UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
COVINGTON

CRIMINAL ACTION NO. 03-25-DLB

UNITED STATES OF AMERICA **PLAINTIFF**

VS. **MEMORANDUM OPINION & ORDER**

MICHAEL WAYNE MORGAN **DEFENDANT**

****

This matter is currently before the Court on Defendant's Motion to Suppress Evidence seized from the Defendant's computer. (Doc. # 11) The government filed its response opposing the motion. (Doc. # 15) An evidentiary hearing was conducted on June 11, 2003. Defendant has filed two post-hearing memoranda (Doc. # 27, 28) to which the government has responded. (Doc. # 29) Thus, the motion is now ripe for review.

I. Issues Raised

In his suppression motion, Defendant argues that because the files containing the pornographic images were "password protected", any written consent given by his wife, Cassie Morgan, was invalid. More particularly, Defendant argues that his wife "did not have access to that portion of [his] computer where the pornographic images were stored." (Doc. # 14 at 2) Defendant also argues that there was a "code" that blocked that portion of his computer. Because his wife did not have that code, she lacked authority to consent to its search. (*Id*.) Defendant further argues that because his wife was acting as an agent of the government when she captured certain screen images using "spy-ware" software,

and those images were captured without a search warrant or other exception to the warrant requirement, those images are subject to exclusion.[1]

II. Statement of Facts

On June 11, 2003, the undersigned conducted an evidentiary hearing wherein the Court heard testimony from Detective Vic Lavender and Captain Jack Prindle of the Boone County Sheriff's Department, watched a videotape of testimony given by Cassie Morgan during a suppression hearing in Boone Circuit Court on March 26, 2002, and heard testimony from the Defendant. The transcript of Cassie Morgan's state court testimony has been filed in the record. (Doc. # 23-1) After reviewing the testimony, the Court makes the following factual findings:

1. On November 28, 2001, Cassie Morgan called Captain Jack Prindle of the Boone County Sheriff's Department (BCSD). (TR of Supp.Hrg. "TR", Prindle at 22, 57) Prior to this call, Prindle had never spoken with Mrs. Morgan. (*Id*. at 22) During their conversation, Mrs. Morgan told Prindle that the week before she was on her husband's computer and observed a reference to a file on the computer that was entitled "5YRSFUCK". (*Id.* at 24-25) Mrs. Morgan was very upset and became suspicious that her husband was involved in child pornography. (*Id.*; Doc. # 23-1 at 1, 5)

2. Prior to calling Prindle, Mrs. Morgan had purchased a spy software program which she had installed on her husband's computer unbeknownst to him. (Prindle, TR at 25; Doc. # 23-1 at 2) Neither Prindle nor BCSD Detective Vic Lavender assisted Mrs.

[1] Defendant did not address this issue in his post-hearing memoranda. However, because it was raised during the evidentiary hearing, the Court will address the merits of the argument.

Morgan in installing the spy software. (Prindle, TR at 25) Mrs. Morgan also told Prindle that she had set the spy software to conduct a screen capture every ten (10) seconds so it would capture those images into an image file. (*Id.*) In order to install the spy software, Mrs. Morgan would have had to log onto the computer, exercise some control over it, insert the software into the computer, and follow the installation instructions. (*Id*. at 27) Mrs. Morgan told Prindle that she was very upset about what she had observed from the spy software that she had installed. (Doc. # 23-1 at 5)

3. During their telephone conversation, Mrs. Morgan also told Prindle that both she and her husband used the computer, they had no individual log-ins for its use, and made no mention of the computer being password protected. (Prindle, TR at 29)

4. On November 29, 2001, Detective Lavender and other officers with BCSD responded to a domestic call at 10110 Squire Drive in Boone County, the home of Defendant and Mrs. Morgan. (Lavender, TR at 8, 18) Upon Lavender's arrival at the residence, he was advised of a compact disc ("CD") by Boone County Sheriff's Deputy Brad Ezell. (Lavender, TR at 8) Deputy Ezell told Lavender he had been given the CD by Mrs. Morgan who admitted to Lavender that she had given the CD to Ezell. (*Id.* at 8, Doc. #23-1 at 8) This CD contained the images she had captured using the spy software. (Doc. #23-1 at 8)

5. During her conversation with the officers on November 29, 2001, Mrs. Morgan never told the officers there was another computer in the house. (*Id.* at 6) Mrs. Morgan also told the officers that she occasionally used the computer in the basement and had access to that computer. (*Id.* at 7) While Mrs. Morgan said she did not know the

password used to access the Internet from the basement computer, she admitted that there was no password to log onto the computer, turn it on, or use the basic screens. (*Id.* at 7-8)

6. At 11:50 a.m. on November 29, 2001, Mrs. Morgan signed a consent to search the computer and associated computer hard drive information for the basement computer. (Gov. Ex. #1, Lavender, TR at 12-13; Doc. #23-1 at 4) This was the computer in which she had installed the spy software. The consent to search was witnessed by BCSD Sargent Rusty Ellis. (Gov. Ex. #1) The written consent authorized the search of:

> the computers, central processing units, all data drives, hard drives, floppy drives, optical drives, tape drives, digital audio tape drives, ZIP drives, and/or any other internal or external storage devices such as magnetic tapes and/or disks; any terminals and/or video display units and/or receiving devices and/or peripheral equipment such as, but not limited printers, digital scanning equipment, automatic dialers, modems, acoustic couplers and/or direct line couplers, peripheral interface boards, and connecting cables and/or ribbons; any computer software, programs and source documentation, computer logs, diaries, magnetic audio tapes and recorders, digital audio discs and/or recorders, any memory devices such as, but not limited to, memory modules, memory chips, bubble memory, and any other form of memory device utilized by the computer or its peripheral devices; (this description constitutes the definition of a computer system as that term may be used throughout this document); *and any and all computer related accessories not specifically mentioned herein.* (Emphasis in original). (*Id.*)

Mrs. Morgan never withdrew her consent. (Prindle, TR at 55)

7. Mrs. Morgan was calm, compliant, and very accommodating with Lavender while he was explaining the consent form to her. (Lavender, TR at 13) Lavender read the consent to search form to Mrs. Morgan verbatim. (*Id.*)[2] Because of Mrs. Morgan's

[2] Mrs. Morgan disputes the fact that Lavender read the consent to search form to her in its entirety. (Doc. #23-1 at 4). However, Mrs. Morgan does admit that Lavender went over the basics of the consent form with her. (*Id.*)

relationship with Defendant, the Court finds Lavender's version of the facts relating to the consent form is more credible than Mrs. Morgan's. Mrs. Morgan did not tell Lavender that the computer was password protected while he was disassembling the computer. (Lavender, TR at 15) Mrs. Morgan also did not mention to Lavender that there were any other computers in the home. (*Id.* at 16; Doc. # 23-1 at 6) Mrs. Morgan also told Lavender that the computer in the basement, which was located in an open area, was their joint computer. (Lavender, TR at 14-15)

8. After the computer was removed from the residence, Lavender relinquished custody of it to Captain Prindle. (Prindle, TR at 29) Prindle was also given a copy of the consent to search signed by Mrs. Morgan as well as the CD containing the spy-ware images. (*Id.*) In order to conduct the search, Prindle made a duplicate mirror image of what was contained on the computer's hard drive. (*Id.* at 31) Prindle did so to maintain the integrity of the evidence and prevent destruction of any evidence. (*Id.*) Prindle utilized "Encase" software during his forensic search and analysis. (*Id.* at 33-34)

9. Using the Encase software, Prindle was able to identify certain graphic image files contained on the hard drive. (*Id.*) During his search of the computer, Prindle determined that the operating software on the computer was Windows XP Home Edition. (*Id.* at 34) During his search of the CD, Prindle determined that spy-ware images were captured on November 27, 2001 and November 29, 2001. (*Id.* 28, 57-59) The vast majority of these images were dated November 29, 2001, prior to the police responding to the residence. (*Id*. at 57, 59) The spy software installed by Mrs. Morgan inserted the date and time of each capture at the top of each created image. (*Id.* at 28, 61)

10. During his forensic search of the hard drive, Prindle determined that there was no individual profile for either Mrs. Morgan or Defendant. (*Id*. at 35) All software and other files, including the pornographic images recovered, were associated with the user name "owner." (*Id.*) There was no password found for the user name "owner." (*Id*. at 35-36) Prindle determined that the default profiles were still in effect at the time of his analysis. (*Id.* at 42)[3] Captain Prindle determined that there was no forensic evidence that any of the files were password protected or encrypted. (*Id.* at 37) In fact, Prindle testified that the operating system on the computer, Windows XP Home Edition, did not have the capability of individual file security or individual file encryption. (*Id.*)

11. During his search, Prindle located 148 images on the computer's hard drive which he determined to depict a minor engaged in some type of sexual performance. (*Id*. at 37, 59-60, 65) None of these 148 images were recovered using the spy-ware software. (*Id.* at 65) Prindle was able to trace the pornographic images back to a software news group reader where certain attachments had been downloaded, some of which contained images themselves, some of which contained truncated files which needed to be reconstituted before viewing was possible, and some of which contained video clips of pornographic images. (*Id.* at 38-39)

12. Prindle also found images from files which had been deleted. (*Id.* at 39-40) His "Encase" retrieval software was able to determine when the file was created, the time the file was last written or modified, the time the file was last accessed, and the time the

[3] If there had been a password, Prindle testified that Mrs. Morgan would have had to have gotten past the password when she installed the spyware software on the computer. (*Id.* at 36)

file was deleted. (*Id.*)

13. Prindle also found software entitled "Internet Eraser," which had been installed onto the computer. This software was used to destroy any evidence that exists and to overwrite files that had been deleted. (*Id.* at 40, 49) Defendant admitted that he installed the Internet Eraser software for the purpose of deleting images which he had viewed using the news reader group website. (Morgan, TR at 71-73) The news reader group from which the images were obtained provided Defendant a user name and password as well as a code. (Morgan, TR at 72) Defendant kept the user name, password, and code private. (*Id.*)

14. While access to the news reader group was restricted via the use of a user name and password, access to the files on the computer itself was not password protected. (Prindle, TR at 46) In fact, once the files were downloaded as images to the computer's hard drive, neither a user name nor password was required to access what had already been downloaded from the news reader group's website. (*Id.* at 47) The use of the user name and password related solely to the user's ability to log onto the news reader group website and/or gain access to that website's information. Any images and/or files which had been downloaded from the news reader group's website were accessible whether or not the person wanting to view those files was logged on to the Internet. (*Id.* at 41)

15. During his testimony, Defendant admitted to accessing "alt.binaries.pictures.underaged.admirers." via the news reader group's website. (Morgan, TR at 76-77) Defendant installed the Internet Eraser software in an effort to delete the

images he had decoded from the news reader's website. (*Id.* at 83) Defendant downloaded some of the pictures from "alt.binaries.pictures.underaged.admirers." to his hard drive by hitting a button that said "decode." (*Id.* at 77-78) Defendant understood that "decode" meant download, and that when he hit the decode button it would decode every single attachment in the news group. (*Id.* at 82) Defendant also admitted that no password was needed to access the computer itself. Rather, a password was only needed to access the Internet and the news reader group's information website. (*Id.* at 80)

III. Analysis

The Warrantless Search of the Basement Computer in this Case did not Violate Defendant's Constitutional Rights.

Although generally considered unreasonable, a warrantless search of a defendant's property, as occurred here, via the forensic search of the computer in question, is valid if conducted pursuant to the person's consent. *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) When seeking to justify a search conducted pursuant to someone's consent, the government has the burden of showing by a preponderance of the evidence that the consent was "freely and voluntarily given," and was not the result of coercion, duress, or submission to a claim of authority. *Bumper v. North Carolina*, 391 U.S. 543, 548 (1968) The voluntariness of the consent is determined by the "totality of the circumstances," *Schneckloth*, 412 U.S. at 227, 249, and must be proven by "clear and positive" proof. *United States v. McCaleb*, 552 F.2d 717, 721 (6th Cir. 1977) Although a subject's knowledge of a right to refuse is a factor to be taken into account, the prosecution is not required to demonstrate such knowledge as a prerequisite to establishing voluntary consent. *Schneckloth*, 412 U.S. at 249

The Supreme Court in *United States v. Matlock*, 415 U.S. 164, 171 (1974) expounded upon the traditional notion of consent by holding that officers may obtain voluntary consent "from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected." In *Matlock,* the Supreme Court defined "common authority" as:

> [M]utual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.

Matlock, 415 U.S. at 171 n. 7 Common authority is not to be implied from the mere property interest a third party has in the property. Moreover, the authority which justifies the third-party consent does not rest upon property laws, but rather, rests on mutual use of the property by persons generally having joint access or control for most purposes. *Id.*

In the personal computer context, courts generally examine whether the relevant files/documents were password-protected or whether the defendant otherwise manifested an intention to restrict third-party access. *Trulock v. Freeh,* 275 F.3d 391, 403 (4th Cir. 2001) (ruling that a warrantless search of plaintiff's password-protected files violated his Fourth Amendment rights); *United States v. Smith,* 27 F.Supp.2d 1111, 1115 (C.D.Ill.1998) (holding that live-in girlfriend could consent to search of computer because (1) the computer was located in an accessible portion of the house; (2) the presence of children's toys located around the computer suggested other family members had access to the computer; (3) defendant's girlfriend was not prohibited from using the computer; and (4) the computer was not password-protected).

In this case, although Defendant argues that the pornographic images were password protected and/or a code was needed to access the images, the facts elicited during the hearing prove otherwise. First, the operating system on the computer, Windows XP Home Edition, did not permit password protection or encryption of specific files. Second, while Defendant may have needed a username, password, and code to access the pornographic images from the news reader group's website, once he downloaded those images to his hard drive for viewing, those same images were not password protected. *Statement of Facts, supra* at ¶ 14 Third, once downloaded, those images were accessible whether or not the person wanting to view the images was connected to the Internet, a point conceded by Defendant on cross-examination. *Id.* at ¶¶ 14-15 Thus, the fact that Cassie Morgan did not know the username, password, or code to access the news reader group website did not restrict her ability to consent to a search of the computer.

It is undisputed that Cassie Morgan had used Defendant's computer prior to consent being obtained. Not only had she advised Captain Prindle that both she and Defendant used the computer, she had installed the spy-ware software on that computer. (*Id.* at 2-3) She also told Detective Lavender that she occasionally used and had access to that computer, and characterized the computer as their joint computer. (*Id.* at 5, 7) It is further undisputed that the computer itself was located in an open area in the basement of the residence. (*Id.*)

Given these facts, the Court is satisfied that the government has carried its burden of showing by a preponderance of the evidence that Cassie Morgan did have joint access to or joint control of the computer. The computer was located in an open, accessible area

of the basement. While Cassie Morgan may not have known how to view the pornographic images downloaded by Defendant, she did have access to the computer itself and its files. Although the Defendant had installed an Internet Eraser software program to purge the computer of these images, the images were not password protected.

Moreover, there is no evidence from which the Court could conclude that the written consent obtained from Cassie Morgan was anything other than knowingly and voluntary. *Statement of Facts* at ¶ 7 Because she had common authority over the computer itself, and her written consent was otherwise valid, the fact that the officers may have had sufficient time to obtain a search warrant is of no consequence. Defendant has cited no authority, nor has the Court found any, which requires officers to obtain a search warrant when they have sufficient time to obtain such a warrant. While the law may favor search warrants, third party consent is a validly recognized exception to the warrant requirement.

Assuming *arguendo* that Cassie Morgan did not have actual authority over the computer, the consent search is still valid because the facts available to the officers would lead a man of reasonable caution to believe that she had actual authority to consent to a search. *Illinois v. Rodriguez,* 497 U.S. 177, 188-89 (1990) The evidence elicited during the hearing supports an alternative finding that Cassie Morgan had apparent authority to consent to a search of the computer.

In his brief, Defendant argues that the pornographic images in this case are analogous to a locked footlocker. In support of his argument, Defendant relies upon *Trulock v. Freeh*, 275 F.3d 391 (4th Cir. 2001). Defendant's reliance on *Trulock* is misplaced. While the images may have been analogous to a locked footlocker while they

were being viewed from the news reader group's website, once they were downloaded by Defendant to the computer's hard drive, the analogy ended. Once downloaded, the images had been placed in a location analogous to a common closet, accessible to anyone.

In *Trulock*, the defendant's townhouse and computer were searched after the defendant's roommate, who had access to all areas of the townhouse and Defendant's computer, consented to a search of Defendant's property. 275 F.3d at 398 Among the things searched were the defendant's password protected documents located in her computer's hard drive. (*Id.)* The Fourth Circuit held that the search of the computer was valid. (*Id.* at 403) However, the court found that the search of the password-protected files was invalid because the files carried an additional expectation of privacy. (*Id.*) In so concluding, the court wrote:

> [a]lthough [Defendant's roommate] had authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files.

Id. Trulock's use of a password to protect the files evidenced an unmistakable intent to exclude others from those files.

Unlike was the case in *Trulock, supra*, there was no password protection of any kind on the Defendant's computer. In fact, Defendant did not protect the files containing the pornographic images and video clips by any means when he saved them to the hard drive. As set forth herein, the username, password, and/or codes only denied Cassie Morgan access to the Internet and the news reader group website from which the defendant downloaded the child pornography. Once Defendant saved the files from the Internet to

the computer's hard drive, the files had no password protection and Cassie Morgan had unfettered access to them. Moreover, even assuming *arguendo* that Defendant may have saved the files to the hard drive unintentionally, the files were not protected.

The facts herein are much more analogous to those in *United States v. Smith*, 27 F.Supp.2d 1111, 1115 (C.D. Ill. 1998), which upheld a search of a defendant's computer files based on third-party consent. In *Smith*, the defendant's housemate consented to a search of the defendant's computer, which was located in an alcove in the housemate's bedroom. The court found that the housemate had the necessary joint control and access to the computer and its surrounding area because the computer was accessible to all members of the household, it had been used by the housemate's daughter, and the defendant had tried to teach the housemate to use it. (*Id.* at 1115-16) Because the files containing images of child pornography were not password protected, the court upheld the third-party consent. *(Id.* at 1116) (third party with shared access to a computer may consent to the search of all the files on the computer that are *not protected* by individualized passwords).

For these reasons, the Court concludes that Cassie Morgan had both actual and apparent authority to consent to a search of the computer in this case. Accordingly, the Court upholds the consent search of Defendant's computer.

Cassie Morgan was not acting as a government agent when she installed the "spy-ware" software on Defendant's computer and captured certain screen images.

The Fourth Amendment proscribes only governmental action and does not apply to a search and seizure, even an unreasonable one, conducted by a private individual not

acting as an agent of the government or with the participation or knowledge of any governmental official. *United States v. Jacobsen*, 466 U.S. 109 (1984)

In *Jacobsen*, employees of Federal Express examined the inside of a damaged package and found a series of four (4) zip-lock plastic bags, the innermost of which contained a quantity of white powder. The employees re-wrapped the package and notified DEA agents. When DEA agents arrived, the box was still wrapped but its top was open and a hole was punched in its side. Without obtaining a warrant, the agents removed the plastic bags and then removed a small amount of the white powder for testing. A field test revealed that the substance was cocaine. Later, agents re-wrapped the package and obtained a warrant to search the place to which it was addressed. 466 U.S. at 111-12

The Supreme Court held that the agents' viewing of what a private party had freely made available for their inspection was not a "search" within the meaning of the Fourth Amendment. *Id.* at 119-120. The Supreme Court reasoned that defendants could have no privacy interest in the contents of the package since it had just been examined by employees of Federal Express and remained unsealed. *(Id.)* The removal of the plastic bags and their visual inspection by DEA agents revealed nothing more than what had previously been revealed by the private search. *(Id.* at 120) The Court further held that while the agents did "seize" the package, their warrantless seizure was not unreasonable under the Fourth Amendment given the fact that the plastic bags contained contraband and little else. *(Id.* at 120-21) The Court went on to analyze the field test separately, and concluded that a chemical test which merely reveals whether or not a substance is cocaine does not infringe upon any legitimate privacy interest. (*Id.* at 122-23)

The Sixth Circuit has held that "a person will not be acting as a police agent merely

because there was some antecedent contact between that person and the police. Rather two criteria must be shown. First, the police must have instigated, encouraged or participated in the search. Second, the individual must have engaged in the search with the intent of assisting the police in their investigative efforts." *United States v. Lambert*, 771 F.2d 83, 88 (6th Cir. 1985), *cert. denied*, 474 U.S. 1034 (1985) (citations omitted) Neither criteria are satisfied here. *See also United States v. Runyan*, 275 F.3d 449, 464 (5th Cir. 2001) (police examination of the same pornographic images which were obtained via private search constitutionally permissible).

In this case, Cassie Morgan was not acting on behalf of the government when she installed the "spy-ware" and captured images from the computer screen in her capacity as a private citizen. There is no evidence that the BCSD, through either Captain Prindle or Detective Lavender, instigated, encouraged or participated in Mrs. Morgan's installation or use of the "spy-ware" software. The first contact she had with the BCSD was November 28, 2001. *Statement of Facts* at ¶ 1 Moreover, Mrs. Morgan lacked the requisite intent. As she explained, her motivation for installing the “spy-ware” software had nothing to do with assisting law enforcement. Rather, she installed the "spy-ware" software because she suspected her husband was viewing child pornography. *(Id.*)

For these reasons, Mrs. Morgan's use of the "spy-ware" software to capture images was a private search that did not implicate the Fourth Amendment. Accordingly, Captain Prindle’s viewing of the “spy-ware” images captured by her did not violate Defendant’s Fourth Amendment rights.

One final matter deserves comment. In his brief, Defendant argues that he "protected" the pornographic images from his wife by deleting them from the hard drive.

In support of this argument, Defendant points out that he installed an "Internet Eraser" software program to delete any images he had downloaded. This argument is without merit. By attempting to delete the images, Defendant relinquished any expectation of privacy he had in the images themselves. *See California v. Greenwood*, 486 U.S. 35, 37 (1988) (defendant has no reasonable expectation of privacy in his curb-side trash). Moreover, Defendant's unsuccessful attempt to delete the images from the hard drive did not create a separate expectation of privacy. *See Commonwealth v. Copenhefer*, 587 A.2d 1353 (Penn. 1991)

In this case, by attempting to delete the pornographic images, Defendant was in essence, attempting to throw out the files. In that regard, the facts are similar to *Greenwood* and its progeny. For these reasons, the Court concludes that Defendant's relinquishment of any reasonable expectation of privacy in the pornographic images by attempting to delete the images is an alternative basis for denying the suppression motion.

Therefore, for the reasons stated herein,

IT IS ORDERED as follows:

1. The defendant's motion to suppress evidence (Doc. # 11) is **DENIED**;
2. This matter is set for a **Status Conference** on **October 22, 2003 at 10:00 a.m.**, U.S. Courthouse, Covington, Kentucky, at which time the Court will schedule this matter for trial;
3. The time period from April 29, 2003 through the date of this Order, totaling 170 days, is deemed **excludable time** pursuant to Title 18, United States Code § 3161(h)(1)(F).

This 15th day of October, 2003.

Signed By:
David L. Bunning
United States District Judge

G:\DATA\Opinions\2-03-25-MOO-suppression-motion.wpd