IN THE UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF FLORIDA
GAINESVILLE DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v. CASE NO. 1:09-cr-00031-MP-AK

OCTAVIUS LEE DURDLEY,

Defendant.

_____/

O R D E R

This matter is before the Court on Docs. 21 and 22, Defendant's Motion to Suppress with supporting memorandum. The government filed a response, Doc. 27, and the Court held an evidentiary hearing on Thursday, February 11, 2010. For the reasons below, the motion to suppress is denied.

The Defendant, Octavius Lee Durdley, was charged in a two count Indictment on September 22, 2009, alleging distribution of child pornography in violation of 18 U.S.C. 2252A(a)(2)(A) and 2252A(b)(1), as well as possession of child pornography in violation of 18 U.S.C. 2252A(a)(5)(B) and 2252A(b)(2). The Government intends to use evidence that was seized during the execution of a search at the Defendant's residence on or about June 17, 2009. The Government searched the Defendant's home pursuant to a Search Warrant (hereinafter "the Warrant") signed by Eighth Judicial Circuit Court Judge Stan R. Morris. (A copy of the Warrant is listed as *"Exhibit 1" to Doc. 22*[1]) The Warrant was issued based on factual assertions made in an Affidavit for Search Warrant (hereinafter "the Affidavit") signed and submitted by Bradford

[1]Henceforth, when the citation "Exhibit" is used, it is meant to refer to Exhibits to Doc. 22, Defendant's memorandum in support of the motion to suppress.

County Sheriff Office Detective Kevin Mueller. (*Exhibit 2*).

Prior to July 17, 2009, the Defendant was employed as a paramedic with Bradford County Emergency Services (hereinafter referred to as "BCES"). It is common for BCES employees to work shifts in excess of twenty-four (24) or more hours and to need locations for temporary residence and shelter while on duty. BCES utilizes at least three Medic Stations, which serve in part, as temporary housing, living quarters, and work stations for BCES employees. BCES Director Allen Parrish has acknowledged that the Medic Stations are makeshift residences. (*See Exhibit 3, Deposition of Allen Parrish, page 5/lines 16- 22*). During his shift, Mr. Durdley utilized a computer located at a medic station. The computer is owned by BCES, located in a common area, and is available for use by the entire BCES workforce of approximately 35 employees. At the end of his shift, Durdley left the workstation, leaving behind a removable storage device (thumb drive) inserted into one of the computer's USB ports.

On July 16, 2009, BCES Operations Captain Ron Johnson[2] discovered the thumb drive plugged into the computer. The files on the thumb drive were closed and were not opened or plainly visible when Ron Johnson began to use the computer. In order to access the files on the thumb drive, Ron Johnson had to first open the root directory of the thumb drive by double mouse clicking on the "My Computer" icon on his computer, then double clicking on the icon assigned to the thumb drive. Ron Johnson testified that after opening the thumb drive, he noticed that he could see several files in the root directory and also several folders in the root

[2]At all times relevant to this case, all BCES employees, including Ron Johnson and Director Allen Parrish, were employed and compensated by the government. At all times relevant to this case, Ron Johnson and Allen Parrish were acting in their official capacity as government employees.

directory.[3] In order to see the contents of those directories, Ron Johnson needed to click on the folder icons to open them. Before opening the subfolders, Ron Johnson examined the file names which appeared in the root directory of the thumb drive. Ron Johnson testified during the hearing that he could tell from the titles of these files that the thumb drive did not belong to him. *See also Johnson deposition page 16/lines 22-24.* In fact, Ron Johnson testified that because some of these filenames contained the term "BRAIN", which was a nickname of Mr. Durdley, he immediately suspected that several of the documents on the thumb drive were written by the Defendant, Octavius Durdley. *See also Johnson deposition, page 18/lines 2-7.*

Despite knowing that the thumb drive did not belong to him and that it appeared to belong to Octavius Durdley, Ron Johnson did not abort his search of the thumb drive, but instead opened several of the files in the root directory and then opened the folders. Eventually, he opened several files in a subfolder that appeared to contain images or videos of child pornography. After accessing these files, Ron Johnson contacted his own supervisor, Director Allen Parrish. Director Parrish contacted Bradford County Sheriff Gordon Smith, who in turn directed one his deputies, Raymond Shuford, to retrieve and examine the thumb drive.

Deputy Shuford arrived at Medic Station 2, was told of Mr. Johnson's discoveries, and conducted a warrantless search and then warrantless seizure of the thumb drive. At approximately 11:45 p.m. on June 16, 2009, Deputy Shuford, after seizing the thumb drive, contacted Detective Kevin Mueller, who is also with the Bradford County Sheriff's Office. On

---

[3]During the hearing Mr. Johnson at first appeared to state that all of the files on the thumb drive were visible in the root directory, without the need to open the subfolders. Later, after reviewing his deposition testimony, he corrected himself to state that some files were in the root directory as well as some subfolders. He also testified that no files containing child pornography were found in the root directory. As discussed below, he had to open the subfolders in the root directory to see the files containing child pornography.

June 17, 2009, at approximately 8 a.m., Det. Mueller reviewed the contents of the thumb drive. Detective Mueller observed videos depicting children posing nude and engaged in sexual acts. One video showed a girl, approximately 6 years of age, being vaginally penetrated by an adult male and conducting oral sex on an adult male. A second video depicted a girl, approximately 10 years of age, posing nude and masturbating.

On the same day, Detective Mueller conducted an interview with Durdley. Durdley admitted ownership of the thumb drive, and stated he commonly used the device for storing information used for his employment. Durdley also stated that he commonly downloaded pornography from the Internet, using the file sharing software "Limewire," on his personal desktop computer located at his residence in Gainesville, Florida.[4] At the conclusion of the interview, Mueller arrested Durdley and charged him with possession of child pornography in violation of Florida law.

Mueller then sought to obtain a search warrant for Durdley's residence in Gainesville. Mueller requested assistance from the North Florida Internet Crimes Against Children (ICAC) Task Force, headquartered at the Gainesville Police Department. ICAC Investigator Fred Cummings, an experienced sex crimes investigator, met with Mueller and BCSO Detective Ray Schuford. Cummings provided a sample affidavit to Mueller to assist him in the preparation of the affidavit. Muller inadvertently left statements representing Cummings' knowledge, experience and training, rather than his own, in the affidavit.

---

[4]In its response to the motion to suppress, the government states, "Further, Durdley stated that it was probable that there was child pornography saved on his desktop hard drive." Doc. 27, pp. 2-3. However, in the Affidavit submitted to support the Search Warrant, Detective Mueller did not include that statement from Durdley about child pornography probably being on the home computer. Thus, for the purposes of determining the validity of the search warrant, the Court will not consider that statement.

The warrant was signed by a circuit court judge, and the officers went to Durdley's residence and executed the warrant. A large number of computer-related items including computer hardware, and software and media files were collected as evidence for analysis. In addition, three published books displaying pictures of nude preteen children were collected as evidence. On August 18, 2009, a forensic review of evidence seized from Durdley's residence was completed, identifying thousands of images and movie files of child pornography.

The Defendant argues that the warrantless search of the thumb drive violated the Fourth Amendment and that evidence gained thereby should not have been relied upon in the subsequent search warrant. Moreover, since the search of the thumb drive led to all the subsequent discoveries, Defendant seeks to exclude all evidence in the case as fruit of the poisonous tree. Second, Defendant claims that even if the search of the thumb drive was lawful, the subsequent search warrant was invalid because it contained language regarding Cummings' experience, rather than the affiant's.

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

It is a "most basic constitutional rule ... that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment-subject only to a few specifically established and well delineated exceptions.' " Coolidge v. New Hampshire, 403 U.S. 443, 454-55, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971) (quoting Katz v. United States, 389 U.S. 347, 357, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967)).

Warrantless searches are thus presumptively unreasonable. Kyllo v. United States, 533 U.S. 27, 31, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). The initial question in this case, though, is whether a search occurred at all.

Under the test applied by the Supreme Court, "a Fourth Amendment search does not occur ... unless 'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and 'society is willing to recognize that expectation as reasonable.' " Id. at 33, 121 S.Ct. 2038 (quoting California v. Ciraolo, 476 U.S. 207, 211, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986)). As the Supreme Court recently stated: "Official conduct that does not 'compromise any legitimate interest in privacy' is not a search subject to the Fourth Amendment." Illinois v. Caballes, 543 U.S. 405, 408, 125 S.Ct. 834, 160 L.Ed.2d 842 (2005) (quoting United States v. Jacobsen, 466 U.S. 109, 123, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984)).

Moreover, it is a matter of black letter law that the Fourth Amendment does not apply to private searches or seizures. Burdeau v. McDowell, 256 U.S. 465, 475, 41 S.Ct. 574, 65 L.Ed. 1048 (1921) ("[The Fourth Amendment's] origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies ...."). And if a private party presents law-enforcement authorities with evidence obtained in the course of an unlawful search it is "not incumbent on the police to stop her or avert their eyes," Coolidge v. New Hampshire, 403 U.S. 443, 489, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971). Similarly, the Supreme Court has "held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." United States v. Miller, 425 U.S. 435, 443, 96 S.Ct. 1619, 48

L.Ed.2d 71 (1976); *see also* Hoffa v. United States, 385 U.S. 293, 302, 87 S.Ct. 408, 17 L.Ed.2d 374 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."). In all of those circumstances, the Supreme Court held that it is appropriate for the Government to rely upon evidence obtained by a private third party.

The Eleventh Circuit in U.S. v. King, 509 F.3d 1338 (11th Cir. 2007) dealt with both the issues described above: (1) whether the defendant has a legitimate expectation of privacy in computer data he inadvertently made accessible to others; and (2) whether the search involved should be considered a private or a government search. The factual context of King is strikingly similar to the instant case. In King, a civilian contractor staying on an airbase in Saudi Arabia connected his computer to the airbase's network. King understood that as a user of the base network, his activities on the network were subject to monitoring. King also believed that he had secured his computer so that others could not access the contents of its hard drive.

Later, however, an enlisted airman was searching the base network for music files when he came across King's computer on the network. The airman was able to access King's hard drive because it was a "shared" drive. In addition to finding music files on King's computer, the airman also discovered a pornographic movie and text files "of a pornographic nature." The airman reported his discovery to a military investigator who in turn referred the matter to a computer specialist.

This specialist located King's computer and hard drive on the base network and verified the presence of pornographic videos and explicit text files on the computer. She also discovered a folder on the hard drive labeled "pedophilia." The folder, however, contained no files. The

computer specialist did not employ any “special means” to access King's computer because “everybody on the entire network” could obtain the same access. The computer specialist then filed a report with the investigator detailing what she had found, and the investigator obtained a search warrant for King's room. During a search of his room, military officials seized King's computer and also found CDs containing child pornography.

The Defendant in King did not intentionally allow others access to his files, including the adult pornography and the folder named "pedophilia." That is, the Eleventh Circuit appeared to accept the following contention by King:

> King asserts that he sought to protect his computer files through security settings, he never knowingly exposed them to the public, and he was unaware that the files were shared on the network.

King, 509 F.3d at 1340.

In other words, King contends that he intended to connect his computer to the base network but did not intend to share the folders that contained the illicit content. When a computer is connected to a network, the default is for none of the folders on the user's computer to be accessible to any of the other users on the network. The reason is security. Computer owners want to be able to use network resources, such as shared internet connections, email, etc., without others on the network being able to put malicious applications on their computers or to view, remove or edit sensitive content.

Users can choose to disregard the security concerns by changing the properties of one or more folders on their computers. To do so, they first have to change the network settings on their computers to allow "sharing" in general, and then they have to change the property of any particular folder from "Not Shared" to "Shared." When a folder is shared, anyone on the network can access it and its contents.

One notable flaw in most operating systems is that the computer remembers and continues to share those folders regardless of which network the user connects to. Thus, if a person chose to share a folder over his home's network (with only the other computers connected to his home's network), and later forgets to turn off sharing, he will inadvertently share that folder with everyone connected to every network he later connects to, such as in the coffee shop, the college network, and in King's case, the airbase's network.[5]

Thus, like Mr. Durdley, it appears from these facts that King accidentally allowed others to have access to his files. Instead of leaving a thumb drive accidentally plugging in to a physical computer tower, King left a folder accidentally "plugged in" to a computer network, by failing to turn off sharing for that folder. Nevertheless, the Eleventh Circuit found that Mr. King's accidental sharing of his files on the network destroyed his reasonable expectation of privacy:

> It is undisputed that King's files were "shared" over the entire base network, and that everyone on the network had access to all of his files and could observe them in exactly the same manner as the computer specialist did. As the district court observed, rather than analyzing the military official's actions as a search of King's personal computer in his private dorm room, it is more accurate to say that the authorities conducted a search of the military network, and King's computer files were a part of that network. King's files were exposed to thousands of individuals with network access, and the military authorities encountered the files without employing any special means or intruding into any area which King could reasonably expect would remain private. The contents of his computer's hard drive were akin to items stored in the unsecured common areas of a multi-unit apartment building or put in a dumpster accessible to the public.
>
> Because his expectation of privacy was unreasonable King suffered no violation of his Fourth Amendment rights when his computer files were searched through the computer's connection to the base network. It follows that his additional claim

---

[5]For a sobering discussion of the implications of this common mistake, see http://www.raymond.cc/blog/archives/2007/08/28/dangers-of-sharing-folders-on-the-network/

> that the later search warrant was invalid because it incorporated information obtained from the search of his computer files also lacks merit.

In the instant case it is undisputed that Durdley inadvertently shared his files with all the users of the public computer. Durdley's files were exposed to anyone who sat down at the computer station who used the traditional means for opening and viewing files (such as Windows Explorer and the My Computer icon). Johnson encountered the files without employing any special means or intruding into any area which Durdley could reasonably expect to remain private once he left the drive attached to the common-use computer. The Court concludes, therefore, that Mr. Durdley had no more reasonable expectation of privacy in the contents of the thumb drive once he attached it to the common-use computer than the defendant in King did in his drive once he attached it to the airbase network.

Moreover, the Court concludes that Mr. Johnson's actions, even if considered a search, would not trigger the Fourth Amendment, because he acted as an employer rather than a law enforcement officer. The Defendant argues that because Mr. Johnson was a government agent and was Defendant's supervisor, any search done by him should be considered a search by government law enforcement. The Defendant stated it this way:

> In the instant case, Ron Johnson was working in his capacity as a government agent and was one of the Defendant's supervisors. Since the Defendant had a reasonable expectation of privacy in the contents of the thumb drive, the warrantless search conducted by Ron Johnson triggered the protections of the Fourth Amendment. Courts have recognized that "searches and seizures by government employers or supervisors of the private property of their employees, therefore, are subject to the restraints of the Fourth Amendment". *See O'Connor v. Ortega*, 480 U.S. 709, 715, 107 S.Ct. 1492, 1496 (1987); *Reyes v. Maschmeier*, 446 F.3d 1199, 1203 (11th Cir. 2006).

The undersigned disagrees. It is true that in the Reyes case cited by Defendant, the Eleventh Circuit concluded that "the Fourth Amendment regulates supervisor conduct in the

government workplace, even if the extent and manner of that regulation is unclear under the Supreme Court's cases." However, the Reyes panel also made clear that the supervisor conduct must be investigatory or law enforcement in intent to trigger the Fourth Amendment. In footnote five, the panel stated,

> At this point, we distinguish between the government as law enforcer and government as employer. See Driebel, 298 F.3d at 637 ("[I]n cases involving the constitutional rights of police officers, courts must distinguish between a police department's actions in its capacity as an employer and its actions as the law enforcement arm of the state.").

Reyes, 446 F.3d at 1204. Here, Mr. Johnson was clearly acting in his capacity as an employer. The mere fact that he was also employed by a government agency does not turn him into a part of the "law enforcement arm of the state." Johnson's testimony at the hearing established that he was using the computer for work purposes and not in a law enforcement capacity. Employers like the BCES possess a legitimate interest in the efficient operation of the workplace and the testimony at the hearing showed that Johnson was performing a search of his workstation in a supervisory capacity and was in no way searching for evidence to be used in criminal proceedings. Thus, his actions in reviewing the contents of a thumb drive attached to a common-use computer are not actions that trigger the Fourth Amendment.

Additionally, the subsequent reviews of the thumb drive by police detectives did not exceed the scope of the private review conducted by Mr. Johnson. In United States v. Jacobsen, 466 U.S. 109, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984), and its predecessor, Walter v. United States, 447 U.S. 649, 100 S.Ct. 2395, 65 L.Ed.2d 410 (1980), the Supreme Court affirmed that an individual can retain a legitimate expectation of privacy after a private individual conducts a search, but in Jacobsen the Court clarified that "additional invasions of [an individual's] privacy by the Government agent must be tested by the degree to which they exceeded the scope of the

private search." Jacobsen, 466 U.S. at 115, 104 S.Ct. 1652. Here, since the police reviews of the thumb drive did not exceed Mr. Johnson's, there can be no "additional invasions" to consider.

In sum, the Court finds that Mr. Durdley had no reasonable expectation of privacy in the thumb drive once he attached it to a common-use computer and forgot to remove it. Second, even if he did, the search by Mr. Johnson would be considered a private, rather than law enforcement search under Ortega and Reyes. Third, the subsequent police search did not exceed the scope of the private search. Thus, nothing about the search of the thumb drive justifies excluding the evidence found thereon.

Mr. Durdley also attacks the validity of the search warrant signed by Judge Morris because of certain admittedly false statements by Detective Mueller in the affidavit submitted to support the application for the warrant. Detective Mueller, working from a template provided by a more experienced Detective, Fred Cummings, wrongly included the knowledge, experience and training of Det. Cummings, rather than Det. Mueller's true knowledge, experience and training. The affidavit then stated that "Based upon your Affiant's knowledge, experience, and training in child exploitation and child pornography investigations, there are certain characteristics common to many individuals involved in the receipt and collection of child pornography." Since the knowledge, experience and training described in the affidavit was Fred Cummings' and not Detective Mueller's, the Defendant argues that the Judge should not have relied upon the descriptions of those common characteristics of child pornographers in finding justification for a search warrant of Durdley's home. That is, the affidavit stated, among other things, that child pornographers tend to retain child pornography for many years, and in a secure, private location such as their home. This information supports the idea that a search of the home would likely turn up evidence of possession and distribution of child pornography.

What the Fourth Amendment requires of a search warrant application is that it enables the issuing judge "simply to make a practical, commonsense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and the 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.' " United States v. Jiminez, 224 F.3d 1243, 1248 (11th Cir.2000) (quoting Illinois v. Gates, 462 U.S. 213, 238, 103 S.Ct. 2317, 2332, 76 L.Ed.2d 527 (1983)) (emphasis added). In this regard, " 'probable cause is a fluid concept-turning on the assessment of probabilities in particular factual contexts[.]' " United States v. Brundidge, 170 F.3d 1350, 1352 (11th Cir.1999) (quoting Gates, 462 U.S. at 232, 103 S.Ct. at 2329). For this reason, "[c]ourts reviewing the legitimacy of search warrants should not interpret supporting affidavits in a hypertechnical manner; rather, a realistic and commonsense approach should be employed so as to encourage recourse to the warrant process and to promote the high level of deference traditionally given to magistrates in their probable cause determination." United States v. Miller, 24 F.3d 1357, 1361 (11th Cir.1994) (citing Gates, 462 U.S. at 236-37, 103 S.Ct. at 2331-32; United States v. Ventresca, 380 U.S. 102, 109, 85 S.Ct. 741, 746, 13 L.Ed.2d 684 (1965)). In reviewing the issuance of the search warrant, the undersigned must determine only that the magistrate had a "substantial basis" for concluding that probable cause existed to uphold the warrant. See Gates, 462 U.S. at 238, 103 S.Ct. at 2331; see also Massachusetts v. Upton, 466 U.S. 727, 728, 104 S.Ct. 2085, 2085, 80 L.Ed.2d 721 (1984) (per curiam).

For the following reasons, the Court finds that the inclusion of the erroneous information in the affidavit is harmless and does not support the exclusion of the evidence found pursuant to the warrant. First, the Defendant has not offered any argument that the description in the

affidavit of the characteristics of child pornographers is inaccurate. Indeed, as stated during the hearing, the language in the affidavit has been used in affidavits prepared by Det. Cummings which have been found trustworthy and which have been relied upon by judges, including the undersigned, for years. As the affidavit itself states, "This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. " Exhibit 2, p. 4. Thus, there was no harm in the Judge relying upon representations of Det. Mueller (concerning the habits of child pornographers) that were accurate and which have risen to the level of common knowledge among investigators and judges.

Second, although Det. Mueller did not have the level of knowledge, training and experience of Det. Cummings, the Court finds that his testimony during the hearing established that he actually had the knowledge of the characteristics of child pornographers described in the affidavit. Det. Mueller is entitled to rely upon what Det. Cummings told him, from Cummings' own knowledge, training and experience, to be true about most child pornographers and their habits. Also Det. Mueller explained various ways in which he has come to learn of the characteristics of child pornographers described in the affidavit.

In sum, after reviewing the application for search warrant and the facts of the case in the context of common sense, the undersigned determines that the issuing judge had a substantial basis for concluding that probable cause existed to uphold a warrant to search Mr. Durdley's

home, notwithstanding the inaccurate description of Mr. Mueller's knowledge, training and experience.

Accordingly, it is hereby

ORDERED AND ADJUDGED:

The motion to suppress, Doc. 21, is denied.

DONE AND ORDERED this *11th* day of March, 2010

s/Maurice M. Paul
Maurice M. Paul, Senior District Judge