991) (employee had no reasonable expectation of privacy in office desk and credenza when frequent and random searches of work spaces was customary); *American Postal Workers Union v. United States Postal Serv.*, 871 F.2d 556, 560 (6th Cir. 1989) (employees did not have a reasonable expectation of privacy in lockers due to the signing of a "notice and waiver provision" regarding locker inspections); *Bohach*, 932 F. Supp. at 1234-35 (police officers did not have a reasonable expectation of privacy in messages sent to one another over the police department's paging system upon notification that all messages would be "logged on the network").

[50] *Yin v. California*, 95 F.3d 864, 872 (9th Cir. 1996), *cert. denied*, 117 S. Ct. 955 (1996).

[51] *Katz*, 389 U.S. at 351.

[52] *Chryst*, 793 P.2d 538, 542 (Alaska App. 1990).

[53] *Id.*

[54] *Chapman*, 679 P.2d 62, 71 (Cal. 1984).

[55] *Id.* at 68-69.

[56] *State v. Butterworth*, 737 P.2d 1297 (Wash. App. 1987) (court held criminal defendant had a

constitutionally protected right of privacy in his unpublished telephone listing). *But see State v. Smith*, 367 N.W.2d 497, 505 (Minn. 1985) ("any constitutional right that a person has to informational privacy clearly does not extend to his address"); *Tobin v. Michigan Civil Serv. Comm'n*, 331 N.W.2d 184 (Mich. 1982) (labor organizations requested names and addresses of civil service employees and the court held that plaintiff civil service employees had no right to privacy in their names and addresses under either state or federal constitutions); *Faydo*, 846 P.2d at 540-41 (Wash. App. 1993) (court distinguished *Butterworth* by holding that a detective did not violate a criminal defendant's state constitutional rights by obtaining the defendant's name from the telephone company because the defendant's telephone listing was not unpublished).

[57] *Jacobsen*, 466 U.S. at 117.

[58] *United States v. White*, 401 U.S. 745, 749 (1971).

[59] It is interesting to note that the fear articulated by the *Chapman* court regarding the ability of a law enforcement agency to form a "virtual biography" of an individual based upon information supplied by a telephone utility seems to closely parallel the facts of *McVeigh*.

[60] 783 F. Supp. 258, 263 (E.D. Va. 1992).

[61] 782 F.2d 146, 150 (10th Cir. 1986).

[62] *Id.* at 147-49.

[63] *Paul v. Davis*, 424 U.S. 693, 713 (1976).

[64] *Id.*

[65] *See Bowers v. Hardwick*, 478 U.S. 186 (1986).

[66] 429 U.S. 589, 599 (1977).

[67] *See Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425, 458 (1977). In *Nixon*, the Court balanced the intrusion into the former President's privacy against the public interest in subjecting the Presidential materials to archival screening pursuant to the Presidential Recordings and Materials Preservation Act. Several of the various circuit courts have also articulated their own balancing tests. *See, e.g., Fraternal Order of Police v. City of Philadelphia*, 812 F.2d 105, 110 (3d Cir. 1987).

[68] It is interesting to note that the opinion rendered by the District Court of D.C. in the McVeigh incident, concerning the enjoining of his discharge, did not allude to any assertion by McVeigh of his

right to privacy. Perhaps plaintiff's counsel was influenced by the decision in *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989), in which the Court stated that certain government employees may have a diminished expectation of privacy for activities that bare on their "fitness and probity." *Id*. at 672. Most notable among the provisions within the congressional policy concerning homosexuality in the armed forces, *see supra* note 37, is one that states that the presence of homosexuals in the armed services is inimical to the "morale, good order, and discipline, and unit cohesion that are the essence of military capability." Thus, a consideration of the holdings of *Von Raab* & *Bowers*, 478 U.S. at 190 (privacy protection not extended to homosexual acts), in light of congressional policy, may have been influential upon counsels' pleadings. Alternatively, the complaint filed in *McVeigh* sought injunctive relief as opposed to compensatory damages. Thus, the privacy issue may still be litigated.

[69] *White*, 401 U.S. at 756 (Douglas, J., dissenting).

[70] *Id.*

[71] The privileged access component is interjected so that the information would not be considered "public."

[72] An example of the factors used by a court in determining whether or not an invasion of privacy has occurred in a workplace context can be found in *Doe v. Southeastern Pennsylvania Transp. Auth.*, 72 F.3d 1133, 1140 (3d Cir. 1995), *cert. denied*, 117 S.Ct. 51 (1996). The *Doe* court made use of factors originally formulated in *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 578 (3d Cir. 1980). The court, when considering an employee's right to privacy in medical records, articulated the following factors: (1) the type of record requested; (2) the information contained; (3) the potential harm of any subsequent nonconsensual disclosure; (4) injuries from disclosure; (5) adequacy of safeguards to prevent unauthorized disclosure; (6) the need for access; (7) the existence of a statutory mandate, public policy or other public interest favoring access.

[73] "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs to concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS, § 652B (1977).

It is also possible that an aggrieved plaintiff may be able to initiate a cause of action for a violation of a state's constitutional or statutory recognition of a right to privacy. For a synopsis of states that recognize such a right, *see* Gantt, *supra* note 14, at 389-90. The recognition of such a right most often is limited to governmental employees. *See, e.g., Luedtke v. Nabors Alaska Drilling, Inc.*, 768 P.2d 1123, 1130 (Alaska 1989). However, the courts of at least one state have said that the state's constitutional privacy initiative creates a right of action against both private and government entities. *See Hill v. National Collegiate Athletic Ass'n*, 865 P.2d 633, 644 (Cal. 1994). A discussion and analysis of each individual state's constitutional or statutory privacy guarantees, however, is beyond the scope of this article.

[74] *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 100-01 (E.D. Pa. 1996).

[75] *Saldana v. Kelsey-Hayes*, 443 N.W.2d 382, 384 (Mich. App. 1989).

[76] *Hill*, 865 P.2d at 648.

[77] *See, e.g., Robyn v. Phillips Petroleum Co.*, 774 F. Supp. 587, 592 (D. Colo. 1991).

[78] *Policemans' Benevolent Ass'n of New Jersey v. Township of Washington*, 850 F.2d 133, 141 (1988).

[79] *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 628 (1989).

[80] *See Von Raab*, 489 U.S. at 672.

[81] *See supra* note 49 and accompanying text.

[82] *Hennessey v. Coastal Eagle Point Oil Co.*, 609 A.2d 11 (N.J. 1992). In *Hennessey*, the court stated that "'a clear mandate of public policy' must be one that on balance is beneficial to the public." *Id*. at 20. To "ascertain[] whether an employee's individual rights constitute a 'clear mandate of public,' . . . [the court] must balance the public interest against the employee's right." *Id*. at 21.

[83] *Phillips v. Smalley Maintenance Servs., Inc.*, 711 F.2d 1524, 1536 (11th Cir. 1983); *Kelley v. Troy State Univ.*, 923 F. Supp. 1494, 1502 (M.D. Ala. 1996). *Accord Van Jelgerhuis v. Mercury Fin. Co.*, 940 F. Supp. 1344, 1368 (S.D. Ind. 1996). *But see Thompson v. City of Arlington*, 838 F. Supp. 1137, 1155 (N.D. Tex. 1993) (an "injury" for the tort of intrusion upon seclusion occurs only "where there has been a physical invasion of a person's property or eavesdropping on another's conversation").

[84] *Vernars v. Young*, 539 F.2d 966, 969 (3d Cir. 1976).

[85] *Slack v. Kanawha County Hous.*, 423 S.E.2d 547, 550-54 (W. Va. 1992).

[86] *Alexander v. F.B.I.*, 971 F. Supp. 603, 609 (D.D.C. 1997).

[87] *Doe v. Kohn Nast & Graf, P.C.*, 862 F. Supp. 1310, 1326 (E.D. Pa. 1994) (citing *Borse v. Piece Goods Shop, Inc.*, 963 F.2d 661, 621 (3d Cir. 1992)).

[88] *Smith v. Colorado Interstate Gas Co.*, 777 F. Supp. 854, 857 (D. Colo. 1991).

[89] *Smyth*, 914 F. Supp. at 101.

[90] *Saldana*, 443 N.W.2d at 384.

[91] *Hanson v. Hancock County Mem'l Hosp.*, 938 F. Supp. 1419, 1437 (N.D. Iowa 1996).

[92] *Robyn*, 774 F. Supp. at 592.

[93] A court would most certainly also look towards Congress' "codification" of its attitude towards homosexuals in military service. *See supra* note 37.

[94] As previously indicated, it is interesting to note that *McVeigh* contained no assertion of the sailor's constitutional or common law right to privacy.

[95] *See, e.g., Hennessey*, 609 A.2d at 19-21 ("the public's interest in ensuring that workers in safety-sensitive positions are drug free outweighs any individual right to privacy").

[96] *See Smyth*, 914 F. Supp. at 100-01; *Williams*, 826 F. Supp. at 954; *Bohach*, 932 F. Supp. at 1234; *See also Comeau v. Brown & Williamson Tobacco Co.*, 915 F.2d 1264, 1275 (9th Cir. 1990) (the court held it was not "unreasonably intrusive" for a an employer to obtain unauthorized credit reports concerning an individual subsequent to extending an offer of employment despite the obtainment of the reports from a third party's computerized data banks); *Bourke v. Nissan Motor Corp.*, No. B068705, (Cal. App. July 26, 1993) (employees had no reasonable expectation of privacy in e-mail due to company policy which restricted use of computer equipment to company business); *United States v. Maxwell*, 45 M.J. 406 (C.M.A. 1996). In *Maxwell*, the F.B.I. procured a warrant to search records and files, at AOL's computer center, for an Air Force officer's e-mail, and the officer challenged the warrant as being infirm due to, among other contentions, the misspelling of his screen name on the warrant. The court held that the officer had a reasonable expectation of privacy in his e-mail, however, it refused to invalidate the warrant. The value of the court's holding as precedent is suspect, however, when viewed in the context of the courts' other statements, namely that "there is the risk that an employee or other person with . . . access to the network service will access the e-mail, despite any company promises to the contrary. One always bears the risk that a recipient of an e-mail message will redistribute the e-mail or an employee . . . will read e-mail against company policy." *Id*. at 418.

[97] *A Framework for Global Electronic Commerce*, report released by President William J. Clinton on July 1, 1997, at 1. The report is accessible via the Internet site of the National Information Infrastructure Task Force at <http://www.iitf.nist.gov>.

[98] Blane Erwin, *et al.*, *Sizing Intercompany Commerce*, FORRESTER RESEARCH, July 23, 1997.

[99] *A Framework for Global Electronic Commerce*, *supra* note 97, at 2.

[100] Heather Green, *et al.*, *A Little Privacy, Please*, BUS. WK., Mar. 16, 1998, pp. 98-100.

[101] *A Framework for Global Electronic Commerce*, *supra* note 97, p. 10.

[102] *Id.* at 11.

[103] *Id.*

[104] Laurie Thomas Lee, *Watch Your E-Mail! Employee E-Mail Monitoring And Privacy Law In The Age Of The "Electronic Sweatshop,"* 28 J. MARSHALL L. REV. 139, at 175 n.2 (1994). Survey results were reported in the July, 1993 issue of the magazine.

[105] *Id.*

[106] *Id.* at 139.

[107] A 1990 study of 186 New York metropolitan area companies found that nearly forty percent were engaged in some type of electronic surveillance of their employees. *Id.* at 144 n.26. And a 1991 study by the Society for Human Resource Management found that twenty-four percent of respondent members used either video cameras, computer terminals, or telephone taps to monitor employees. *Id.*

[108] BLACK'S LAW DICTIONARY 930 (5th ed. 1979).

[109] *Id.* at 930-31.

[110] 18 U.S.C. § 2703(c)(1)(B)-(C).

[111] *McVeigh*, 983 F. Supp. at 220. *See also supra* note 24, and accompanying text.

[112] This recommendation could potentially be problematic. The constitutional basis of the ECPA is the Commerce Clause. U.S. CONST. art. I, § 8, cl. 3. When employing the Commerce Clause to uphold legislative enactments, the Supreme Court has stated that "Congressional power over areas of private endeavor . . . has been held limited only by the requirement that the means chosen by Congress must be reasonably adapted to the end permitted by the Constitution." *Hodel v. Virginia Surface Mining & Reclamation Ass'n, Inc.*, 452 U.S. 264, 286 (1981). For private employers that make available to their employees an Internet connection via an ISP, it may suffice that the ISP engages in interstate commerce. However, a constitutional challenge could arise in the case of a private employer that does not use an ISP, but instead provides its own Internet gateway. Alternatively, an employer in the latter case that conducts business with out-of-state customers may be reachable via Commerce Clause legislation. *See Heart of Atlanta Motel, Inc. v. United States*, 379 U.S. 241, 255-58 (1964).

[113] *See Ortega*, 480 U.S. at 723.

[114] Samuel D. Warren & Louis D. Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193, 196 (1890).