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

UNITED STATES OF AMERICA

v. **CASE#1:09CR31 MMP/AK**

OCTAVIUS LEE DURDLEY
_____/

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

COMES NOW the United States of America, by and through the undersigned Assistant United States Attorney, and files this Response to Defendant's Motion To Suppress Evidence.

The Defendant contends that, during the course of the investigation that led to his indictment, the police violated his rights under the Fourth Amendment. *See*, e.g., Doc. 21 at 10,11. He specifically challenges the examination of a thumb drive[1] inserted into a desk top computer at a medic station. *Id*. He also objects to certain information related to an officer's training and experience used in support of a search warrant of defendant's residence. As a result, the Defendant asks this Court to suppress the evidence "derived from the execution of the search warrant, and statement made by the Defendant during and after the execution of the search warrant." *Id.* at 17.

What the defendant fails to acknowledge, however, is that he did not have a reasonable

[1]A "thumb drive" is an electronic media storage device commonly known as a USB flash drive. It consists of flash memory data storage device integrated with a USB (Universal Serial Bus) 1.1 or 2.0 interface. USB flash drives are typically removable and rewritable, much smaller than a floppy disk, and most weigh less than 30 g (1 oz). USB flash drives are often used for the same purposes as floppy disks were. They are smaller, faster, have thousands of times more capacity, and are more durable and reliable because of their lack of moving parts. Until approximately 2005, most desktop and laptop computers were supplied with floppy disc drives, but most recent equipment has abandoned floppy disk drives in favor of USB ports.

expectation of privacy in the thumb drive left at his workplace. Furthermore, even without the challenged information in the search warrant affidavit, there remains sufficient probable cause to support the warrant. For these reasons and the reasons that follow, the United States respectfully requests that the Defendant's Motion be denied.

I. Relevant Facts.

1. On June 16, 2009, Defendant Octavius Lee Durdley was employed as a lieutenant with the Bradford County Emergency Services (BCES) in Starke, Florida. During his shift, he 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 the computer. Another BCES employee, Ron Johnson, subsequently used the computer and accessed the contents of the drive. He observed images of child pornography that were contained on the thumb drive. Johnson notified his superior who alerted the Bradford County Sheriff's Office (BCSO).

2. On June 17, 2009, BCSO Investigator Kevin Mueller reviewed the contents of the thumb drive and 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, Investigator 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. Further, Durdley stated that it was probable that there was child pornography saved on his desktop hard drive. At the conclusion of the interview, Mueller arrested Durdley and charged him with possession of child pornography in violation of Florida law.

3. 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 Cummings experience and training in the affidavit. 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.

4. 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.

5. On September 22, 2009, a grand jury indicted Defendant Durdley with one count of knowingly receiving and distributing child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A) and 2252(A)(b)(1), and with one count of knowingly possessing material that contained images of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B) and 2252A(b)(2).

6. On January 22, 2010, Durdley filed a motion to suppress. His motion raises two issues: (1) Was evidence found on a flash drive at the Defendant's workplace lawfully obtained? and, (2) Does the affidavit for a search warrant of Defendant's residence support probable cause absent erroneous information regarding the affiant's training and experience?

II. Argument and Authority.

A. Durdley had no expectation of privacy in the thumb drive left at his workplace and therefore suffered no violation of his Fourth Amendment rights when the thumb drive was searched.

A search is constitutional if it does not violate a person's "reasonable" or "legitimate" expectation of privacy. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). While Durdley may retain a reasonable expectation of privacy in a thumb drive under his own control, circumstances may eliminate that expectation. An individual will not retain a reasonable expectation of privacy in information that the person has made openly available. *Id.* at 351 "What a person knowingly exposes to the public, even in his own home or office, is not subject of Fourth Amendment protection." *Id.*

The defendant has cited to *O'Connor v. Ortega*, 480 U.S. 709 (1987), where the Supreme Court introduced a distinct framework for evaluating warrantless searches in government workplaces. According to *O'Connor,* a government employee can enjoy a reasonable expectation of privacy in his workplace. *See id.* at 717 (O'Connor, J., plurality opinion); *id. at* 730(Scalia, J., concurring). However, that expectation of privacy becomes unreasonable if "actual office practices and procedures, or . . . legitimate regulation" permit the employee's supervisor, co-workers, or the public to enter the employee's workspace. *Id*. at 717 (O'Connor, J., plurality

opinion). The reasonable expectation of privacy test formulated by the O'Connor plurality asks whether a government employee's workspace is "so open to fellow employees or to the public that no expectation of privacy is reasonable." *Id.* at 718. Government employees retain a reasonable expectation of privacy in the workplace only if a case-by-case inquiry into "actual office practices and procedures" shows that it is reasonable for employees to expect that others will not enter their space. *Id.* at 717.

Following *O'Connor*, courts evaluating public employees' reasonable expectation of privacy have considered the following factors: whether the work area in question is assigned solely to the employee; whether others have access to the space; whether the nature of the employment requires a close working relationship with others; whether office regulations place employees on notice that certain areas are subject to search; and whether the property searched is public or private. *See Vega-Rodriguez v. Puerto Rico Tel. Co.*, 110 F.3d 174, 179-80 (1st Cir. 1997). In general, courts have rejected claims of an expectation of privacy in an office when the employee knew or should have known that others could access the employee's workspace.

Under the *O'Connor* standard, Durdley did not possess a reasonable expectation of privacy when he used the computer at BCES. Durdley was aware that the computer where his thumb drive was found was not his personal workstation. He knew that the computer he was using was property of BCES, that it was located in a common area of BCES, and that the computer was available for use by all BCES employees. Furthermore, Durdley knew that his job required a close working relationship with others and that his co-workers and superiors would be able to view the contents of any files located in his thumb drive while it remained attached to the computer.

Assuming a government employee maintains a reasonable expectation of privacy, there are many exceptions where government employers are entitled to conduct reasonable work-related searches. The government, as an employer, can conduct a workplace search that violates a public employee's reasonable expectation of privacy so long as the search is "reasonable." *See O'Connor*, 480 U.S. at 722-23 (plurality); id. at 732 (Scalia. J., concurring). *O'Connor* establishes that public workplace searches by employers fall within the "special needs" exceptions that permit the government to dispense with the usual warrant requirement when its officials are acting in a non-law enforcement capacity. *See, e.g., New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring) (applying the "special needs exception to permit public school officials to search student property without a warrant in an effort to maintain discipline and order in public schools).

A warrantless search will be deemed "reasonable" if the employer participates in the search for a work-related reason, rather than merely to obtain evidence for use in criminal proceedings, and the search is justified in its inception and permissible in scope. *See O'Connor*, 480 U.S. at 721 (plurality). "The operational realities of the workplace," such as office practices, procedures, or regulations, frequently undermine employees' privacy expectations. *Id.* at 717. An employee's expectation of privacy must be assessed in the full context of their particular employment. *Id.* Employers and supervisors are focused primarily on the need to complete the government agency's work in a prompt and efficient manner. Requiring an employer to obtain a warrant whenever the employer wished to enter an employee's office, desk, or file cabinet for a work-related purpose would seriously disrupt the routine conduct of business and be unduly burdensome. *Id.* at 721-22.

Under analogous circumstances, the Eleventh Circuit held that a defendant did not have a legitimate expectation of privacy when the contents of his personal laptop computer were connected to the network of an army base. *United States v. King*, 509 F.3d 1338, (11th Cir. 2007). In *King*, although the defendant had experience with computer security and had taken affirmative steps to install security settings on his computer, the court felt that society was not prepared to accept King's subjective expectation of privacy as objectively reasonable because he left his computer attached to the army base network where it could be viewed by anyone with network access . Id. at 1341-42.

Similarly in this case, even if Durdley possessed a subjective expectation of privacy because he did not think that anyone would examine the contents of his thumb drive; society is not prepared to accept Durdley's subjective expectation of privacy as objectively reasonable. Durdley left his thumb drive in the work station. Everyone in the mobile EMS station had access to all of his files and could observe them in the same way that Ron Johnson did. Johnson did not conduct a search of Durdley's thumb drive; rather, Johnson conducted a search of the computer at the mobile EMS station, and Durdley's files were part of that computer. Durdley's files were exposed to anyone who sat down at the computer station and Johnson encountered the files without employing any special means or intruding into any area where Durdley could reasonably expect would remain private. Further, Johnson's search was reasonable because 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 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

Because his expectation of privacy was unreasonable Durdley suffered no violation of his Fourth Amendment rights when his thumb drive files were searched through a routine search of the computer at the mobile station.

B. With the erroneous information removed from the probable cause affidavit there is still sufficient evidence to support a finding of probable cause.

A warrant is valid if, absent the misstatements or omissions, there remains sufficient content to support a finding of probable cause. *See Franks v. Delaware*, 438 U.S. 154, 171-72 (1978). Probable cause to support a search warrant exists when the totality of the circumstances allows the conclusion that "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *See Illinois v. Gates*, 462 U.S. 213, 238 (1983).

Detective Mueller unintentionally misstated his experience and training in the affidavit. There is no evidence that Detective Mueller made deliberate or reckless misstatements, rather, Detective Mueller adopted portions of an existing document. With the erroneous information removed from the affidavit there is still sufficient evidence to support a finding of probable cause. Detective Mueller accurately conveyed the information that he obtained from the thumb drive and from interviewing Durdley. The Detective's training and experience were not necessary to the finding of the elements of probable cause. Probable cause was firmly established when Detective Mueller explained in his affidavit that he found explicit child pornography on Durdley's thumb drive and Durdley admitted that he commonly downloads porn from the Internet onto his home computer.

A thumb drive is much like a floppy disk or CD-Rom; it is used as a means to transfer, transport, and store personal files such as documents, pictures and videos. Thumb drives have no

mechanical components, they are not computers. Consequently, it is reasonable to conclude that the child pornography found on Durdley's thumb drive originated from a separate computer. Given that Durdley admitted that he downloaded pornography onto the computer located at his residence there existed a fair probability that the child pornography located on Durdley's thumb drive originated from the computer located inside his residence. The totality of the circumstances provide a sufficient basis to support a finding of probable cause and that resultantly there was no violation of Durdley's constitutional rights.

III. Conclusion

The evidence in the affidavit for search warrant was lawfully obtained and did not violate Durdley's rights under the Fourth Amendment. Further, the misrepresentations in the affidavit for search warrant were insignificant and immaterial and if removed there is still sufficient evidence to support a finding of probable cause.

Respectfully submitted,

THOMAS F. KIRWIN
United States Attorney

s/ F. T. WILLIAMS
FT. WILLIAMS
Assistant United States Attorney
Fla Bar# 936219
300 East University Ave., Ste 310
Gainesville, Florida 32601
(352) 378-0996

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true copy of the foregoing was furnished this 5th day of February, 2010, to Nick G. Zissimopulos, by electronic filing.

s/ F. T. WILLIAMS
FT. WILLIAMS
Assistant United States Attorney