F I L E D
United States Court of Appeals
Tenth Circuit

FEB 22 2002

PATRICK FISHER
Clerk

PUBLISH

UNITED STATES COURT OF APPEALS

TENTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. ERIC NEIL ANGEVINE, Defendant-Appellant.	No. 01-6097

Appeal from the United States District Court
for the District of Western District of Oklahoma
(D.C. No. 00-CR-106-M)

Randal A. Sengel (Daniel G. Webber, Jr., United States Attorney, with him on the brief), Assistant United States Attorney, Oklahoma City, Oklahoma, for Plaintiff-Appellee.

Michael D. Scheitzach (Richard W. Anderson with him on the briefs), Oklahoma City, Oklahoma, for Defendant-Appellant.

Before **SEYMOUR**, Circuit Judge, **BRORBY**, Senior Circuit Judge, and **EBEL**, Circuit Judge.

BRORBY, Circuit Judge.

Eric Neil Angevine conditionally pled guilty to knowing possession of child pornography. On appeal, Professor Angevine argues the district court (1) improperly denied his motion to suppress images of child pornography seized from his Oklahoma State University computer, and (2) incorrectly applied the sentencing guidelines in determining his sentence. Our jurisdiction arises from 28 U.S.C. § 1291. For reasons set forth below, we affirm in part and dismiss in part.

BACKGROUND

Professor Angevine taught Architecture at Oklahoma State University. Pursuant to his employment, the University provided Professor Angevine an office computer. This computer was networked with other University computers and in turn was linked to computers around the world via the Internet. Professor Angevine used this computer to download over 3,000 pornographic images of young boys. After viewing the images and printing some of them, Professor Angevine deleted the pornographic files.

With the cooperation of Professor Angevine's wife, officers from the Stillwater, Oklahoma Police Department obtained a search warrant to look for child pornography on his University computer. Police seized the computer from Professor Angevine's office and turned it over to a police computer expert.

Although Professor Angevine attempted to erase the pornographic files, the computer expert used special technology to retrieve the data that had remained latent in the computer's memory.

After police arrested Professor Angevine, he submitted a motion to suppress the pornographic images seized from the University computer. Professor Angevine also submitted a motion arguing the search warrant used to seize the computer was invalid because police recklessly omitted material information in their application affidavit. To address these omissions, Professor Angevine asked for a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). The district court held the computer-use policies and procedures at Oklahoma State University prevented Professor Angevine from having a legitimate expectation of privacy in the data on the seized University computer. Accordingly, the district court held a *Franks* hearing was unnecessary since police did not need a search warrant to seize the University computer. The district court also denied Professor Angevine's motion to suppress the images found on the University computer.

Subsequently, Professor Angevine conditionally pled guilty to knowing possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). Under his plea agreement, Professor Angevine retained the right to appeal the denial of his suppression motion. However, Professor Angevine waived the right to appeal his sentence calculation unless the district court departed upward from the sentencing guidelines or controlling precedent relevant to the case subsequently developed.

Oklahoma State University has a computer policy that explains appropriate computer use, warns employees about the consequences of misuse, and describes how officials administer and monitor the University computer network. Initially, the policy maintains "[t]he contents of all storage media owned or stored on University computing facilities are the property of [the] University." The policy prohibits employees from using University computers to "access obscene material as defined by Oklahoma or federal law." The policy warns viewing obscene materials may result in "disciplinary action up to and including discharge, dismissal, ... and/or legal action." Providing for enforcement, the policy states:

> [T]he University reserves the right to view or scan any file or software stored on the computer or passing through the network, and will do so periodically ... to audit the use of University resources. Violation[s] of policy that come to the attention of University officials during these and other activities will be acted upon.... The University cannot guarantee confidentiality of stored data. Users should be aware that use of one of the data networks, such as the Internet, and electronic mail and messages, will not necessarily remain confidential from third parities outside the University in transit or on the destination computer system, as those data networks are configured to permit fairly easy access to transmissions.

The University policy also explains system administrators keep logs of file names which "may indicate why a particular data file is being erased, when it was erased, and what user identification has erased it." Furthermore, the policy provides when University officials believe an employee is violating state or federal law "and that access to an individual's data is required in order to conduct an internal investigation into such possibility, system administrators may monitor all the activities of and inspect the files of such specified user(s) on their computers and networks." To this effect, the University policy claims a "right of access to the contents of stored computing information at any time for any purpose which it has a legitimate 'need to know'" including access to "word processing equipment, personal computers, workstations, mainframes, minicomputers, and associated peripherals and software."

Additionally, Oklahoma State University officials posted a "splash screen" on University computers. Each time Professor Angevine turned on the computer in his office a banner appeared. This banner stated:

> Use of this computing system in any way contrary to applicable Federal or State statutes or the policies of Oklahoma State University or Computing and Information Services is prohibited and will make you subject to University disciplinary actions, including possible immediate termination, and may also subject you to criminal penalties.
>
> Under Oklahoma law, all electronic mail messages are

> presumed to be public records and contain no right of privacy or confidentiality except where Oklahoma or Federal statutes expressly provide for such status. The University reserves the right to inspect electronic mail usage by any person at any time without prior notice as deemed necessary to protect business-related concerns of the University to the full extent not expressly prohibited by applicable statutes.

Professor Angevine now appeals the denial of his suppression motion and again asks for a *Franks* hearing challenging the validity of the police search warrant. Professor Angevine also appeals the calculation of his sentence.

DISCUSSION

I.

Professor Angevine argues the district court erred in failing to suppress child pornography seized from an Oklahoma State University computer. Specifically, Professor Angevine argues the district court incorrectly held he had no "expectation of privacy in his office computer because his employer, Oklahoma State University, had a computer use and Internet policy that allowed [the University] a 'right of access' on a 'need to know basis.'" In reviewing the district court's refusal to grant a suppression motion, "we accept the district court's factual findings absent clear error and review *de novo* the district court's determination of reasonableness under the Fourth Amendment." *United States v. Olguin-Rivera*, 168 F.3d 1203, 1204 (10th Cir. 1999).

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 (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 (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).[1]

We address employees' expectations of privacy in the workplace on a case-by-case basis. *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987). "Within the workplace context, [the Supreme Court] has recognized that employees may have

[1] Because we conclude society is not prepared to recognize as reasonable an expectation of privacy in the seized University computer, we need not consider whether Professor Angevine himself had a subjective expectation of privacy.

a reasonable expectation of privacy against intrusions by police." *Id.* at 716. 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. 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.

Oklahoma State University policies and procedures prevent its employees from reasonably expecting privacy in data downloaded from the Internet onto University computers. The University computer-use policy reserved the right to randomly audit Internet use and to monitor specific individuals suspected of misusing University computers. The policy explicitly cautions computer users that information flowing through the University network is not confidential either in transit or in storage on a University computer. Under this policy, reasonable Oklahoma State University computer users should have been aware network administrators and others were free to view data downloaded from the Internet. The policy also explicitly warned employees legal action would result from violations of federal law. Furthermore, the University displayed a splash screen warning of "criminal penalties" for misuse and of the University's right to conduct inspections to protect business-related concerns. These office practices and procedures should have warned reasonable employees not to access child pornography with University computers.

Professor Angevine's relationship to the University computer also does not suggest a reasonable expectation of privacy. "'Although ownership of the item[s] seized is not determinative, it is an important consideration in determining the existence and extent of a defendant's Fourth Amendment interests.'" *Anderson*, 154 F.3d at 1231 (quoting *United States v. Erwin*, 875 F.2d 268, 270-71 (10th Cir. 1989)). The University explicitly reserved ownership of not only its computer hardware, but also the data stored within. Professor Angevine does not dispute Oklahoma State University owned the computer and the pornographic data he stored on it. Because the computer was issued to Professor Angevine only for work related purposes, his relationship to the University computer was incident to his employment. Reasonable people in Professor Angevine's employment context would expect University computer policies to constrain their expectations of privacy in the use of University-owned computers.

Additionally, the pornographic images seized by police were not within Professor Angevine's immediate control. The Supreme Court found a reasonable expectation of privacy in seized records where an employee "had custody of the papers at the moment of their seizure." *Mancusi v. DeForte*, 392 U.S. 364, 369 (1968). Unlike *Mancusi*, Professor Angevine did not have access to the seized data because he had previously attempted to delete the files from the University computer's memory. Police only recovered the data through special technology unavailable to Professor Angevine.

Finally, Professor Angevine did not take actions consistent with maintaining private access to the seized pornography. We are reluctant to find a reasonable expectation of privacy where the circumstances reveal a careless effort to maintain a privacy interest. *Anderson*, 154 F.3d at 1232. Professor Angevine downloaded child pornography through a monitored University computer network. University policy clearly warned computer users such data is "fairly easy to access" by third parties. The policy explained network administrators actively audit network transmissions for such misuse. While Professor Angevine did attempt to erase the child pornography, the University computer policy warned system administrators kept file logs recording when and by whom files were deleted. Moreover, given his transmission of the pornographic data through a monitored University network, deleting the files alone was not sufficient to establish a reasonable expectation of privacy.

Although we have found a reasonable expectation of privacy in information stored within offices, *United States v. Leary*, 846 F.2d 592, 598 (10th Cir. 1988), we have never held the Fourth Amendment protects employees who slip obscene computer data past network administrators in violation of a public employer's reasonable office policy. Considering "all of the relevant circumstances," *Anderson*, 154 F.3d at 1232, we hold Professor Angevine could not have an objectively reasonable expectation of privacy. Accordingly, we affirm the district court's denial of the motion for a *Franks* hearing and motion to suppress.

II.

Next, Professor Angevine argues the district court erred when it applied an incorrect guideline in calculating his sentence. The government counters Professor Angevine waived the right to appeal his sentence pursuant to a plea agreement. "A defendant's knowing and voluntary waiver of the statutory right to appeal his sentence is generally enforceable." *United States v. Black*, 201 F.3d 1296, 1300 (10th Cir. 2000) (quotation marks and citation omitted). As a threshold matter, Professor Angevine does not point to "public policy constraints" that suggest we should refuse to enforce his waiver. *Id*. at 1301. Rather, he argues two exceptions included in his plea agreement allow this appeal:

> (i) defendant specifically does not waive the right to appeal an upward departure from the sentencing guideline range *determined by*

> *the Court to apply to this case*, and (ii) his waiver of rights to appeal ... shall not apply to appeals or challenges based on changes in the law reflected in Tenth Circuit or Supreme Court cases decided after the date of this agreement which are held by the Tenth Circuit or Supreme Court to have retroactive effect.

(Emphasis added.)

Professor Angevine argues he has not waived his right to appeal his sentence because the district court made an "upward departure by analogy." However, Professor Angevine cites no case law, and we can find none, supporting this theory. The district court did not apply an upward departure to Professor Angevine's sentence. After determining United States Sentencing Guideline 2G2.2 applied to this case, the district court sentenced Professor Angevine to fifty-one months. Professor Angevine does not dispute this sentence is within the normal punishment range for U.S.S.G. § 2G2.2.[2]

Professor Angevine also contends our decision in *United States v. Neal*, 249 F.3d 1251 (10th Cir. 2001), represents a retroactive change in the law applicable to his case. In *Neal* we upheld a sentencing court's upward departure.

---

[2] Professor Angevine also argues because the plea agreement does not specify a punishment range his waiver was involuntary. This argument is foreclosed by *United States v. Rubio*, 231 F.3d 709, 712 (10th Cir. 2000) (finding waiver knowing and voluntary where agreement lacked "a definitive sentence or sentencing range").

Id. at 1259. In this case, the district court did not depart from the guideline it determined was applicable. Professor Angevine's plea agreement explicitly grants the district court the power to determine the applicable guideline. Because we choose to enforce Professor Angevine's plea agreement, we do not reach the merits of his objection to the district court's sentencing calculation.[3]

For the forgoing reasons, the district court's denial of Professor Angevine's motion to suppress is **AFFIRMED**. Professor Angevine's appeal of the calculation of his sentence is **DISMISSED** for lack of jurisdiction.

---

[3] In the alternative, Professor Angevine failed to supply the record necessary for us to consider the merits of the district court's sentencing calculation. Our rules provide, "[t]he presentence investigation report must be included if the appeal is from a sentence imposed under 18 U.S.C. § 3742." 10th Cir. R.10.3(D)(3). Moreover, "[w]hen the party asserting an issue fails to provide a record sufficient for considering that issue, the court may decline to consider it." 10th Cir. R.10.3(B). Professor Angevine asserts the district court applied an incorrect sentencing guideline, but includes only two pages of the presentence investigation report upon which the district court made its decision. Moreover Professor Angevine includes only two pages of the plea agreement. In this case, we decline to upset a knowing and voluntary plea agreement upon consideration of an insufficient record.