Employees' Rights to Privacy

by Lisa Mann
02-01-2000
Employers' Need to Know: Employees' Rights to Privacy
by
Lisa Mann
Modrall, Sperling, Roehl, Harris & Sisk, P.A.
February, 2000

Increasingly, employers are discovering that they need to know facts about their employees which may not be immediately apparent in the workplace -- facts about their employees or prospective employees' credit and prior histories, facts about their employees' conduct in the workplace during "personal" or "break" time, facts about their employees' use of e-mail or Internet, facts about their employees' off-duty conduct, and facts about their employees' medical conditions. Inquiry into these facts too often gives rise to claims of invasion of privacy by the employee. Depending on the context of the inquiry, employers may need to balance the legitimacy of their need to know against the employees' rights of privacy.

I. Background Investigations

Many employers wish to perform background investigations on prospective or current employees. New Mexico law allows employers to hire credit bureaus to provide limited information to non-credit-granting governmental agencies, including names, addresses, former addresses, places of employment and former employment (§ 56-3-3 NMSA 1978). This information, while limited, can be used to evaluate the truthfulness of representations made by present or prospective employees. Other information, such as information about bankruptcies, accounts placed for collection, suits and judgments, paid tax liens, arrests and indictments pending trial, and conviction of crimes, may only be obtained by public employers conducting investigations for security purposes.

In addition, employers should also be aware of recent amendments to the federal Fair Credit Reporting Act, which severely limit an employer's ability to obtain information about employees and prospective employees without obtaining those employees' prior consent. The Consumer Credit Reporting Reform Act became effective September 30, 1997, and requires employers (both public and private) to make full disclosure to employees and prospective employees whenever a report is obtained, and to obtain the employees' consent before obtaining such a report.[(1)] Furthermore, if an employer denies employment or takes any other adverse action against an employee or prospective employee based on information in the credit report, the employer has to provide the employee with a copy of the credit report and a written description of the employee's rights under the Fair Credit Reporting Act, as well as other disclosures. Previously, employers were not required to comply with the Act with respect to employees earning annual salaries of $20,000 or more. Now, the exemption only applies to employees earning $75,000 or more. Therefore, the new amendments will apply to a far greater number of employees.

Employers must carefully consider their options if they wish to conduct background investigations of current or prospective employees. Violations of the federal laws

may result in civil and criminal penalties. On the other hand, these laws do not preclude employers from relying on the information obtained from properly conducted background investigations. And the laws are silent about whether employers may decline to employ prospective employees who refuse to allow properly limited background investigations. These and other areas are still awaiting court challenges and employers are advised to be careful in their utilization of background investigations pending further clarification of the law.

As part of their investigation of prospective employees, most employers check references from former employers. A recent decision from the New Mexico Court of Appeals has made clear, however, that a former employer may face liability for providing an unqualifiedly positive reference for a former employee, when that employer is aware of information that creates a substantial, foreseeable risk of physical harm to third parties by the employee.[2] In that case, a patient at a psychiatric hospital brought a claim of negligent misrepresentation against Dona Ana County, claiming that her injuries from sexual and physical abuse by a former detention sergeant hired by the hospital resulted from the hospital's reliance on an unqualifiedly favorable reference provided by Dona Ana County law enforcement officers. The Court of Appeals held that when the county law enforcement officers undertook to provide an employment reference, they owed a duty not to make negligent misrepresentations to the subsequent employer, and that this duty extended to the patient, if a substantial risk of physical harm to a third person was foreseeable. Essentially, the Court of Appeals made clear that when a prior employer elects not to remain silent, and provides a reference, the employer has a duty not to misrepresent the true facts about the former employee. The Court noted, however, that a former employer is not required to provide references at all; it is only when the employer elects to provide a reference that its duty not to misrepresent the facts becomes applicable.

Medical Examinations

Mandatory physical examinations have been subject to privacy challenges. Public employers are, of course, aware of the Americans With Disabilities Act's restrictions on requiring physical examinations. In addition, however, employers should be cautious about the scope of required physical examinations, as overly broad physical examinations may give rise to privacy concerns on the part of employees. In one recent case, for example, employees of a research facility operated by state and federal agencies successfully challenged the facility's policy testing employees' blood samples for syphilis, pregnancy, and sickle cell anemia traits.[3] The blood samples were obtained pursuant to the employer's policy of conducting pre-placement examinations and periodic health examinations, but the employees were not notified that the samples would be tested for these intimate medical conditions. The court of appeals found that this testing could well have violated the employees' rights to be free from unlawful search under the Fourth Amendment of the United States Constitution, and as well as their due process rights to privacy., and reversed a grant of summary judgment in favor of the employer. With respect to the tests for syphilis and pregnancy, the court noted "that the Constitution prohibits unregulated, unrestrained employer inquiries into personal sexual matters that have no bearing on job performance."[4] The court also upheld the employees' claims of discrimination under Title VII, noting that the pregnancy tests were administered only to female employees, and the sickle cell anemia tests were administered only to black employees. The court noted, however, that these tests might well be upheld if the

employees had authorized the testing, or if the employees reasonably should have known that the blood and urine samples they provided would be used for the testing and failed to object.[5]

Interestingly, these same tests passed scrutiny under the ADA challenge. The court noted that employment entrance examinations need not be concerned solely with the individual's ability to perform job-related functions, and the ADA does not require such examinations to be "job-related or consistent with business necessity." Accordingly, because the ADA did not limit the scope of medical examinations, the court upheld dismissal of the employees' claims under the ADA.[6]

In an earlier case, the same circuit court of appeals upheld a public employer's right to request an employee to submit to an independent medical examination (IME).[7] The employee had a history of greatly excessive absences, a record of on-the-job illnesses, and had refused to provide medical records to the public employer. She then refused the employer's request that she submit to an IME, and brought suit, claiming that such a request violated her rights under the ADA and her right to privacy under the Fourth Amendment. The court rejected both claims. As to the ADA claim, the court noted that "when health problems have had a substantial and injurious impact on an employee's job performance, the employer can require the employee to undergo a physical examination designed to determine his or her ability to work[.]"[8] With respect to the constitutional claim for invasion of privacy, the court acknowledged that the employee had a societally-recognized expectation of privacy in not being subjected to a medical examination, but found several factors present that diminished that expectation of privacy: California had a state statute permitting medical testing of public employees, the employee was subject to a union contract which incorporated that statute, and the employee had "a record of extended and egregious absenteeism."[9] When that diminished privacy interest was balanced against the employer's valid concern with the productivity and stability of its work force, the court found the employer's request that the employee submit to an IME to be reasonable, and therefore constitutional.[10]

In summary, employers should be careful about subjecting employees to physical examinations, ensuring that these examinations are necessary to ascertain the employees' fitness for duty, and are no more intrusive than necessary to accomplish that goal. Prior disclosure of the scope of, and reasons for the examination is likely to go a long way in eliminating privacy challenges to such examinations.

Drug Testing

Drug and alcohol testing has been the subject of many recent court challenges by employees claiming that such testing violates their rights of privacy. Some challenges focus on the fact of testing, and others on the manner of testing.

Challenges to drug testing are less likely to be successful when the employer's designation of a position as "safety-sensitive," and therefore subject to random, or suspicionless, drug testing, is carefully thought-out and well-based. Conversely, such challenges are likely to prevail when the employer fails to think through its designation of positions as subject to random drug testing. For example, in one case, a City of Albuquerque employee was fired from his position as a heavy truck driver when he had a positive drug test which was administered on his first day back from medical leave.[11] The Tenth Circuit Court of Appeals found the City's testing of the

employee to be an unreasonable search in violation of the Fourth Amendment, because the provisions of the City's substance abuse policy did not apply to the employee and could not have alerted him to the possibility that he would be required to undergo drug testing, and the employee was not told that he would be subjected to drug testing as a condition of employment when he returned to work.[12] The court noted that before his medical leave, the employee had been a bus driver; following his medical leave he was not moving to a more safety-sensitive position. Accordingly, the court found that this sort of "unwarned testing" was "the most intrusive possible, contravening all of one's reasonable expectations of privacy."[13]

The same conclusion was initially reached by a different appellate court in reversing the dismissal of a lawsuit brought by an elementary school custodian, after he was subjected to a random urinalysis drug screening and given the option of termination or enrollment in a substance abuse program.[14] The court focused on the fact that the custodian had never been informed that his position was designated as "safety-sensitive," and that the district's drug policy did not delineate which positions were considered "safety-sensitive."[15] However, when the same case came back to a different panel of the same court two years later with a more fully developed record, the court reached the opposite conclusion.[16] The court relied on evidence that the employee had notice that his position as a custodian was specifically designated as safety sensitive and that he would be subjected to random testing. Accordingly, the court held that the school board's need to conduct suspicionless searches pursuant to its drug testing policy outweighed the privacy interests of employees in an elementary school who interact regularly with students, use hazardous substances, operate potentially dangerous equipment, or otherwise pose any threat or danger to students.[17]

The upshot of this analysis is that employers must consider carefully why they are designating certain positions as "safety-sensitive," to make sure that these reasons are documented in advance of implementation of random drug testing, and to make sure that drug testing policies are well-publicized and explained to employees. If employers follow these precautions, drug testing policies are more likely to be upheld.

Methods of drug testing have also been challenged in the courts on privacy grounds. In one case from Kansas, for example, a nurse in a private hospital challenged a drug screening program which required her to provide urine samples while under observation by her supervisor.[18] The court dismissed the nurse's ADA and invasion of privacy claims, finding she had signed a form consenting to drug testing when she first became employed, and she had acknowledged her addiction to Demerol and was participating a drug treatment program which included periodic monitored drug testing as a prerequisite to her resumption of nursing duties. Accordingly, while the court sympathized with the embarrassing situation in which the employee found herself, her claims under the ADA and for invasion of privacy were not valid.[19]

An appellate court reached a slightly different conclusion in a challenge by firefighters to a city drug testing policy that required them to give urine specimens under the direct supervision of a monitor furnished by the testing laboratory.[20] The court agreed with the lower court that direct observation of drug testing was not an unreasonable search and seizure, reasoning that firefighters had only a diminished expectation of privacy because they were in a highly regulated industry and because they had consented to random drug testing in their collective bargaining agreement.

The court also emphasized that the safety concerns associated with this type of employment are well-known to prospective employees and also serve to diminish an employee's expectation of privacy.[21] Moreover, the court also found that the direct observation method was a legitimate means to serve the city's interest in preventing cheating on drug tests.[22] While this analysis was sufficient to dispose of the constitutional claims, it did not necessarily dispose of the invasion of privacy claims under state law, since the "reasonableness" standard applicable to constitutional claims was not necessarily identical to the "reasonable person" standard applied to common law claims of invasion of privacy.[23] Employers should be wary of insisting on observed drug testing, since such obvious intrusions on employees' privacy are more likely to lead to litigation than are other methods. If an employer has specific reasons for insisting on monitored drug testing, however, those reasons should be clearly communicated to employees, and uniformly applied to minimize the risks associated with such testing.

Finally, employees who refuse to take drug tests may bring court challenges following their subsequent terminations. Where these challenges have been based on the employees' privacy rights, they have generally been unsuccessful. In one case, for example, a private employer requested an employee to undergo a drug test after it had received several reports of that employee's use of marijuana both on and off the job.[24] The employee complied with that request, but the employer subsequently obtained information suggesting that the employee had tampered with the specimen originally provided. When the employer asked the employee to undergo another drug test, he refused, and was fired. The employee sued, claiming that the employer's request that he undergo another drug test was an unwarranted invasion of privacy. The court rejected that argument, reasoning that the employer's legitimate interest in determining whether the employee had tampered with the first sample provided it with sufficient reason to request a second sample, and nothing in that second request could be construed as "highly offensive" to an ordinary reasonable person.[25] Similarly, in another recent case, the court dismissed claims brought by a former school employee who contended that the school board's demand that he submit to a drug test, enter an employee assistance program, or resign his employment violated his constitutional right to privacy.[26] The employee had never submitted to a drug test, and the court concluded that there was no interpretation of the Fourth Amendment that would make the employee's claims viable on those facts.[27]

It is obvious from these cases that drug testing by employers is frequently the subject of litigation. Well thought-out drug testing policies, advance notice to employees of those drug testing policies and the intent to enforce those policies, and uniform enforcement of those policies may not completely protect employers against such litigation, but it will assist in obtaining a favorable result if such litigation is brought.

Workplace Searches

Another fertile area for employee litigation on privacy grounds arises in the context of workplace searches by employers. The availability of sophisticated technology for those searches may make these challenges even more potent. In virtually all of these cases, however, the presence or absence of advance warning to employees is dispositive.

In one case, for example, police officers challenged the police department's practice of installing surveillance cameras and tape recorders in police vehicles, claiming that such equipment constituted an unwarranted invasion of privacy rights.[28] The court rejected these claims, reasoning that police officers did not have a reasonable expectation of privacy while on duty in a patrol car, especially since the police officers knew that the surveillance equipment was installed in their vehicles.[29] In another case, employees of a quasi-public telephone company challenged the videotaping of their workplace.[30] The appellate court upheld the dismissal of their constitutional privacy claims, reasoning that employers possess a legitimate interest in the efficient operation of the workplace, and supervisors could legitimately monitor the employees' actions in that workplace. The legitimacy of such monitoring did not depend on the technology used to achieve it, particularly when the employer had notified its work force that video cameras would be installed and told the employees about the cameras' field of vision.[31] Because the employees had no objectively reasonable expectation of privacy against disclosed video surveillance while at work, they had no claim under the Fourth Amendment.[32]

If the employer chooses to utilize audio surveillance methods, however, the employer must be careful not to run afoul of federal law prohibiting wiretapping. In one recent case, for example, the private employer, Wal-Mart Stores, used hidden voice-activated recording devices to tape employees' private conversations.[33] Four former employees whose conversations were recorded sued Wal-Mart under the omnibus Crime Control and Safe Streets Act of 1968, which allows any person whose "wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of [the Act]" to "recover from the person which engaged in that violation such relief as may be appropriate."[34] Appropriate relief under the federal Act includes actual damages or statutory damages of $100 a day for each day of violation or $10,000, whichever is greater, punitive damages if warranted, and reasonable attorneys' fees and costs. The jury awarded each of the employees $20,000, and the judge awarded attorneys' fees and costs. On appeal, the court of appeals reduced the awards to the $10,000 statutory minimum amount, but affirmed the award of attorneys' fees and costs against Wal-Mart, even though the plaintiffs had failed to prevail on their claims for constructive discharge and punitive damages.[35]

Similarly, in another case, two teachers invoked the same federal law when they successfully sued a high school principal who had tape recorded their telephone conversations for a three-month period after he learned of their plans to orchestrate the principal's termination.[36] The court rejected defendant's argument that because the communications occurred over the school's telephone system, the teachers could have no legitimate expectation of privacy in those conversations, reasoning that the federal Act protected "wire communications" "against interception by electronic, mechanical, and other devices regardless of the speaker's expectation of privacy."[37]

In another recent case, a former Acting Assistant Secretary of State sued various State Department officials and employees who allegedly monitored his telephone conversations when he was investigating President Clinton's passport files.[38] The State Department Operations Center telephone console provided State Department officers with the ability to monitor all telephone calls placed through the Operations Center, and the plaintiff's telephone calls were apparently monitored in that fashion. The defendants claimed that the Operations Center functioned as a switchboard operator, entitled to an exception under the federal Act.[39] The court of appeals

rejected that argument, reasoning that "the switchboard operator, performing only the switchboard function, is never authorized simply to monitor calls."[40] The court also rejected defendants' argument that the employee had provided implied consent to telephone monitoring because he was never told that the operators had left the line after placing the calls, pointing to the lack of evidence that the plaintiff had ever been told that specific conversations would be monitored, and the circumstances of the telephone calls did not suggest that the conversations would be monitored.[41] Because the court could not say that the plaintiff's claims were without merit, as a matter of law, the court allowed the case to proceed to trial.[42]

Challenges to physical searches of employee offices have yielded mixed results. In one case, an state child protective investigator brought a constitutional challenge as a result of a warrantless search of her office following an anonymous tip that she kept child pornography in her file cabinet.[43] The appellate court upheld the dismissal of her constitutional claims, finding that the search a reasonable in scope and justified as a workplace search, despite the fact that the employee kept her file cabinets locked, no one except her had the keys to the file cabinet, and the search was conducted for evidence in her desk, storage unit and filing cabinet. Because the court found that the search was prompted by serious allegations of specific misconduct against an employee in a sensitive position, prompt attention was called for, and the targets of the search were places where the employee would likely store the pornographic pictures the employer had reason to believe she had. Accordingly, the search was an objectively reasonable workplace search.[44]

In other cases, however, searches of public employees' offices were found to have violated the employees' constitutional rights to privacy. A doctor employed at a state hospital successfully claimed that the hospital administrators' search of his private office and seizure of personal items from the office for several months constituted an unlawful invasion of his privacy.[45] The hospital sought to investigate the doctor's management practices; to that end, the doctor was placed on administrative leave, the lock to his private office was changed, and the hospital undertook a series of searches of his office, his desk, and his private file cabinets. Investigators examined, read, and seized numerous personal letters, lecture notes and teaching aids, framed artwork, personal photographs, copies of published and unpublished articles, rejection letters from medical journals, a manuscript for a new book, and confidential medical files of patients not connected with the hospital. The doctor was ultimately fired, and filed suit, claiming that the searches of his office violated his constitutional rights. The jury awarded the doctor more than $400,000, and the verdict was sustained on appeal. The court noted that the search itself was far broader than necessary to accomplish the announced purpose of the investigation: "it has long been apparent that stale and unsubstantiated allegations do not entitle supervisors to rummage through employees' desks and file cabinets without a reasonable belief that specific evidence of misconduct will be found, let alone scrutinize romantic letters or mementos they may happen to locate."[46]

While that case involved fairly egregious conduct by the public employer in disregarding the employee's right to privacy, another case presented a closer issue. An employee who served as town clerk and town tax collector brought constitutional claims after the town placed a police guard in her office to watch over her on her last day of service.[47] The employee had lost her bid for re-election and, by state law, was required to have an audit of accounts promptly made following the election. She made arrangements for the audit, and told the auditor she planned to take the books

and records home with her over the weekend to prepare for the audit. The auditor informed a member of the town council of her plans, and the council voted to have the police chief take action to prevent the employee from removing the town's books and records from the town hall. A police officer entered the employee's office on her last day of work and remained there while she worked. When she finished, he escorted her to the vault, where she deposited the records, and then out of the town hall. The court found that the police officer's random and undirected trespass constituted an unreasonable search of what had been maintained as a private office. Moreover, although the court acknowledged that workplace efficiency might justify an immediate warrantless search by the employee's supervisor, there was no reason to deploy a police officer, "whose invasion of the private office is inherently more intrusive than an equally effective search by the employee's supervisor."[48] Accordingly, the warrantless search of the employee's office violated her Fourth Amendment rights.[49] The court refused, however, to find a constitutional violation in the police officer's "seizure" of the records, because it found legitimate the town's interest in protecting its administrative records.[50]

Employers' monitoring of employees' use of electronic mails (or "e-mails") and the Internet has also been challenged on grounds of unreasonable search and seizure. In one recent case, an employee of a branch of the CIA was charged with receiving and possession materials containing child pornography, as a result of a routine search of employees' use of the Internet and electronic mail.[51] A systems operations manager responsible for managing the computer network had been examining use of the system to determine its capabilities. When he discovered extensive use of pornographic Internet web sites, he traced the activity in those web sites to the defendant's work station and discovered that over one thousand files containing pictures had been downloaded at that work station. After reporting his discovery to his supervisors, the systems manager copied the contents of the hard drive in defendant's computer, which revealed several files depicting child pornography. The defendant challenged the "seizure" of the computer files, contending they were conducted without a search warrant. The court rejected that argument, finding that employees had no reasonable expectation of privacy with regard to Internet use, because the employer had a policy notifying employees that Internet access was limited to business use, and such use would be monitored.[52] Accordingly, the employer's monitoring of defendant's computer use did not constitute an unreasonable search.

In another case, however, the court found that Navy violated an officer's rights when it conducted an investigation based on an anonymous e-mail that came into the hands of another Navy officer's wife.[53] After she forwarded the e-mail to her husband, he contacted the Internet service provider and ascertained the identify of the Navy officer, who was then administratively discharged for homosexual conduct. The court found that the discharge violated the Navy's own "don't ask, don't tell" regulations. Moreover, the court noted that the Navy also probably violated the Electronic Communications Privacy Act of 1986 when it informally contacted the Internet service provider without a warrant to ascertain the officer's identity.[54] Accordingly, the court issued an injunction, preventing the officer's discharge pending trial.[55]

These cases suggest that employers should be careful in authorizing searches of employees' offices computers, and personal belongings. Such searches should be narrowly tailored to serve legitimate interests of the employer, and should be

focused only on areas where it is likely that the materials sought are likely to be found.

Inquiries into Off-Duty Conduct

Employers often feel the need to inquire into employees' off-duty conduct in the context of sexual harassment investigations. Those inquiries are usually upheld by the courts, as long as the employer has not investigated matters unrelated to the sexual harassment claims. In one case, for example, the court dismissed allegations against a city arising from the investigation of a police officer accused of sexual harassment, finding no violation of the officer's constitutional rights to privacy.(56) The police officer was accused of sexual harassment against co-workers, and the police lieutenant responsible for the investigation interviewed the officer and, on a separate occasion, the police officer's wife, to ascertain whether the police officer's prior statements were truthful. The investigator also interviewed co-workers to determine if they had any relevant information about the allegations. The court found the investigation reasonable, in light of the accusations against the police officer and the department's duty to investigate claims of sexual misconduct on the job.(57)

In another case, a former federal employee sued the United States Treasury for violating the federal Privacy Act when it reviewed the employee's personnel file and interviewed his supervisor in an effort to ascertain the facts regarding the employee's romantic relationship with a subordinate employee.(58) The court found no Privacy Act violation, because the employer's staff clearly needed to know the information, the employee had to be identified in order to investigate his job-related misconduct, the employee admitted that he had discussed the details of his termination and relationship with several of his co-workers, and that he had suffered no adverse effect from any disclosures.(59)

CONCLUSION

Employers are well-advised to keep their employees' privacy interests in mind when conducting inquiries into employees' conduct. If employers make their legitimate interests known to employees in advance, and announce specifically the measures they intend to take to effectuate those interests, employers may be able to reduce employees' expectations of privacy in the workplace, thereby protecting employers against accusations of invasion of privacy by the employees.

1. 15 U.S.C. § 1681a(o)(5), § 1681b(2) (1997).

2. Davis v. Bd. of County Commissioners, 1999-NMCA-110, 987 P.2d 1172 (Ct. App. 1999).

3. Norman-Bloodsaw v. Lawrence Berkeley Laboratory, 135 F.3d 1260 (9th Cir. 1998).

4. Id., 135 F.3d at 1269.

5. Id., 135 F.2d at 1270.

6. Id., 135 F.3d at 1273.

7. Yin v. State of California, 95 F.3d 864 (9th Cir. 1996).

8. Id., 95 F.3d at 868.

9. Id., 95 F.3d at 871.

10. Id., 95 F.3d at 873.

11. Rutherford v. City of Albuquerque, 77 F.3d 1258 (10th Cir. 1996).

12. Id., 77 F.3d at 1261.

13. Id., 77 F.3d at 1262.

14. Aubrey v. School Board of Lafayette Parish, 92 F.3d 316 (5th Cir. 1996).

15. Id., 92 F.3d at 319.

16. Aubrey v. School Board of Lafayette Parish, 1998 WL 416153 (5th Cir. 1998).

17. Id., 1998 WL 416153 at *4.

18. Jones v. HCA Health Services of Kansas, Inc., 1998 WL 159505 (D. Kan. 1998).

19. Id., 1998 WL 159505 at *16.

20. Wilcher v. City of Wilmington, 139 F.3d 366 (3rd Cir. 1998).

21. Id., 139 F.3d at 374.

22. Id., 139 F.3d at 378.

23. Id., 139 F.3d at 380.

24. Frye v. IBP, Inc., 1998 WL 400080 (D. Kan. 1998).

25. Id., 1998 WL 400080 at *7.

26. Cox v. McCraley, 993 F. Supp. 1452 (M.D. Fla. 1998).

27. Id., 993 F. Supp. at 1456.

28. Gross v. Taylor, 1997 WL 535872 (E.D. Pa. 1997).

29. Id., 1997 WL 535872 at *6-8.

30. Vega-Rodriguez v. Puerto Rico Telephone Co., 110 F.3d 174 (1st Cir. 1997).

31. Id., 110 F.3d at 181.

32. Id. At 182.

33. Desilets v. Wal-Mart Stores, 1999 WL 161113 (1st Cir. 1999).

34. 18 U.S.C. § 2520(a).

35. 1999 WL 161113, *6.

36. Kinsey v. Case, 162 F.3d 1173 (10th Cir. 1998), cert. denied, 1999 WL 166252 (1999).

37. Id., citing Briggs v. American Air Filter Co., 630 F.2d 414, 417 n. 4 (5th Cir. 1980) and United States v. Harpel, 493 F.2d 346, 349 (10th Cir. 1974).

38. Berry v. Funk, 146 F.3d 1003 (D.C. Cir. 1998).

39. 18 U.S.C. § 2511(2)(a)(i) provides:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire ... communication service, who facilities are used in the transmission of a wire ... communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of this service or to the protection of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

40. 146 F.3d at 1010.

41. Id., at 1011.

42. Id., at 1014.

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

44. Id., 128 F.3d at 492.

45. Ortega v. O'Connor, 146 F.3d 1149 (9th Cir. 1998).

46. Id.

47. Rossi v. Town of Pelham, 1997 WL 816160 (D.N.H. 1997).

48. Id., 1997 WL 816160 at *5.

49. Id., 1997 WL 816160 at *10.

50. Id., 1997 WL 816160 at *13.

51. United States v. Simons, 29 F.Supp.2d 324 (E.D. Va. 1998).

52. Id., at 327. The policy provided:

Audits. Electronic auditing shall be implemented within all FBIS unclassified networks that connect to the Internet or other publicly accessible networks to support identification, termination, and prosecution of unauthorized activity. These electronic audit mechanisms shall ... be capable of recording:

* Sent and received e-mail messages;

* Web sites visited, including uniform resource locator (URL) of pages retrieved;

* Date, time and user associated with each event.

...

53. McVeigh v. Cohen, 983 F.Supp. 215 (D.D.C. 1998).

54. Id. at 219-20, citing 18 U.S.C. § 2703(c)(1)(B).

55. Id., at 221-22.

56. Hughes v. City of North Olmsted, 93 F.3d 238 (6th Cir. 1996).

57. Id., 93 F.3d at 242.

58. Pippinger v. Rubin, 129 F.3d 519 (5th Cir. 1997).

59. Id., 129 F.3d at 530.