

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 00-20926

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

WESLEY JOSEPH SLANINA, also known as Wesley J Slanina,

Defendant-Appellant.

Appeal from the United States District Court
for the Southern District of Texas

Before JOLLY, SMITH, and BENAVIDES, Circuit Judges.

BENAVIDES, Circuit Judge:

Defendant Wesley Joseph Slanina ("Slanina") appeals his conviction for possession of child pornography. Slanina argues that the district court should have suppressed evidence obtained from computer equipment in his office and home, as well as his statements to law enforcement.⁽¹⁾ For the reasons that follow, we affirm the district court's denial of Slanina's motion to suppress.

I.

Slanina worked as the Fire Marshall for Webster, Texas for nine years. As Fire Marshall, his duties included public safety and fire prevention, fire inspections, review of city plans, enforcement of building codes, and handling of arson related calls. Additionally, he served as the Emergency Management Coordinator, concentrating on hurricanes and explosions. Slanina's immediate supervisor was Fire Chief Bruce Ure ("Ure"), who answered to the Public Safety Director, Mike Keller ("Keller"). As Public Safety Director, Keller was in charge of both the police and fire departments. Keller had once been Slanina's direct supervisor, but in November 1998 Keller and the City Manager, Roger Carlisle ("Carlisle"), decided to hire a full-time fire chief, selecting Ure for that position. Prior to Ure's arrival, Keller conducted Slanina's performance evaluations. Although Ure later assumed this responsibility, Keller maintained ultimate authority over Slanina's employment, including the review of his evaluations and any salary increases.

Prior to June 1999, Slanina's desk was located in City Hall, where he had a city-provided computer with Internet access but no connection to the city's intra-office network. When a new fire station was built, however, Slanina moved into his own office in the new station. He brought with him his old computer, but in the new fire station he had no Internet access or network connection. On Friday, June 11, 1999, Ryan Smith ("Smith"), the Management Information Systems Coordinator, began working to install the city network on the fire station computers. At around 5:00 p.m., Smith entered Slanina's new office with a grand master key and attempted to continue his work. The computer was turned on, but a screen saver was in place. Smith moved the mouse and discovered that the screen saver was protected by a password. To bypass the screen saver password, Smith restarted the computer. When he rebooted, however, Smith found that Slanina had installed a BIOS password. Without this password, Smith was unable to immediately access the computer's hard drive and could not install the network on Slanina's computer.⁽²⁾ Smith then contacted Ure to inform him of the problem, and Ure directed Smith to call Slanina and obtain the password.

Slanina had not come to work that Friday, as he was still recuperating from his recent surgery to have his wisdom teeth removed. Smith did not feel comfortable calling Slanina, so Ure himself phoned him. Ure informed Slanina that the computer technician was in his office attempting to install the network, but was unable to do so because of the password. Slanina initially balked, but after Ure indicated that Smith was already working overtime and that the job had to be completed that day, Slanina agreed to call Smith. On the phone with Smith, Slanina sounded nervous and hesitated before giving his password. He wanted to know exactly what Smith would do to his computer, and Smith promised that he was simply installing

the network and configuring his computer to the server.

Having received the password, Smith then resumed his work on Slanina's computer. In order to complete the task, Smith had to walk between Slanina's office and the server room. Upon returning to the office, Smith unexpectedly encountered Slanina-just ten minutes after they had talked on the phone. Needless to say, Smith was surprised to see Slanina, his jaw still swollen from the surgery. Smith's suspicions were further aroused when after he left the room, Slanina jumped back on his computer. Finally, when Slanina asked how much longer the network installation process would take, Smith lied, telling him that it would be another "couple of hours." Smith overstated the time to give himself a chance to see if something was wrong.

When Slanina finally left, Smith saw that the email was running, but minimized on the screen. As Smith clicked on the email to close it, he noticed the presence of newsgroups.⁽³⁾ Three months earlier, Keller had told Smith that no one was permitted to have newsgroups on their computers, but the policy had not been disseminated to the fire station employees, including Slanina. Smith expanded the email to look further at the newsgroups and saw three titles suggesting the presence of pornography. It was widely known that employees were not allowed to have pornographic material on their computers. To further investigate, Smith clicked on one newsgroup title, "alt.erotica.xxx.preteen", and saw that about 25 of the approximately 60 files had been read. At that point, however, he did not view any of the files.

Before contacting Ure, Smith wanted to be certain that Slanina's computer did have pornographic material on it. He conducted a search for JPEG files, which contain photographic images, and GIF files, which are used for other graphic images. His search located one such file in the Recycle Bin, and Smith restored the file. When he saw that it contained an image of adult pornography, he printed the file and attempted to contact Slanina's superiors. Neither Ure nor Keller were available, though, and initially Smith was only able to reach the Assistant Fire Chief, Dean Spencer ("Spencer"). By the time Spencer arrived at the station, Smith had spoken to Ure, telling him that he had found child pornography on Slanina's computer. Ure instructed him to secure the office, so at 7:00 p.m. Smith changed the lock on the door, turned the computer off, and left.

The next day, Smith spoke again to Ure, who by now had contacted Keller at an FBI conference in South Padre Island. Keller told Ure and Smith to remove the computer from the fire station and place it in his office, which was located in the police station. When they went to Slanina's office, Smith showed Ure the pornography⁽⁴⁾ before removing the computer. On Sunday afternoon, Keller returned from his conference and contacted Smith and Ure, asking them to meet him in his office at 3:00 p.m. Once there, Keller instructed Smith and Ure to get what was needed to view the contents of Slanina's computer, as well as any zip disk or drive⁽⁵⁾ in Slanina's office. Smith and Ure then returned to Slanina's office and retrieved the monitor and disks before rejoining Keller in his office. Smith showed Keller the picture of adult pornography he had printed on Friday night, and also pointed him to where he had found the image on the computer. With Smith's assistance, Keller searched material on the computer and zip drive for about two hours, viewing explicit child pornography. Finally, Keller contacted City Manager Carlisle and informed him that child pornography had been discovered on Slanina's computer. Their discussion addressed the possibility of criminal violations as well as the misuse of city property. Human Resources was then contacted, and Keller indicated to Smith and Ure that they should notify the FBI the next day.

At 7:15 a.m. on Monday morning, Ure met Slanina in the parking lot as he arrived at work, milk and doughnuts in hand. Ure told Slanina that they needed to meet in Keller's office, and asked him to get into

Ure's vehicle. Remembering that Slanina had undergone dental surgery the previous week, Ure asked him whether he had taken any medication that morning. Slanina said he had not, remarking that doing so would be a violation of city policy because he drove a city vehicle to work. In fact, though, he had taken medication, specifically the painkiller Vicodin. As they approached Keller's office at the police station, Slanina became visibly anxious, rocking back and forth. When they arrived, Slanina met Captain Ray Smiley ("Smiley") of the Internal Affairs Division and was furnished with a written copy of the Internal Affairs investigation. He was told that he would be suspended pending the investigation, which concerned the misuse of city property by obtaining child pornography with a city computer. Keller informed him that they had seized his computer and ordered Slanina to surrender his badge and city identification.

Keller told Slanina that he was not in custody and could leave at any time, but Slanina stayed with them. He admitted to accessing the newsgroups and downloading the pictures of child pornography. Keller explained that they would be contacting the FBI. Slanina promised to comply with the investigation, saying that he wanted to get the process going. Although he was embarrassed, Slanina said that he was relieved that it was finally out in the open. He confessed that he had some more "stuff" at his home, which Keller understood to mean more pornography. Keller told Slanina that he could either consent to a search of his home computer or they could obtain a search warrant. Wanting to be present when the police came to his home and confronted his family, Slanina consented and accompanied Keller, Ure and Smiley to his house. Once there, Slanina spoke with his wife and Keller informed her that her husband was under investigation for child pornography. Slanina then led them to his study, where he invited them to take the computer, zip drives and disks. After they gathered the equipment, Keller indicated to Slanina that he should return with them.

When they got back to the police station, Slanina waited in a conference room while Keller performed some administrative tasks related to the Internal Affairs investigation. Keller then searched the home computer and found more child pornography. Several weeks later, they discovered that the home computer actually belonged to the city. At about 9:00 a.m., Keller told Detective Sergeant Charles Propst ("Propst") to interview Slanina. He stated that although Slanina was not yet under arrest, they had found child pornography on his computer. Propst led Slanina into an interview room, where Sergeant Shari Burrows ("Burrows"), a Galveston child protective services officer, was present. The interview was taped, and Slanina was reminded again that he was not under arrest and was free to leave at any time. Nevertheless, pursuant to the Galveston County District Attorney's policy, Burrows provided Slanina with *Miranda* warnings. Slanina was fully cooperative and, at the end of the interview, signed a written statement. He then returned to Keller's office and offered to provide whatever help they needed. Finally, Slanina indicated that he wanted to leave, and was told that he could. Two days later, he was fired.

The office and home computer equipment, drives, and disks were turned over to the FBI, which examined active files and recovered deleted files from the hard drives. Each computer had two hard drives. Child pornography was found on each hard drive, and all together these hard drives contained thousands of files with such images. In addition, news servers had been installed on both computers, set to search for images of preteen and child sex. Additionally, three zip disks were also searched. The zip disk from Slanina's office contained more than one hundred files of child pornography. No child pornography was found on the two zip disks recovered from Slanina's home.

On February 14, 2000, Slanina was indicted on two counts of possession of child pornography under 18 U.S.C. §§ 2252A(a)(5)(B), 2256. He moved to suppress all statements made by him to law enforcement

officers and all evidence obtained from his office computer equipment and home computer equipment. At the conclusion of the suppression hearing, the district court denied the motion, stating:

I find that [at] the time and occasion in question back on June the 11th, 1999, the defendant did not have a reasonable and legitimate expectation of privacy in the city's computer located at the defendant's office at the city facilities. This is shown by the defendant's actions on that date.

I also find that the defendant gave a knowing, voluntary, and intelligent consent to the search and seizure of the city's computer at the defendant's residence, along with the disks and zip drives located at the residence.

Finally, I find that the statements and confession given by the defendant to the authorities on June the 14th, 1999, were voluntarily and knowingly given, and that the defendant was not in custody at the time that the statements and confession were given.

As a result of the district court's ruling, the following evidence was admitted: two CD ROM disks containing a copy of the contents of the office computer; six CD ROM disks containing a copy of the contents of the home computer; an Iomega zip disk recovered from Slanina's office; two Iomega zip disks from his residence; and a CD ROM disk containing a copy of what was found on the three zip disks. Moreover, at trial the district court admitted into evidence copies of representative samples of images stored on Slanina's work computer and office zip disk. After a bench trial, the district court found Slanina guilty on both counts and sentenced him to thirty-three months in prison, followed by three years of supervised release. The district court also imposed a \$200 special assessment and a \$2000 fine. Slanina timely filed a notice of appeal.

II.

Slanina argues that the district court erred by holding that he did not have a reasonable expectation of privacy. He further contends that Keller's warrantless search of the office computer equipment violated the Fourth Amendment. Regarding the search of his home computer, he argues that his consent was not voluntary. Finally, assuming *arguendo* that it was voluntary, Slanina contends that his consent and his subsequent statements to police were nonetheless tainted by the earlier unconstitutional search of his office computer. We now address these issues in turn, reviewing the district court's factual findings for clear error and its legal conclusions *de novo*. *United States v. Runyan*, 275 F.3d 449, 456 (5th Cir. 2001).

A.

The threshold question in our Fourth Amendment analysis is whether Slanina had a "constitutionally protected reasonable expectation of privacy." *California v. Ciraolo*, 476 U.S. 207, 211 (1986) (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)). This analysis involves two questions: "(1) whether the defendant is able to establish an actual, subjective expectation of privacy with respect to the place being searched or items being seized, and (2) whether that expectation of privacy is one which society would recognize as reasonable." *United States v. Gomez*, 276 F.3d 694, 697 (5th Cir. 2001) (quoting *United States v. Kye Soo Lee*, 898 F.2d 1034, 1037-38 (5th Cir. 1990)).⁽⁶⁾ In the present case, Slanina clearly demonstrated a subjective expectation of privacy with respect to his office and office computer equipment. He had closed and locked the door to his office. To limit access to his

computer files, he installed passwords, thereby making it more difficult for another person to get past the screen saver and reboot his computer. *Cf. Runyan*, 275 F.3d at 458 (holding that defendant exhibited subjective expectation of privacy in images of child pornography by storing them in containers away from plain view). Moreover, Slanina did not forfeit his expectation of privacy in the files by providing the BIOS password to Smith, as he gave Smith the password for the limited purpose of installing the network, not perusing his files.

Having determined that Slanina did exhibit a subjective expectation of privacy, we now must decide whether this expectation was objectively reasonable. The government notes that other city employees had a grand master key to Slanina's office. Furthermore, it claims that the city's need to develop network systems and upgrade equipment required complete computer access, and that Slanina's installation of the passwords did not change this situation. Finally, it points out that the computer was purchased by the city and that employees knew they were not allowed to use city computers to access and store pornography. Given these circumstances, the government contends, any expectation of privacy was unreasonable. We disagree.

Slanina had a private office at the new fire station, and the ability of a select few of his coworkers to access the office does not mean that the office was "so open to fellow employees or the public that no expectation of privacy is reasonable." *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987) (plurality). Moreover, even though network administrators and computer technicians necessarily had some access to his computer, there is no evidence that such access was routine. *Cf. Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001) (finding that government employee's expectation of privacy was reasonable and noting that state agency's access to computer did not appear to be frequent, widespread, or extensive). The city did not disseminate any policy that prevented the storage of personal information on city computers and also did not inform its employees that computer usage and internet access would be monitored. *See United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) (holding that in light of employer policy to inspect and monitor Internet activity, employee had no reasonable expectation of privacy in files transferred from Internet). Accordingly, given the absence of a city policy placing Slanina on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer, we hold that Slanina's expectation of privacy was reasonable.

B.

Having concluded that Slanina had a reasonable expectation of privacy in his office and office computer equipment, we now must decide whether the warrantless search of them violated the Fourth Amendment. The government characterizes Smith and Keller's search as a reasonable employer search related to an investigation into workplace misconduct, and therefore not subject to the warrant requirement. Slanina, however, contends that the workplace exception does not apply in this case. He argues that once Smith contacted Ure, after finding only the newsgroup titles and the image of adult pornography, he effectively became an agent of the police. Under this theory, the subsequent search of the computer by Keller, in which images of child pornography were first discovered, was not an investigation into work-related misconduct. Rather, it was a criminal investigation performed by the police, and therefore subject to the warrant requirement.

In *O'Connor v. Ortega*, a plurality of the Supreme Court considered the constitutionality of a state hospital administrator's search of a doctor's desk and file cabinets pursuant to an investigation into noncriminal work-related misconduct. *Id.* at 712-13. Concluding that the doctor had a reasonable

expectation of privacy, the Court nevertheless refused to apply the warrant requirement to the search. Instead, it held "that public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances." *Id.* at 725-26; *see also United States v. Johnson*, 16 F.3d 69, 73-74 (5th Cir. 1994) (applying test articulated in *O'Connor*). Specifically, such workplace searches must be reasonable both at the inception and in scope. *O'Connor*, 480 U.S. at 726.

Although *O'Connor* provides the starting point of our analysis, it does not end our inquiry, as the facts before us are distinguishable on at least two noteworthy points. First, in the present case, although Slanina's use of the city-provided computer equipment to access and store pornography certainly constituted workplace misconduct, it also violated criminal law. It cannot be said that by the time Keller, a law enforcement officer with expertise in child pornography investigations, searched Slanina's office computer, there was no criminal dimension to the investigation. The Supreme Court specifically excepted this situation from its holding in *O'Connor*, declining to "address the appropriate standard when an employee is being investigated for criminal misconduct or breaches of other nonwork-related or regulatory standards." *Id.* at 729 n.*. Second, the *O'Connor* Court suggested that its holding might not extend to the context of investigations into work-related misconduct by government employers who, like Keller, are also law enforcement officers. *See id.* at 724 (noting that while law enforcement officials are expected to learn the "niceties of probable cause . . . [i]t is simply unrealistic to expect supervisors in most government agencies to learn the subtleties of the probable cause standard").

Other circuits, however, have shed light on this issue. In *United States v. Simons*, the Fourth Circuit considered the legality of a government employer's search of an employee's office for evidence of child pornography. The defendant was an employee of a division of the Central Intelligence Agency ("CIA") and was suspected of using his office computer to access pornography. With help from network administrators, the defendant's employer copied his hard drive from a remote location. *Id.* at 396. A criminal investigator from the CIA Office of the Inspector General ("OIG") was then contacted. *Id.* Upon viewing the copy of the hard drive, the investigator found images of child pornography. *Id.* Later the same day, the network administrator entered the defendant's office and seized the hard drive, replacing it with a copy. *Id.* A few days later, the FBI was called. *Id.* The defendant appealed his conviction for possession of child pornography, claiming that the search of his office by the network administrator violated the Fourth Amendment. The Fourth Circuit rejected this challenge, holding that the *O'Connor* standard applied to the office search. *Id.* at 400. Importantly, the court assumed that the purpose of the search was "to acquire evidence of criminal activity," *id.*, which had been committed at the government office using government equipment. Nevertheless, it concluded, the *O'Connor* exception to the warrant requirement applied, observing that the government employer "did not lose its special need for the 'efficient and proper operation of the workplace,' merely because the evidence obtained was evidence of a crime." *Id.* (quoting *O'Connor*, 480 U.S. at 723).

We approve of the Fourth Circuit's reasoning in *Simons*, agreeing that *O'Connor*'s goal of ensuring an efficient workplace should not be frustrated simply because the same misconduct that violates a government employer's policy also happens to be illegal. *See also* 4 Wayne R. LaFare, *Search and Seizure* § 10.3 (3d ed. 2002) (noting that cases upholding searches by government employers into criminal, work-related misconduct are fully consistent with the reasoning in *O'Connor*).⁽⁷⁾ *There is an obvious distinction, however, between the facts confronted by the Fourth Circuit in Simons and the*

situation before us in the instant case. In *Simons*, the person conducting the search was a network administrator for the government employer, not a law enforcement official. By contrast, in the present case the critical search was performed by Keller, who was both a supervisor and a law enforcement officer. Therefore, we must also inquire whether the *O'Connor* exception should extend to the situation in which the criminal work-related misconduct is being investigated by an employer who is also a law enforcement officer.

Again, we look to guidance from other courts, which have answered this question in the affirmative. In several cases, searches by law enforcement personnel into work-related misconduct have been reviewed under the *O'Connor* standard. For example, in *United States v. Fernandes*, 272 F.3d 938, 942-43 (7th Cir. 2001), the Seventh Circuit held that a search by a county prosecutor into allegations of bribery against his deputy prosecutor was reasonable under *O'Connor*. Recognizing that in *O'Connor*, the search was not conducted by someone "in the business of investigating the violation of the criminal laws," the court nonetheless rejected the defendant's argument that this distinction rendered the search of his office illegal. *Id.* at 943 n.3. It looked instead to the purpose of the search, noting that the county prosecutor was conducting an investigation into work-related misconduct. *Id.* See also *Gossmeier v. McDonald*, 128 F.3d 481, 490-92 (7th Cir. 1997) (applying *O'Connor* to search by child protective services inspector general regarding allegations of child pornography against employee); *Shields v. Burge*, 874 F.2d 1201, 1203-05 (7th Cir. 1989) (applying *O'Connor* to search by police officers pursuant to investigation of work-related misconduct by fellow officer).

Our review of the relevant caselaw from our sister circuits leads us to the inescapable conclusion that Keller's search of Slanina's office computer equipment, including the hard drives and zip disks, should be reviewed under the *O'Connor* standard. As an expert in child pornography investigations, Keller undoubtedly appreciated the possibility that the investigation into Slanina's misuse of city computer equipment might result in evidence of criminal violations. Nevertheless, any evidence of criminal acts was also proof of work-related misconduct. Once Smith and Ure uncovered evidence of work-related misconduct, the city did not lose its interest in being able to fully investigate such misconduct in a regular and efficient manner. The record evidence demonstrates that as of the time of Keller's search, the probe remained at least partly an investigation into employee misconduct. The subsequent involvement of the City Manager and human resources in the process attests to this characterization. To hold that a warrant is necessary any time a law enforcement official recognizes the possibility that an investigation into work-related misconduct will yield evidence of criminal acts would frustrate the government employer's interest in "the efficient and proper operation of the workplace." *O'Connor*, 480 U.S. at 723. We decline to impose such a burden on government employers. Therefore, in assessing the constitutionality of Keller's search, we apply the standard articulated in *O'Connor*.

Under *O'Connor*, a search by a government employer must be justified at its inception and reasonably related to the circumstances justifying the interference in the first place. *Id.* at 726. We have little difficulty concluding that Keller's search passes this test. At the inception of his search, Smith had already discovered titles of newsgroups suggesting the presence of child pornography on Slanina's computer. Smith had also found an image of adult pornography, which represented a violation of city policy. On this evidence alone, Keller was justified in conducting a full search of the computer and accompanying disks to look for evidence of misconduct. Moreover, the scope of the search was also reasonable. The computer had been provided to Slanina by the city, and any use of it to access pornography was a violation of city policy. Keller was entitled to determine the extent of Slanina's

C.

Our conclusion that Keller's warrantless search of Slanina's office computer equipment was reasonable under O'Connor is not by itself sufficient to affirm the district court's admission of the evidence from the office computer equipment. After Keller's search, the FBI conducted an exhaustive search of the same equipment, and the evidence obtained from the FBI search was admitted at trial. Because we conclude that the FBI search does not fall under the O'Connor warrant exception, we must determine whether the admission of the evidence violated the Fourth Amendment. To answer the question, we need not venture outside the Fifth Circuit for guidance, as recent precedent from within this circuit provides the answer. In United States v. Runyan, 275 F.3d 449 (5th Cir. 2001), a defendant convicted on child pornography charges challenged inter alia the exhaustive police search of disks that had only partly been searched by a private party. The search was upheld, as the court stated that "the police do not exceed the scope of a prior private search when they examine the same materials that were examined by the private searchers, but they examine these materials more thoroughly than did the private parties." Id. at 464. Similarly, the FBI's full search of the computer equipment, which had already been partially searched by Keller, did not run afoul of the Fourth Amendment. Once Keller looked at the computer and the zip disk, Slanina's expectation of privacy in them had already been eroded. See id. at 465. He could not then complain about the FBI search of the same materials even though the FBI may have looked at more files than Keller. See id.

III.

Because we find no Fourth Amendment violation in the search of the office computer equipment, we need not address Slanina's argument that the consent to search his home computer and his statements to police were tainted. Accordingly, we now consider Slanina's argument that he did not voluntarily consent to the search of his home computer. The district court found that Slanina "gave a knowing, voluntary, and intelligent consent to the search and seizure of the city's computer" at his residence. Voluntariness of consent is a question of fact, which we review for clear error. United States v. Dortch, 199 F.3d 193, 201 (5th Cir. 1999). We look to six factors in determining whether consent is voluntary:

(1) the voluntariness of the defendant's custodial status; (2) the presence of coercive police procedures; (3) the extent and level of defendant's cooperation with the police; (4) the defendant's awareness of his right to refuse consent; (5) the defendant's education and intelligence; and (6) the defendant's belief that no incriminating evidence will be found.

Id. No single factor is dispositive Id. Slanina relies heavily on the fact that he knew that incriminating evidence would be found at his home, which militates against a finding of voluntariness. Moreover, he notes that Keller informed him that a search warrant would be obtained if he did not provide his consent, and that he was under the influence of a painkiller that made him disoriented. Finally, he claims that he was being held in custody despite Keller's assurances that he was free to leave at any time.

The government points out, however, that Slanina was extremely cooperative during the meeting in Keller's office and once they arrived at his house. His foremost concern throughout this time was minimizing the disruption to his wife and children. He acknowledged that he was embarrassed about the

discovery of the pornography on his office computer, but relieved that it was finally out in the open. Furthermore, he displayed no signs that the painkiller was affecting his judgment or actions. To the contrary, the testimony of those present with him in Keller's office suggests that he fully realized the enormity of the situation he faced and acted to contain the damage to his family. Given this strong evidence supporting the district court's conclusion, we cannot say that its finding of voluntariness was clearly erroneous.

IV.

For the foregoing reasons, we conclude that the warrantless search of Slanina's office computer equipment, including the computer and the zip disk, did not violate the Fourth Amendment. We also hold that the district court's finding that Slanina voluntarily consented to the search of his home computer equipment was not clearly erroneous. Accordingly, we **AFFIRM** the district court's ruling and Slanina's conviction.

1. Slanina also contends that the district court erred in denying his motion to dismiss the indictment on the grounds that the child pornography statute is unconstitutionally vague and overbroad. As Slanina concedes, the Fifth Circuit has already answered this question, upholding the validity of the statute. See *United States v. Fox*, 248 F.3d 394, 407 (5th Cir. 2001). The *Fox* decision conflicts with the Ninth Circuit's decision in *Free Speech Coalition v. Ashcroft*, 198 F.3d 1083, 1097 (9th Cir. 1999), cert. granted sub nom. *Ashcroft v. Free Speech Coalition*, 531 U.S. 1124 (2001). Nevertheless, until the Supreme Court instructs otherwise, we are bound by the *Fox* decision and therefore reject Slanina's challenge.

2. Technically, Smith could have accessed the hard drive without the BIOS password, but this process would have taken several hours. Specifically, he would have had to disconnect the computer's internal battery for some time in order to reset the system.

3. A newsgroup is an Internet discussion group focused on a particular topic. Users of the newsgroup share messages and can download files, including images. In addition to these groups, there are automated processes, such as news servers, allowing individuals to automatically receive files on a particular subject.

4. It is unclear exactly what images Ure saw. Smith recalls that he showed Ure "what was on the computer, the picture [he] had printed off." 4 R. 32. Ure, however, claims that he saw an actual image of child pornography. *Id.* at 98.

5. A zip disk is a removable, high density 3.5" disk used with small, portable zip drives.

6. The government contends that the district court made an "implied factual finding that Slanina had no subjective expectation of privacy[,] and that this finding should be reviewed for clear error. Gov. Br. 39. We disagree. Instead, we read the district court's holding literally, i.e., that Slanina "did not have a reasonable and legitimate expectation of privacy in the city's computer located at [his] office at the city facilities." 4 R. 315. In concluding that there was no objectively reasonable expectation of privacy, the district court properly considered Slanina's actions. See *United States v. Cardoza-Hinojosa*, 140 F.3d 610, 615 (5th Cir. 1998) (noting that one factor in determination of whether reasonable expectation of privacy exists is "whether [the defendant] has exhibited a subjective expectation of privacy").

7. We recognize the potential conflict between Simons and the Ninth Circuit's decision in *United States v.*

Taketa, 923 F.2d 665 (9th Cir. 1991). In *Taketa*, the Ninth Circuit upheld the search of a state investigator's office by officials of the Drug Enforcement Administration ("DEA"), who were looking into allegations of misuse of a pen register. The court concluded that the *O'Connor* exception applied to the office search because it was part of an internal investigation into work-related misconduct. *Id.* at 673-74. Nevertheless, it held that the subsequent video surveillance of the state investigator should not be reviewed under *O'Connor* because the character of the investigation had changed. *Id.* at 675. In reaching this conclusion, it relied on testimony from the DEA investigator that once confirmation of the defendant's misuse of the wiretap was provided, the internal investigation ceased and became a criminal investigation. *Id.* Even if *Taketa*, not *Simons*, illustrates the proper application of *O'Connor* to the context of a criminal investigation by a government employer, there remains a critical distinction with our case. Unlike in *Taketa*, where the government employer testified that the investigation became wholly criminal, at the time of Keller's search, he was still conducting an internal investigation into work-related misconduct as well as a criminal search. Because of the dual nature of Keller's search, the government employer's interest in the prompt and efficient operation of the workplace are more compelling in the present case than in *Taketa*, in which the investigation was purely criminal.

8. Recognizing the need to tread lightly in this relatively new area of Fourth Amendment jurisprudence, we stress that our decision is limited to the unique facts before us. Specifically, we note Keller's dual roles as supervisor and law enforcement officer, as well as the dual nature of Slanina's misdeeds, simultaneously violative of both workplace regulations and criminal law. We have no occasion to consider the constitutionality of a search of a government employee by a law enforcement officer who is not also the employee's supervisor. Moreover, we do not address the situation where the criminal acts of a government employee do not also violate workplace employment policy.