IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF KANSAS

CARLUS L. HAYNES,

Plaintiff,

vs. **Case No. 03-4209-RDR**

OFFICE OF THE ATTORNEY GENERAL PHILL KLINE, et al.,

Defendant.

MEMORANDUM AND ORDER

This is a civil action filed by a former assistant attorney general against the Kansas Attorney General and several employees of that office. Plaintiff seeks damages and injunctive relief for actions taken by members of the Attorney General's office in viewing private information contained on his work computer. He asserts that these actions constitute violations of his Fourth and Fourteenth Amendment rights as well as 18 U.S.C. § 2511. This matter is presently before the court upon plaintiff's motion for preliminary injunction.

On December 10, 2003 the court held a hearing on plaintiff's motion for temporary restraining order. The court declined to take any action at that time because the defendants had only recently learned of the motion. The court scheduled a hearing on plaintiff's preliminary injunction motion for December 16, 2003. The court heard very little evidence during the hearing.

Plaintiff offered only his own testimony. The defendants presented no evidence, other than during the cross-examination of the plaintiff. Based upon this very brief look at the issues in this case, the court is now prepared to issue findings of fact and conclusions of law.

In his motion, plaintiff seeks injunctive relief preventing the defendants from accessing, copying, reproducing, altering, or otherwise searching his private files, e-mails, or electronic communications. He further seeks an order preventing the defendants from searching the personal and private files of other Attorney General's office employees who have sent plaintiff personal and private communications or have received personal and private communications from plaintiff. Finally, he has orally requested that he be allowed to access his work computer records so he can obtain copies of some of the materials and delete some of the documents.

Findings of Fact

1. Plaintiff was employed by the Kansas Attorney General's office(AG's office) on February 7, 2003. His position was as the "Tobacco Enforcement Attorney." He had graduated from Washburn Law School in 2002 and passed the bar in December 2002.

2. Plaintiff was given an orientation at the time he was hired. The orientation included information on computer use.

He was told that his computer had two files: private and public. He was further told that he could put personal information in the private file and that no one would have access to it. He was also told he should put other documents concerning his work in the public file.

3. The computers at the AG's office display the following information for a brief period each time they are turned on:

> Computer Use Procedures
>
> Office computer use shall be in compliance with computer use procedures. Obtain full procedures from your deputy or supervisor.
>
> Computer use for non-official business is authorized only if kept to minimum duration & frequency & if it does not interfere with state business. This system shall not be used unlawfully nor for any purpose which could embarrass the user, recipient or Attorney General.
>
> There shall be no expectation of privacy in using this system; however, intentional access to another user's e-mail without permission shall be prohibited, except as authorized by computer use procedures.
>
> Despite deletion, files may remain available in storage. Personal data on the system may be subject to removal. Data may be subject to state public records and records preservation laws.
>
> User software installation is prohibited unless specifically authorized. Software may not be copied for use outside this office unless authorized.
>
> Office of the Attorney General

4. Plaintiff was aware of this policy, even though he states that he had a difficult time reading it when it flashed on the computer screen because of its short duration. He was not aware of any other written policies on computer use. He had never specifically asked for the additional policies and the

defendants had never voluntarily provided them. There was no evidence offered that the defendants had ever monitored or viewed any private documents, files or e-mails of the employees in the AG's office.

5. During his employment, plaintiff was counseled for personal use of the AG's office fax machine. He had used the fax machine to send a court document in a personal court proceeding.

6. On October 9, 2003 plaintiff was told that he could either accept a job as a special attorney general with the worker's compensation division or be terminated. Plaintiff decided not to accept the other position. On October 10th plaintiff was told that he would be terminated in two weeks.

7. On Saturday, October 11th and Sunday, October 12th, plaintiff went to his office in the AG's office and attempted to log onto his computer. He was unable to do so. He learned that other employees were able to log onto their computers. On October 13th he arrived for work prior to 8:00 a.m., and again attempted to log on to his computer. Again, he was not able to do so. However, at approximately 8:00 a.m. he was able to log onto his computer and he began to copy the files on the computer to disks that he had purchased. At 8:30 a.m., Eric Rucker, Senior Deputy Assistant Attorney General, advised him that he

could not use the computer to copy any materials. Rucker informed him that he would not debate the matter with a "third-year law student." Shortly thereafter, plaintiff's supervisor came into his office and told him that he had fifteen minutes to leave. He was again told that he could not copy any materials from the computer.

8. Following plaintiff's termination, employees of the Attorney General's office retrieved and reviewed information contained on plaintiff's computer, including personal e-mails. No evidence was presented on who viewed the materials or why they were viewed. The defendants have suggested that the materials are being retained because of possible litigation that may be filed by the plaintiff concerning his termination.

9. At some time after October 13th, plaintiff contacted an attorney about possible litigation concerning his termination. He has retained that attorney to negotiate with the AG's office. Plaintiff's counsel has written the AG's office and requested certain information about individuals employed at the AG's office from June 1, 2002 to October 31, 2003.

Conclusions of Law

1. The standards for a preliminary injunction are well-settled. The court may grant a preliminary injunction if the party seeking it shows: (1) a substantial likelihood of

prevailing on the merits; (2) irreparable harm in the absence of the injunction; (3) proof that the threatened harm outweighs any damage the injunction may cause to the party opposing it; and (4) that the injunction, if issued, will not be adverse to the public interest. See Sprint Spectrum v. State Corporation Commission, 149 F.3d 1058, 1060 (10th Cir. 1998). If the movant establishes the second, third and fourth factors, then "the first factor is relaxed to require only that the movant raise questions so serious, substantial, difficult, and doubtful as to make them a fair ground for litigation and thus for more deliberate inquiry." Longstreth v. Maynard, 961 F.2d 895, 902 (10th Cir. 1992).

2. The court shall first consider the issue of irreparable harm. Plaintiff has suggested that, without injunctive relief, he will continue to suffer emotional distress and invasion of his privacy through the actions of the defendants in violation of the Fourth Amendment. The defendants have countered that injunctive relief is not appropriate because the harm, if any, has already occurred. They point out the information on plaintiff's computer has been retrieved and viewed. They note that plaintiff apparently understood when he filed this action that these events had already occurred.

3. The court recognizes that some harm may have already

occurred. However, the court also recognizes that additional harm might occur in the future unless injunctive relief is granted. At the present time, there is nothing to prevent the defendants from further viewing of the information on the plaintiff's computer or dissemination of that material. The defendants offered no evidence concerning what they intend to do with the documents retrieved from plaintiff's computer. The release of these documents by the defendants could harm the plaintiff in such a manner that compensation by monetary damages might be inadequate. Plaintiff has made clear that the documents include very personal information, including medical records and letters concerning personal relationships. A plaintiff's harm from the denial of a preliminary injunction is irreparable if it is not fully compensable by monetary damages. Basicomputer Crop. v. Scott, 973 F.2d 507, 511 (6th Cir. 1992). Moreover, irreparable harm is generally viewed as established when a plaintiff's claim is based upon a violation of the plaintiff's constitutional rights. See, e.g., Covino v. Patrissi, 967 F.2d 73, 77 (2nd Cir. 1992) (plaintiffs may establish irreparable harm based on an alleged violation of their Fourth Amendment rights). In sum, the court finds that the plaintiff has sufficiently established irreparable harm.

3. The court next turns to the issue of balancing of the

harms. The court does not find that the defendants have established any harm in granting most of the requests made by the plaintiff. The defendants have failed to articulate any harm to them arising from injunctive relief preventing further viewing or dissemination of the documents or by allowing plaintiff access to the documents for the purpose of copying them. The defendants have suggested that they might be harmed if the plaintiff is allowed to delete information from the computer files.

4. The court believes that the balance of harms weighs in favor of the plaintiff on the issues of further review and dissemination by the defendants and in receipt of copies of the information by plaintiff. The defendant "cannot reasonably assert that it is harmed in any legally cognizable sense by being enjoined from constitutional violations." Zepeda v. U.S.I.N.S., 753 F.2d 719, 727 (9th Cir. 1983).

5. The court next considers the public interest. The court does not believe that the public interest will be harmed by granting most of the relief sought by the plaintiff. Plaintiff has suggested that his Fourth Amendment rights, his privacy rights, and perhaps the rights of the employees presently employed by the AG's office will be protected if he is granted injunctive relief concerning his computer documents. The

primary concern of the defendants seems to be the possibility that plaintiff might delete some of the documents. The defendants assert that the loss of these documents might inhibit their ability to defend themselves in any lawsuit arising from the plaintiff's termination. The court believes that the relief granted by the court will promote the public interest.

6. The court believes that the plaintiff has established the second, third, and fourth factors of the aforementioned preliminary injunction standards. Accordingly, the court finds that plaintiff need only raise questions so serious, substantial, difficult and doubtful as to make them a fair ground for litigation and thus for more deliberate inquiry.

7. The beginning point for any discussion of the law concerning public employer searches in government workplaces must begin with the plurality opinion of the United States Supreme Court in O'Connor v. Ortega, 480 U.S. 709 (1987). This opinion provides the groundwork for analyzing these types of claims, although it does not involve a search of computer files. In United States v. Angevine, 281 F.3d 1130 (10th Cir.), cert. denied, 537 U.S. 845 (2002), the Tenth Circuit considered O'Connor in the context of a search by a government employer of a computer owned by the employer and used by employees. The defendant, an Oklahoma State University professor, had been

prosecuted for possession of child pornography. He sought to suppress the pornography that had been seized from his university computer. The district court denied the motion to suppress, and the Tenth Circuit affirmed. The Court, noting the university's policy that allowed the university to audit and monitor Internet use and warned that information flowing through the university network was not confidential, determined that the defendant did not have an objectively reasonable expectation of privacy. The Court, relying heavily on O'Connor, set forth the law as follows:

> The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. To establish a Fourth Amendment violation, the defendant must prove "a legitimate expectation of privacy" in the place searched or the item seized. Rakas v. Illinois, 439 U.S. 128, 143, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978). "Determining whether a legitimate...expectation of privacy exists...involves two inquiries. First, the defendant must show a subjective expectation of privacy in the area searched, and second, that expectation must be one that society is prepared to recognize as reasonable." United States v. Anderson, 154 F.3d 1225, 1229 (10th Cir.1998) (quotation marks and citations omitted), cert. denied, 526 U.S. 1159, 119 S.Ct. 2048, 144 L.Ed.2d 215 (1999). "The ultimate question is whether one's claim to privacy from the government intrusion is reasonable in light of all the surrounding circumstances." Id. (quotation marks and citation omitted).
>
> We address employees' expectations of privacy in the workplace on a case-by-case basis. O'Connor v. Ortega, 480 U.S. 709, 718, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987). "Within the workplace context, [the Supreme Court] has recognized that employees may have

> a reasonable expectation of privacy against intrusions by police." Id. at 716, 107 S.Ct. 1492. However, "[p]ublic employees' expectations of privacy ... may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." Id. at 717, 107 S.Ct. 1492. Additional factors we consider include: "(1) the employee's relationship to the item seized; (2) whether the item was in the immediate control of the employee when it was seized; and (3) whether the employee took actions to maintain his privacy in the item." Anderson, 154 F.3d at 1232.

281 F.3d at 1133-34 (footnote omitted).

8. As noted in Angevine, the issue of employees' expectations of privacy in the workplace is fact specific and the ultimate question becomes whether the claim to privacy from government intrusion is reasonable in light of all of the surrounding circumstances. See, e.g., United States v. Slanina, 283 F.3d 670, 676 (5th Cir.) (use of passwords and locking office doors to restrict an employer's access to computer files is evidence of the employee's subjective expectation plus where employer has no policy notifying employees that computer use could be monitored, and there is no indication that the employer directs others to routinely access the employees' computers, the employees' subjective beliefs that their computer files are private may be objectively reasonable), remanded on other grounds, 537 U.S. 802 (2002); Leventhal v. Knapek, 266 F.3d 64, 73-74 (2nd Cir. 2001) (state agency employee had reasonable expectation of privacy in contents of work computer where

employee occupied private office and had exclusive use of computer, and agency did not routinely conduct searches of office computers nor had it adopted a policy against mere storage of personal files); United States v. Simons, 206 F.3d 392 (4th Cir. 2000) (CIA division's official Internet usage policy eliminated any reasonable expectation of privacy that employee might otherwise have in copied files because it allowed monitoring of "all file transfers, all websites visited, and all e-mail messages"); Muick v. Glenayre Electronics, 280 F.3d 741 (7th Cir. 2002)(employee had no reasonable expectation of privacy in laptop files where employer announced it could inspect laptops it furnished to employees and employer owned laptops).

9. After a careful review of the limited evidence presented by the parties, the court is persuaded that plaintiff has raised serious issues concerning the violation of his Fourth Amendment rights. He contends that the facts show that he had a reasonable expectation of privacy in the contents of his private information contained on his work computer. The court believes that he has successfully demonstrated a subjective expectation of privacy and has raised serious issues concerning whether this expectation of privacy is objectively reasonable. The only evidence relied upon by the defendants to suggest that

plaintiff's expectation of privacy was not objectively reasonable is the policy that was displayed each day on the employees' computers in the AG's office. The defendants point specifically to the portion of that policy that reads as follows: "There shall be no expectation of privacy in using this system." This particular statement obviously has considerable significance here. The court, however, must consider this fact in conjunction with the other information provided in the policy as well as the oral representations made by AG employees to the plaintiff. These other facts, suggest that plaintiff's expectation of privacy was objectively reasonable. In reaching this conclusion, the court notes that we have received a very limited look at the policies and procedures concerning computer use at the AG's office. The facts that we have learned include the following: employees are allowed to use their work computers for private communications; employees are told how to create "public" and "private" files; employees are advised that "intentional access to another user's e-mail without permission" is prohibited; employees are given passwords to prevent others from gaining access to their computers; and there was no evidence that any AG official had ever monitored or viewed any private files, documents or e-mails of any employee. The court does not believe this is the final

word on this issue but, at this time, the court is persuaded that plaintiff has produced sufficient evidence to raise serious issues so as to make them fair ground for litigation.

9. The defendant has not offered any evidence to justify its search of the plaintiff's documents. There was no evidence offered that the search of the documents on plaintiff's computer arose from plaintiff's prior use of the AG's office fax machine. Accordingly, the court is convinced that plaintiff has carried his burden in demonstrating entitlement to a preliminary injunction.

10. The court shall issue a preliminary injunction prohibiting the defendants from accessing, copying, reading, reproducing, altering or otherwise searching the private files, documents, e-mails or other electronic communications of plaintiff. The court shall further prohibit the defendants from communicating, disseminating or discussing any of the information obtained as a result of viewing or accessing the private files, documents, e-mails or other electronic communications of plaintiff. The court shall also direct defendants to provide plaintiff with access to his private materials so that he can determine what files, records, e-mails or other electronic communications he wants copied. The defendants shall provide copies of the files, records, e-mails,

or other electronic communications requested by plaintiff. Plaintiff shall not be allowed to delete any information contained on his work computer. The issuance of the aforementioned preliminary injunction will preserve the status quo pending a final determination of the case on the merits. Tri-State Generation and Transmission Assoc., Inc. v. Shoshone River Power, Inc., 805 F.2d 351, 355 (10th Cir. 1986).

11. The requirement of security for this preliminary injunction shall be waived because plaintiff is proceeding in forma pauperis in this action. Holmes by Holmes v. Sobol, 690 F.Supp. 154, 161-62 (W.D.N.Y. 1988).

IT IS THEREFORE ORDERED that plaintiff's motion for preliminary injunction (Doc. # 5) be hereby granted in part and denied in part.

IT IS FURTHER ORDERED that the defendants are hereby enjoined from accessing, copying, reading, reproducing, altering or otherwise searching the private files, e-mails, or other electronic communications of plaintiff.

IT IS FURTHER ORDERED that the defendants are hereby enjoined from communicating, disseminating or discussing any of the information obtained as a result of viewing or accessing the private files, documents, e-mails or other electronic communications of plaintiff.

IT IS FURTHER ORDERED that the defendant shall allow plaintiff access to his private materials so that he can determine what files, records, e-mails or other electronic communications he wants copied. The defendants shall provide copies of the files, records, e-mails, or other electronic communications requested by plaintiff. Plaintiff shall not be allowed to delete any information contained on his work computer.

IT IS SO ORDERED.

Dated this 23rd day of December, 2003 at Topeka, Kansas.

s/Richard D. Rogers
United States District Judge