

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF KANSAS

CARLUS L. HAYNES,

Plaintiff,

vs.

Case No. 03-4209-RDR

ATTORNEY GENERAL OF
KANSAS, et al.,

Defendants.

MEMORANDUM AND ORDER

This is a civil action filed by a former assistant attorney general against Phill Kline, the Kansas Attorney General, and several employees of that office: Eric Rucker, Whitney Watson, Scott Davidson and Amanda Nations. Plaintiff seeks damages for actions taken by members of the Attorney General's office in viewing private information contained on his work computer. He asserts these actions constitute violations of his Fourth and Fourteenth Amendment rights under 42 U.S.C. § 1983.¹ This matter is presently before the court upon defendants' motion for summary judgment.

I.

Plaintiff alleges he had a legitimate expectation of privacy in the information stored on his work computer, and the search of the computer by the defendants following his termination violated

¹ Plaintiff had originally also asserted a wiretap claim under 18 U.S.C. § 2511 and a state law invasion of privacy claim. He has advised the court that he is no longer pursuing these claims.

his Fourth Amendment rights. Plaintiff further contends he had a property interest in the private information stored on his work computer, and the defendants' actions in preventing him from accessing and obtaining that information after he was terminated deprived him of property without just compensation in violation of the Fourteenth Amendment.

Defendants contend they are entitled to summary judgment on plaintiff's Fourth and Fourteenth Amendment claims. They initially argue that they are entitled to summary judgment on plaintiff's Fourth Amendment claim because plaintiff has failed to establish a reasonable expectation of privacy in his computer files. They next contend that, even if plaintiff had a reasonable expectation of privacy in his computer files, they are entitled to qualified immunity because this right was not clearly established at the time of the search. Finally, the defendants assert that they are entitled to summary judgment on plaintiff's Fourteenth Amendment claim for a variety of reasons including qualified immunity.

We review the legal issues raised by defendants' motions for summary judgment considering all of the evidence in a light most favorable to the nonmoving party. Schwarz v. Brotherhood of Maintenance of Way Employees, 264 F.3d 1181, 1183 (10th Cir. 2001). Summary judgment is warranted when there is "no genuine issue as to any material fact and . . . the moving party is entitled to judgment as a matter of law." Oliver v. Woods, 209 F.3d 1179, 1184

(10th Cir. 2000).

Because qualified immunity is one of the issues raised in defendants' motions for summary judgment, it should be noted that the Tenth Circuit has set forth a different approach for summary judgment on qualified immunity issues.

When a § 1983 defendant raises the defense of qualified immunity on summary judgment, the burden shifts to the plaintiff to show that 1) the official violated a constitutional or statutory right; and 2) the constitutional or statutory right was clearly established when the alleged violation occurred. Farmer v. Perrill, 288 F.3d 1254, 1259 (10th Cir. 2002). First, "[t]aken in the light most favorable to the party asserting the injury, do the facts alleged show the officer's conduct violated a constitutional right?" Saucier v. Katz, 533 U.S. 194, 201, 121 S.Ct. 2151, 150 L.Ed.2d 272 (2001). If so, we must subsequently ask "whether the right was clearly established." Id. If the plaintiff does not satisfy either portion of the two-pronged test, the Court must grant the defendant qualified immunity. Gross v. Pirtle, 245 F.3d 1151, 1156 (10th Cir. 2001). If the plaintiff indeed demonstrates that the official violated a clearly established constitutional or statutory right, then the burden shifts back to the defendant, who must prove that "no genuine issues of material fact" exist and that the defendant "is entitled to judgment as a matter of law." Id. In the end, therefore, the defendant still bears the normal summary judgment burden of showing that no material facts remain in dispute that would defeat the qualified immunity defense. Farmer, 288 F.3d at 1259. When the record shows an unresolved dispute of historical fact relevant to this immunity analysis, a motion for summary judgment based on qualified immunity should be "properly denied." Salmon v. Schwarz, 948 F.2d 1131, 1136 (10th Cir. 1991) . . .

Olsen v. Layton Hills Mall, 312 F.3d 1304, 1312 (10th Cir. 2002).

II.

The following facts are either uncontroverted or shall be considered true for the purposes of deciding this summary judgment

motion. Plaintiff was employed by the Kansas Attorney General from February 7, 2003 to October 13, 2003 as an assistant attorney in the tobacco enforcement division. On October 10, 2003, plaintiff was told that he had to accept another position or be terminated from his employment. Plaintiff chose not to accept the new position. He was told he would be terminated in two weeks. Later that day Eric Rucker, senior deputy attorney general, instructed Scott Davidson, the computer specialist in the Attorney General's office, to restrict plaintiff's access to his computer over the weekend. He told him to allow plaintiff access to the computer on Monday morning, but to monitor plaintiff's activity on the network to ensure that plaintiff could not copy data. Over the weekend plaintiff attempted to access his computer, but was unable to do so. On October 13, 2003 plaintiff came to work and was eventually able to access his computer. He began to copy his personal files and work product. Rucker approached plaintiff and accused him of stealing. Plaintiff explained that he was attempting to copy his personal files. Approximately an hour later, plaintiff was terminated. He was told he had fifteen minutes to leave. He was not allowed to take anything with him, including personal items.

Subsequent to his termination, certain files on his computer, including personal e-mail messages, were viewed by employees of the Kansas Attorney General, including Davidson. Several months later,

plaintiff was given access to all of his e-mail and documents that remained on his computer after the termination of his employment.

Each morning when plaintiff logged onto the computer he used at the Attorney General's office, the "Computer Use Procedures" appeared on his computer screen. Plaintiff was aware of this document, and he even relied upon the warnings and instructions contained in that document. This document stated as follows:

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

III.

The court shall now turn to the arguments raised by the defendants. Before we consider the substantive arguments concerning plaintiff's claims, we must first address a contention asserted by some of the defendants. Defendants Attorney General Kline and Nations contend they are entitled to summary judgment on

all claims because there is no evidence before the court that they were involved in the search of the documents on plaintiff's computer. We must agree. "A claim seeking personal liability in a civil rights suit must be predicated on the defendant actor's personal involvement; there must be an affirmative link to causally connect the actor with the alleged violation." Gates v. Unified School Dist. No. 449, 996 F.2d 1035, 1042 (10th Cir. 1993). There is no evidence to support any contention that these defendants were involved in the search of the plaintiff's computer. Plaintiff has failed to point to any exhibit or testimony showing that these defendants were involved in any of the incidents that led to this litigation. Accordingly, the court finds they are entitled to summary judgment on all of the claims asserted by plaintiff.

A.

The Fourth Amendment prohibits government agents from conducting unreasonable searches and seizures. U.S. Const. Amend. IV. The Supreme Court has made clear that employees may have reasonable expectations of privacy within their workplaces which are constitutionally protected against intrusions by government agents. O'Connor v. Ortega, 480 U.S. 709, 716 (1987). "As with the expectation of privacy in one's home, such an expectation in one's place of work is 'based upon societal expectations that have deep roots in the history of the [Fourth] Amendment.'" Id. (quoting Oliver v. United States, 466 U.S. 170, 178 n. 8 (1984)).

However, an employee's expectation of privacy in the content of offices, desks and files may be reduced by an employer's practices, procedures, and legitimate regulation over the use of the employer's property. Id. at 717. The question of whether an employee has a reasonable expectation of privacy in his work area must be determined on a case-by-case basis. Id. at 718.

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 determined that the defendant did not have an objectively reasonable expectation of privacy. In reaching this conclusion, the Court found the following factors important: (1) 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; (2) the university owned the computer and explicitly reserved ownership of data stored within; (3) the defendant did not have access to the pornography because he had previously sought to delete it; and (4) the defendant did not take actions consistent with maintaining private

access to the pornography.

Having carefully considered all of the evidence provided by the parties, the court does not find that plaintiff has sufficiently demonstrated an objectively reasonable expectation of privacy. The overwhelming factor here is the warning conveyed by plaintiff's employer to him each time he used his computer. This warning explicitly indicated that information flowing through or stored on the computer could not be considered confidential. There is no evidence before the court to suggest anything contrary to the information provided in the Computer Use Procedures. In that document, plaintiff was told that "[t]here shall be no expectation of privacy in using this system." He was also warned that "[p]ersonal data on the system may be subject to removal." Finally, plaintiff was informed that contents on the computer may be subject to disclosure under the Kansas Open Records Act. These various warnings clearly put plaintiff on notice that he did not have an expectation of privacy in the computer and its contents.

Even if the court had determined that the defendants had violated plaintiff's Fourth Amendment rights, we would find that they are entitled to qualified immunity. The court is not persuaded that it would have been clear to a reasonable government official that his conduct was unlawful in the situation he confronted.

Recently, in Douglas v. Dobbs, ____ F.3d ____, 2005 WL 1953501

(10th Cir. 2005), the Tenth Circuit set forth the standards to be applied in determining this application of qualified immunity as follows:

A clearly established right is one whose contours must be sufficiently clear that a reasonable official would understand that what he is doing violates that right. Anderson v. Creighton, 483 U.S. 635, 640 (1987). Because knowledge that an action violates a clearly established statutory or constitutional right is required, the "essential inquiry is: would an objectively reasonable official have known that his conduct was unlawful?" Lawrence v. Reed, 406 F.3d 1224, 1230 (10th Cir. 2005). Warning against rights asserted at too high a level of generality, the Supreme Court has made clear that the relevant inquiry must be undertaken in the specific context of the case. Brosseau v. Haugen, 125 S.Ct. 596, 599 (2004). A plaintiff may not simply allege a Fourth Amendment violation in the abstract, but must demonstrate through relevant prior cases that a defendant's actions in a "more particularized sense" constitute a violation of a constitutional right. Id. at 599-600. "If the law at that time did not clearly establish that the officer's conduct would violate the Constitution, the officer should not be subject to liability or, indeed, even the burdens of litigation." Id. at 599.

The law concerning the expectation of privacy in an employee's work computer is not clearly established. The law is in a state of flux with the outcome heavily dependent upon the particular facts of each case. Here, the Attorney General's Office had taken steps to inform all employees that there should be no expectation of privacy in the data on their work computers. This was done through a screen message that each employee viewed or had the opportunity to view each time the computer was turned on. This type of message has been viewed as extremely significant by the courts that have

considered this issue. See 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); United States v. Bailey, 272 F.Supp.2d 822 (D.Neb. 2003) (employee had no reasonable basis to believe activities on work computer were private "when, through company's screen notification, they have actual knowledge that the computer can be searched"); United States v. Monroe, 52 M.J. 326 (C.A.A.F.2000) (sergeant had no reasonable expectation of privacy in his government e-mail account because e-mail use was reserved for official business and network banner informed each user upon logging onto the network that use was subject to monitoring). However, other factors also play a part in the determination of the expectation of privacy. 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). Given the circumstances that existed at the Kansas Attorney General's office, we do not find that plaintiff has demonstrated that the defendants violated a clearly established constitutional right.

B.

The defendants contend they are entitled to summary judgment on plaintiff's claim based upon the Fourteenth Amendment because (1) plaintiff did not have a property interest in the private documents on his work computer; (2) any deprivation of these documents was de minimis; (3) plaintiff has not demonstrated that he did not receive due process; and (4) they are entitled to qualified immunity on this claim.

"The fundamental requirement of due process is the opportunity to be heard at a meaningful time and in a meaningful manner." Mathews v. Eldridge, 424 U.S. 319, 333 (1976). In Parratt v. Taylor, 451 U.S. 527, 541-43 (1981), overruled on other grounds,

Daniels v. Williams, 474 U.S. 327, 330-31 (1986), the Supreme Court held that when a plaintiff alleges deprivation of a property interest occurring as a result of "a random, unauthorized act," the Fourteenth Amendment's due process requirement is satisfied if the state provides an adequate post-deprivation remedy. While Parratt dealt with negligent deprivations of property, the Court later ruled that this reasoning also applied to intentional deprivations of property. Hudson v. Palmer, 468 U.S. 517, 533 (1983). Accordingly, such claims are not cognizable under § 1983 when a state's post deprivation remedies are adequate to protect a plaintiff's procedural due process rights. Here, the claim asserted by plaintiff states a claim under the Kansas Tort Claims Act or for conversion. See McCormick v. City of Lawrence, 253 F.Supp.2d 1172, 1199 (D.Kan. 2003), aff'd, 99 Fed.Appx. 169 (10th Cir. 2004). Thus, because post-deprivation tort remedies were available to plaintiff in state court, his constitutional right to due process was not violated. Id. The defendants are, therefore, entitled to summary judgment on this claim.

IT IS THEREFORE ORDERED that defendants' motion for summary judgment (Doc. # 108) be hereby granted. Judgment shall be granted to all defendants and against the plaintiff.

IT IS SO ORDERED.

Dated this 26th day of August, 2005 at Topeka, Kansas.

s/Richard D. Rogers
United States District Judge