IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA, Plaintiff,	)	**CRIMINAL ACTION**
v.	)	No. 05-10254-01-MLB
STEVEN C. PERRINE, Defendant.	)	

MEMORANDUM AND ORDER

This case comes before the court on a number of motions filed by defendant, along with various response and reply briefs:

A. Defendant's motion to dismiss certain counts based on the Commerce Clause, and the government's response. (Docs. 14, 24.)

B. Defendant's motion to dismiss certain counts based on the statute of limitations, and the government's response. (Docs. 15, 23.)

C. Defendant's motion to dismiss certain counts based on outrageous government conduct, and the government's response. (Docs. 16, 26.)

D. Defendant's motion to dismiss certain counts based on the Confrontation Clause, and the government's response. (Docs. 17, 28.)

E. Defendant's motion to dismiss certain counts based on the Eighth Amendment, and the government's response. (Docs. 18, 25.)

F. Defendant's motion to suppress personally

identifiable information, the government's response, defendant's reply, and supplemental briefs from both parties. (Docs. 19, 29, 30, 35, 36.)

The court held a hearing on May 3, 2005. At that hearing, defendant chose to limit his presentation of evidence to that establishing his standing to bring a motion to suppress evidence seized pursuant to a warrant. (Doc. 19.) The only evidence received was limited testimony by defendant, along with two court orders from a Pennsylvania state court directing two internet companies to disclose subscriber identifying information that ultimately led law enforcement personnel to defendant, and a search warrant affidavit and two search warrants from a Kansas state court. The balance of the hearing was devoted to argument by the parties.

Under the government's version of the facts,[1] this case began in Pennsylvania, on or about September 2, 2005, when an individual reported to local authorities that he saw child pornography in a Yahoo! chat room. The complainant, Mr. James Vanlandingham, reported that he entered a Yahoo! chat room and began a chat with an unknown person using the Yahoo! screen name "stevedragonslayer." Vanlandingham reported that stevedragonslayer invited Vanlandingham to watch a webcam video that appeared to depict two female children who were walking around a bathroom in the nude.

Vanlandingham claimed that he immediately contacted local police officials about the incident. While waiting for police to arrive,

[1] Most of these facts are derived from an affidavit filed in support of a search warrant in Kansas state court. At the hearing, the government provided a copy of the affidavit, which is dated December 22, 2005.

Vanlandingham stayed online and continued to chat with stevedragonslayer. He asked if stevedragonslayer had more videos, to which the latter replied that he did not know what might offend Vanlandingham. Vanlandingham responded that he liked "the young hard stuff," after which stevedragonslayer played a number of video clips that showed children engaged in various explicit sexual acts.

Stevedragonslayer stopped sending video clips prior to police arriving at Vanlandingham's home; however, Vanlandingham was able to preserve a record of the chat conversation. Based on Vanlandingham's account of these events, Pennsylvania law enforcement obtained a court order directing Yahoo! Inc. to provide the subscriber information for the screen name "stevedragonslayer." These records showed that stevedragonslayer logged into Yahoo! from the IP address 68.103.177.146. Further investigation revealed that this IP address was maintained by Cox Communications, Inc. Pennsylvania authorities then obtained a second court order directing Cox Communications, Inc. to provide the subscriber information for that IP address. Cox reported that the Yahoo! logins from this particular IP address at the times reported by Yahoo! were associated with an account belonging to Steve Perrine, 11944 Rolling Hills Court, Wichita, KS 67212-5157.

Armed with this identifying information, Pennsylvania authorities contacted Kansas law enforcement. The Wichita Police Department (WPD) then took over the investigation. Further research showed that Steve Perrine had a prior state conviction for sexual exploitation of a child and was then on probation. A WPD detective sought and obtained a search warrant for defendant's home. The search was apparently conducted on December 22, 2005. In addition to seizing

defendant's computer, police also found firearms and drug paraphernalia. Accordingly, they obtained an amended search warrant authorizing them to seize those items as well. The government contends that forensic examination of defendant's computer revealed legions of images depicting child pornography. Furthermore, defendant testified at the hearing that he was, in fact, stevedragonslayer.

Defendant is charged in a six-count superseding indictment with various offenses related to distribution, receipt, and/or possession of child pornography, as well as being a felon in possession of a firearm. (Doc. 12.) The indictment also includes forfeiture counts for computer equipment and firearms associated with the other charged crimes. Defendant filed a number of motions seeking to dismiss certain counts in the indictment or otherwise limit the government's presentation of evidence.

Following the hearing, while evaluating the motions and briefs, the court noted that defendant had raised additional arguments in a reply brief. (Doc. 30.) This brief was filed the day before the hearing, and new arguments raised therein were not addressed at the hearing. Uncertain of whether the government was even aware, at the time of the hearing, that these new matters had been raised, the court directed additional briefing and scheduled another evidentiary hearing. (Doc. 33.) The additional briefing has been received and, finding no need for another hearing, the evidentiary hearing scheduled for May 30, 2006, is hereby cancelled. (Docs. 35, 36.) Defendant's motions are denied for reasons set forth herein.

A. Commerce Clause

In this motion, defendant presents an as-applied challenge to

his prosecution under 18 U.S.C. § 2254, claiming that under the facts of this case, his activities lie beyond the scope of Congress' authority under the Commerce Clause. (Doc. 14 at 4.) Defendant bases this argument on the circumstances surrounding his prior state conviction for sexual exploitation of a child, K.S.A. 21-3516(a)(2). Id. at 2. Defendant claims that over a year-and-a-half after his computer was seized in relation to the state charges, the state returned his computer without erasing the images of child pornography contained on its hard drive. Id.

Based on these alleged facts, defendant argues that the transfer of the computer from state authorities to himself was non-economic, intrastate activity that lies beyond the bounds of Congress' authority to circumscribe under the Commerce Clause. Id. at 3-4. Accordingly, defendant argues, he cannot now be prosecuted under 18 U.S.C. § 2252 based on his having child pornography on this same computer because the computer was transferred to him outside the stream of commerce. Id.

Defendant mistakenly focuses on the wrong object in evaluating the relationship of his activities to interstate commerce. The government's brief and the evidence presented at the hearing make clear that the focus of any Commerce Clause inquiry must not be directed toward defendant's computer, but rather at the images contained therein. The government's evidence suggests that defendant was engaged in the receipt, distribution, and possession of child pornography over the internet after he received his computer back from state officials. The facts suggest that these images traveled in interstate commerce, and would therefore fall well within Congress'

Commerce Clause authority to regulate or prohibit. See also United States v. Grimmett, 439 F.3d 1263, 1273 (10th Cir. 2006) (even totally intrastate production of child pornography was within Congress' Commerce Clause power to proscribe under 18 U.S.C. § 2251). Since defendant does not raise an issue as to pornographic images that he received, distributed, and/or possessed after he received his computer back from state officials, the court need go no further in its analysis. Defendant's motion to dismiss is DENIED.

B. Statute of Limitations

Defendant next asserts that the statute of limitations bars his prosecution on the child pornography counts. Unfortunately, neither defendant nor the government cited any case law for their respective interpretations of the statutes governing this issue. Instead the two sides spar over whether the limitations period is governed by 18 U.S.C. § 3282 or § 3283. Section 3282 provides, in relevant part, as follows:

> Except as otherwise expressly provided by law, no person shall be prosecuted, tried, or punished for any offense, not capital, unless the indictment is found or the information is instituted within five years next after such offense shall have been committed.

Id. § 3282(a). By its own terms, this section applies to all non-capital offenses, except those for which Congress has expressly provided a different limitations period. This version of section 3282 became effective on April 30, 2003; however, the prior version was identical in all material respects. The date is relevant because Count 3 of the superseding indictment charges conduct that may have occurred as early as March 1, 2003 - two months before this statute

was amended.

The version of section 3283 in effect from April 30, 2003 through January 4, 2006, read as follows:

> No statute of limitations that would otherwise preclude prosecution for an offense involving the sexual or physical abuse, or kidnaping, of a child under the age of 18 years shall preclude such prosecution during the life of the child.

Prior to April 30, 2003, section 3283 read:

> No statute of limitations that would otherwise preclude prosecution for an offense involving the sexual or physical abuse of a child under the age of 18 years shall preclude such prosecution before the child reaches the age of 25 years.

Thus, the only material change between these two versions is that prior to April 30, 2003, section 3283 ensured that the limitations period would not expire prior to the child victim's twenty-fifth birthday, while the later version extended the limitations period throughout the life of the child.

Defendant argues that the child pornography counts are governed by section 3283, while the government counters that section 3282 controls. In particular, the government asserts, without authority, that section 3283 only applies to "contact offenses," but that defendant in not charged with a "contact offense." (Doc. 23 at 2.) Defendant asserts that, since section 3283 controls, the government must prove that any alleged minor victims have not attained age twenty-five and/or that they are still alive.

The court finds that it need not resolve whether section 3283 could apply in this case. The plain language of that section makes clear that it does not supplant any other statute prescribing a limitations period. Instead, section 3283 merely acts to ensure that,

regardless of any other applicable limitations period, in no event will the limitations period run prior to a child victim's twenty-fifth birthday (for the older version) or prior to a child victim's death (in the case of the newer version). In other words, section 3283 extends, but does not replace, any other applicable limitations period. See United States v. Jeffries, 405 F.3d 682, 683 (8th Cir. 2005). Accordingly, section 3282 provides the relevant limitations period for the crimes charged in the indictment. Since all the charged activity occurred less than five years prior to the indictment, prosecution is not barred thereby. Defendant's motion on this point is DENIED.[2]

C. Outrageous Government Conduct

Defendant asserts that, in 2003, after he was sentenced on his state conviction for Sexual Exploitation of a Child, law enforcement returned his computer without erasing the images containing child pornography. (Doc. 16 at 2.) He claims that the government therefore took advantage of his "addiction" to child pornography, thereby inducing him to participate in the criminal acts with which he is now charged. Id. at 3.

Defendant bears the burden of proving the defense of outrageous

[2] In the last paragraph of his motion, defendant asserts that "[t]o the extent that the definition of 'identifiable minor' excuses the Government from proving the actual identity of an identifiable minor, 18 U.S.C. § 2256(9)(B) prevents this Court from exercising jurisdiction in this matter." The court fails to see how this argument flows from any other part of defendant's motion. Nevertheless, section 2256(9)(B) expressly contradicts defendant's assertion. Section 2256(9)(B), which defines the term "identifiable minor" specifically states that it "shall not be construed to require proof of the actual identity of the identifiable minor." The court finds no jurisdictional bar in this language.

government conduct. United States v. Pedraza, 27 F.3d 1515, 1521 (10th Cir. 1994). In order to do so, he must show "that the challenged conduct violates notions of 'fundamental fairness' and is 'shocking to the universal sense of justice.'" Id. (quoting United States v. Harris, 997 F.2d 812, 816 (10th Cir. 1993)). Proof of this defense requires defendant to prove either: "(1) excessive government involvement in the creation of the crime, or (2) significant governmental coercion to induce the crime." Id. Excessive government involvement in the creation of a crime requires the government to engineer and direct the criminal enterprise from beginning to end. Id. While less specific, significant government coercion only occurs when the coercive acts of government agents are particularly egregious. Id. Application of this defense is to be decided by the court, not a jury.[3] United States v. Mosley, 965 F.2d 906, 909 n.3 (10th Cir. 1992). Ultimately, the question is whether, under the totality of the circumstances, the government's conduct was sufficiently egregious to violate due process. See Pedraza, 27 F.3d at 1521.

Implicit in the elements of a defense of outrageous government conduct is the requirement that the challenged conduct be done intentionally. See United States v. Ayeki, 289 F. Supp. 2d 183, 190 n.2 (D. Conn. 2003); United States v. Schneider, 157 F. Supp. 2d 1044, 1065 (N.D. Iowa 2001). Without evidence that government conduct was

[3] Unless defendant can show that the government's failure to erase these images from his computer is relevant to some other issue in this case, he will not be permitted to protract the trial or otherwise risk confusing the jury by presenting evidence on this point to the jury. Fed. R. Evid. 401, 402.

done intentionally, rather than through neglect or incompetence, it is difficult to conceive of a set of circumstances in which such activity was rise to the level of "shocking . . . the universal sense of justice." Harris, 997 F.2d at 816.

In this case, the government maintains that, while the failure to erase the child pornography from defendant's computer was improper, it was unintentional. Indeed, returning these images to defendant was probably negligent, even incompetent; however, defendant has failed to make any showing that any government official acted intentionally in leaving the images on his computer. Accordingly, the court finds that this conduct does not rise to a level which would be fundamentally unfair or otherwise shock anyone's sense of justice. There is certainly no evidence that the government engineered and directed the charged crimes from beginning to end. Likewise, there is nothing so egregious about the challenged mistakes that would support a finding of governmental coercion.

Moreover, the government asserts that it will not use any of these images as evidence in this case. Instead, the government will only present evidence on images and video clips received and distributed after defendant received his computer back from the state. The government's position is generally consistent with the indictment, wherein Counts One and Two charge defendant with distribution and receipt of child pornography after November 20, 2003, the date defendant's computer was returned by the state. By contrast, Count Three charges defendant with possession of child pornography as early as March 1, 2003. This count has the potential to take in images defendant possessed prior to the return of his computer.

Nevertheless, the government conceded in its response that "[t]he present charges are for criminal conduct occurring after the computer and its contents were returned to the defendant, sometime after November 20, 2003." (Doc. 26 at 7.) Therefore, despite the fact that the indictment charges conduct dating back as far as March 1, 2003, the court will not permit the presentation of evidence that defendant possessed child pornography on the computer returned by the state prior to November 20, 2003. As the underlined phrase suggests, this would not preclude the government from presenting evidence that defendant possessed child pornography on some other computer, or in some other form of media, as far back as the date charged in Count Three. In sum, defendant's motion to dismiss on the basis of outrageous government conduct is DENIED. However, the court will limit the admission of evidence pre-dating the return of defendant's computer, as previously described.

D. Confrontation Clause

While defendant's argument on this motion was somewhat ambiguous as expressed in his brief, he clarified his position at the hearing. In a nutshell, defendant argues that under Ashcroft v. Free Speech Coalition, 535 U.S. 234, 122 S. Ct. 1389, 152 L. Ed. 2d 403 (2002), the government must prove the actual identity of any alleged minors depicted in pornographic images he is alleged to have possessed, distributed, or received. He further argues that, if the government fails to find the actual minors shown in these images, and fails to require them to testify under oath and subject to cross-examination that they are, in fact, the persons shown in any pornographic images, then defendant's Confrontation Clause rights, as further clarified in

Crawford v. Washington, 541 U.S. 36, 124 S. Ct. 1354, 158 L. Ed. 2d 177 (2004), will be violated.

Defendant's initial premise, that the government must prove the actual identity of any children depicted in allegedly pornographic images has been soundly rejected in this circuit.

> [O]ur cases since Free Speech Coalition have consistently held that juries can review the images themselves to determine whether real children are depicted. Indeed, in United States v. Kimler, 335 F.3d 1132 (10th Cir. 2003), cert. denied, 540 U.S. 1083, 124 S. Ct. 945, 157 L. Ed. 2d 759 (2003), we considered a defendant's challenge to his conviction under the same statute at issue here on the ground that Free Speech "requires either direct evidence of the identity of children in the proscribed images or expert testimony that the images depicted are those of real children rather than computer generated 'virtual' children." Id. at 1140. The Government had introduced only the e-mails and images retrieved from the defendant and his computer. Id. at 1135-36. We concluded:
>
> > Free Speech Coalition, did not establish a broad, categorical requirement that, in every case on the subject, absent direct evidence of identity, an expert must testify that the unlawful image is of a real child. Juries are still capable of distinguishing between real and virtual images; and admissibility remains within the province of the sound discretion of the trial judge.
>
> Id. at 1142.
>
> . . . .
>
> Therefore, we hold that the Government has the burden of proving beyond a reasonable doubt that the images at issue in a § 2252 prosecution depict actual minors. However, this does not necessarily require expert testimony or identification of the actual child victims. See Kimler, 335 F.3d at 1142. Instead, juries often will be able to distinguish between real and virtual images, and "where no evidence suggests that the images are anything other than real, the government need offer no supporting evidence

> beyond the images themselves." Harms, 371 F.3d at 1213.

United States v. Sims, 428 F.3d 945, 956-57 (10th Cir. 2005).

Although defendant's argument regarding the method the government must employ to prove that any pornographic images contain real children has not found favor in the courts of appeal, his Confrontation Clause argument attacks the issue from a new direction. He argues that

> [a]ny identification of the alleged "minors" involved constitutes testimony about which Defendant has not been provided an opportunity to cross-examine, is not reliable, as defined by Crawford, and any use thereof, or reference thereto, must be suppressed and held inadmissible.

(Doc. 17 at 2.) Defendant cites no authority for this extension of Crawford.

The court rejects defendant's proposed application of Crawford. As the Supreme Court did in that case, the court begins with the text of the Confrontation Clause: "In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him." U. S. Const. Amend. VI. Elaborating on this clause, the Supreme Court concluded that it entitled a criminal defendant to have an opportunity for cross-examination in the case of testimonial statements made by witnesses against him. Crawford, 541 U.S. at 59, 124 S. Ct. at 1369.

Moving straight to the nub of this issue, photographs are not statements. See Simmons v. United States, 390 U.S. 377, 387, 88 S. Ct. 967, 973, 19 L. Ed. 2d 1247 (1968). Alternatively, even if a photograph or similar image containing child pornography could

arguably be considered a statement, it would undoubtedly be a statement by the photographer, not the children.[4] By contrast, defendant wants to confront the children depicted in the images. The children are not witnesses against him; therefore, he has no right to confront them. Instead, the images speak for themselves. The Confrontation Clause affords no bar to the government's introduction of these inanimate objects any more than it would bar the introduction of a gun to show that a defendant was a felon in possession of a firearm (which, presumably, the government will do in this case). Defendant's motion is DENIED.

E. Eighth Amendment

Defendant also contends that punishing him for possessing the images returned to him by the government violates the Eighth Amendment. (Doc. 18.) Rights associated with the Eighth Amendment do not attach until conviction. See Graham v. Connor, 490 U.S. 386, 395 n.10, 109 S. Ct. 1865, 1871 n.10, 104 L. Ed. 2d 443 (1989); Berry v. City of Muskogee, Okla., 900 F.2d 1489, 1493 (10th Cir. 1990). Any Eighth Amendment claim would be premature because it is as yet uncertain if defendant will be convicted and, if so, what his punishment would be. Defendant's motion is accordingly DENIED.

F. Motion to Suppress

1. Arguments Raised in Defendant's Initial Motion

[4] While photographs, in general, may attempt to convey some manner of statement by either the photographer or the subject of the photo, the only "statement" relevant to these proceedings is whether the images show actual minors engaged in sexual activity. Whatever "statements" defendant may argue such images convey, the court absolutely rejects the argument that they intend to make any statement regarding the age or existence of the children depicted therein.

Defendant seeks to suppress all evidence seized at his residence, as well as the subscriber identification evidence obtained from Yahoo! and Cox Communications. (Doc. 19.) He reasons that police obtained his subscriber identification information in contravention of the Cable Communications Policy Act (CCPA), 47 U.S.C. § 551, and the Fourth Amendment. He further claims that this information was instrumental in leading law enforcement officers to his home and justifying the warrant supporting a search of the residence. Accordingly, he argues, all this evidence is "fruit of the poisonous tree," and must be suppressed. (Doc. 19 at 3.)

As the government notes, however, the CCPA authorizes disclosure of this type of subscriber information to government entities as authorized by Chapters 119, 121, or 206 of Title 18. 47 U.S.C. § 551(c)(2)(D). Under Chapter 121 of Title 18, section 2703 prescribes a number of procedures by which government entities, federal or state, may obtain the type of information at issue here. There is some question as to the exact procedure used; however, the matter is irrelevant because, even assuming a defect in the procedure used to obtain the court orders which directed Yahoo! and Cox Communications to provide defendant's subscriber information, suppression of the evidence is not a remedy available for such a violation. Instead, 18 U.S.C. § 2708 provides, "The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." In turn, the available remedies are described in section 2707 as including a civil action against violators other than the United States, and administrative discipline against federal employees under certain circumstances. By

contrast, Chapter 121 never suggests that suppression of such evidence in a criminal prosecution is an available remedy. United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

Reading Chapter 121 as a whole, the logical conclusion to be drawn from the use of the phrase "nonconstitutional violations of this chapter" in section 2708 is that any constitutional violations should be evaluated under the relevant constitutional standards. Thus, in this case, in order to suppress evidence, defendant must show that it was seized through a Fourth Amendment violation. However, the identifying information at issue here - defendant's name, address, etc. - was information that he voluntarily transmitted to the third-party internet service providers, Cox and Yahoo!. Indeed, defendant also admitted at the hearing that he had enabled peer-to-peer file sharing on his computer, thereby giving anyone with internet access the ability to gain entrance to his computer. Under such a scenario, a defendant holds no reasonable expectation of privacy that the Fourth Amendment will protect. Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001); Kennedy, 81 F. Supp. 2d at 1110.

2. New Arguments Raised in Defendant's Reply Brief

As an alternative basis for suppression, defendant argues that Vanlandingham, a private citizen, became a government actor when he contacted police while attempting to obtain additional information from stevedragonslayer. (Doc. 30 at 6.)

> The Tenth Circuit applies a two part test in determining when a search by a private individual becomes government action: "1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party

> performing the search intended to assist law enforcement efforts or to further his own ends." Pleasant v. Lovell, 876 F.2d 787, 797 (10th Cir. 1989). Both inquiries must be answered in the affirmative before an otherwise private search will be deemed governmental for Fourth Amendment purposes. See United States v. Leffall, 82 F.3d 343, 347 (10th Cir. 1996).

Kennedy, 81 F. Supp. 2d at 1112. Defendant has the burden of proof on this point. Id.

Defendant has utterly failed to put forth any evidence to establish the first element of this test. Even relying on the search warrant affidavit that chronicled Vanlandingham's encounter with stevedragonslayer, there is not even a hint that law enforcement was aware that Vanlandingham was attempting to elicit more information or evidence from defendant until after the officer arrived at Vanlandingham's house. By that time, the online encounter was over. Thus, defendant is not entitled to relief on this theory.

Next, defendant asserts that the warrant authorizing the search of his computer was overly broad because it failed to limit the scope of the computer search to evidence of specific crimes or specific types of material. (Doc. 30 at 9.)

The Fourth Amendment to the United States Constitution 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.

The particularity requirement ensures that the search is as limited as possible, and was intended to prevent the wide-ranging,

"exploratory rummaging" of a "general search," which the colonists abhorred. United States v. Foster, 100 F.3d 846, 849 n.3 (10th Cir. 1996) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467, 91 S. Ct. 2022, 2038, 29 L. Ed. 2d 564 (1971)). Government agents may only seize items that are described in the warrant, and "nothing is left to the discretion of the officer . . . ." Id. at 849.

> [A] warrant's description of things to be seized is sufficiently particular if it allows the searcher to reasonably ascertain and identify the things authorized to be seized." United States v. Finnigin, 113 F.3d 1182, 1187 (10th Cir. 1997) (omitting quotations and citations). Further, the warrant must leave nothing to the officer's discretion as to what is to be seized, so that the officer is prevented from generally rummaging through a person's belongings. See Lawmaster v. Ward, 125 F.3d 1341, 1347-48 (10th Cir. 1997).

United States v. Hargus, 128 F.3d 1358, 1362 (10th Cir. 1997). The scope of a warrant is sufficiently limited to satisfy constitutional concerns when it

> "allow[s] the executing officers to distinguish between items that may and may not be seized." Finnigin, 113 F.3d at 1187 (quoting United States v. Leary, 846 F.2d 592, 602 (10th Cir. 1988)). "Even a warrant that describes the items to be seized in broad or generic terms may be valid when the description is as specific as the circumstances and the nature of the activity under investigation permit." Davis [v. Gracey], 111 F.3d [1472,] 1478 [10th Cir. 1997] (internal quotations omitted).

Id. at 1362-63. In evaluating a search warrant for compliance with the particularity requirement, the court considers the warrant as a whole, rather than reading particular parts in isolation. United States v. Conley, 4 F.3d 1200, 1208 (3d Cir. 1993) ("[T]he phrases in a search warrant must be read in context and not in isolation."); see also Andresen v. Maryland, 427 U.S. 463, 480-81, 96 S. Ct. 2737,

2748-49, 49 L. Ed. 2d 627 (1976); United States v. Artez, 389 F.3d 1106, 1115 n.5 (10th Cir. 2004); United States v. Robertson, 21 F.3d 1030, 1033-34 (10th Cir. 1994).

The relevant parts of both the original search warrant and the amended warrant authorized the search and seizure of the following items:

> 1. Any unknown computer which consists of any equipment which can collect, analyze, creates, display, convert, store, conceal, or transmit electronic, magnetic, optical, or devices (such as central processing units and memory typewriters); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, CD-ROM drives and disks, DVD drives and disks, optical storage devices, and other memory storage devices); and related communications devices (such as modems, cables and connections, recording equipment, which may be, or is used to generate communication with others regarding child exploitation or the production,, possession or distribution of child pornography as described in K.S.A. 21-3516.
>
> . . . .
>
> 3. Any and all documentation in any form, including, electronically stored material of the production, possession, or distribution or [sic] child pornography as described in K.S.A. 21-3516.
>
> . . . .
>
> 6. Any and all documentation in any form, including, but not limited to recorded, or electronically stored material which explain or state co conspirators of the production, possession, or distribution or [sic] child pornography as described in K.S.A. 21-3516.
>
> . . . .
>
> 8. To forensically process and search in a controlled setting all electronic media, including but not limited to internal and peripheral storage devices such as fixed disks, external hard disks, floppy disks, and other

> memory storage devices for the purpose of viewing and/or retrieving for evidentiary purposes all data including electronic images, documents and stored electronic communications.

(Doc. 35 exhs. E, G.)

Defendant argues that paragraph 8 authorized an unrestricted search of all defendant's computers for anything and everything, thereby violating the particularity requirement of the Fourth Amendment. (Doc. 30 at 9-10.) More specifically, defendant argues that paragraph 8 runs afoul of the rules set forth for computer search warrants by United States v. Carey, 172 F.3d 1268 (10th Cir. 1999), and its progeny. Id. The government counters that, reading paragraphs 1, 3, 6, and 8 in context, it is clear that the warrant only authorized a search for child pornography. (Doc. 35 at 6-7.)

If the court were to only consider paragraphs 1 and 8, defendant's argument might have merit. Although paragraph 1 only authorizes seizure of computer equipment that can be used to create, receive, or distribute child pornography, as a practical matter, that pretty much encompasses any computer (or at least all those with an internet connection). Thereafter, paragraph 8, read literally, would authorize a wholesale rummaging of the entire contents of any computer seized pursuant to paragraph 1. This would clearly violate the rules requiring specificity with regard to the search of a computer hard drive. See United States v. Brooks, 427 F.3d 1246, 1251-52 (10th Cir. 2005) (summarizing the Carey line of cases).

However, paragraphs 1 and 8 are not the only ones relating to the government's search of defendant's computer. Paragraph 3 specifically authorizes the government to search for "[a]ny and all

documentation in any form, including, electronically stored material of the production, possession, or distribution or child pornography as described in K.S.A. 21-3516." Similarly, paragraph 6 authorizes a search of the same types of media for evidence that might identify co-conspirators in the production, possession or distribution of child pornography. These two paragraphs are sufficiently particular to satisfy the Fourth Amendment standards for computer searches set forth by the Tenth Circuit. United States v. Campos, 221 F.3d 1143, 1147-48 (10th Cir. 2000) (approving of a search warrant authorizing seizure of computer equipment "which may be, or [is] used to visually depict child pornography, child erotica, information pertaining to the sexual activity with children or the distribution, possession, or receipt of child pornography, child erotica or information pertaining to an interest in child pornography or child erotica."). Moreover, the court finds that "documentation in any form, including, electronically stored material" encompasses images and videos of child pornography contained on electronic media. See United States v. Pendergrass, 1995 WL 56673, *2 (4th Cir. Feb. 7, 1995) (term "documents" in a search warrant includes photographs); United States v. Tabares, 951 F.2d 405, 408 (1st Cir. 1991) (term "records" in a search warrant includes photographs).

Accordingly, the court concludes that paragraph 8 does not authorize the government to search or seize any items not already specified in other parts of the warrant. Instead, paragraph 8 merely makes clear that the government intends to remove the computer from the residence and perform a forensic search in a laboratory setting. Construed in that manner, the warrant satisfies the Fourth Amendment's

particularity requirements. There has been no suggestion that the scope of the actual search went beyond that which was authorized by the other parts of the warrant, and paragraphs 1, 3, and 6, in particular. Accordingly, defendant's motion to suppress on this basis is denied.

Alternatively, even if paragraph 8 could only be interpreted to authorize an unrestricted search of defendant's computer, the remedy would be controlled by United States v. Brown, 984 F.2d 1074 (10th Cir. 1993), where the court of appeals said,

> At issue in this case is the effect of the language in each of the two warrants quoted in part above (Warrants I and II). Each of these warrants described, with specificity, some items to be searched or seized, but added an authorization to search or seize other items which the officers determined or reasonably believed to be stolen. Mr. Brown argues that this language renders the warrant unconstitutionally broad.
>
> We find United States v. LeBron, 729 F.2d 533 (8th Cir. 1984) instructive. There, a warrant authorized a search for a list of specific items as well as for "other property, description unknown, for which there exists probable cause to believe it to be stolen." Id. at 536. That language, the court found, was not descriptive and did not adequately limit the discretion of the officers. Id. at 536. The instant warrant contained language very similar to the LeBron warrant.
>
> However, as in LeBron, the questionable portion of the warrant may be severed. "'[T]he infirmity of part of a warrant requires the suppression of evidence seized pursuant to that part of the warrant . . ., but does not require the suppression of anything described in the valid portions of the warrant (or lawfully seized-on plain view grounds, for example-during their execution).'" LeBron, 729 F.2d at 537 n.2 (quoting United States v. Fitzgerald, 724 F.2d 633, 637 (8th Cir. 1983) (en banc), cert. denied, 466 U.S. 950, 104 S. Ct. 2151, 80 L. Ed. 2d 538 (1984)). At least eight circuits have held that where a warrant contains both specific as well as

> unconstitutionally broad language, the broad portion may be redacted and the balance of the warrant considered valid. See United States v. George, 975 F.2d 72, 79 (2d Cir. 1992); United States v. Blakeney, 942 F.2d 1001, 1027 (6th Cir. 1991), cert. denied, 502 U.S. 1035, 112 S. Ct. 881, 116 L. Ed. 2d 785 (1992); United States v. Holzman, 871 F.2d 1496, 1510 (9th Cir. 1989); Fitzgerald, 724 F.2d at 636-37; United States v. Riggs, 690 F.2d 298, 300 (1st Cir. 1982); United States v. Christine, 687 F.2d 749, 759-60 (3d Cir. 1982); In re Search Warrant Dated July 4, 1977, 667 F.2d 117, 130-33 (D.C. Cir. 1981), cert. denied, 456 U.S. 926, 102 S. Ct. 1971, 72 L. Ed. 2d 441 (1982); United States v. Cook, 657 F.2d 730, 734-35 (5th Cir. 1981). See also 1 Wayne R. LaFave & Jerold H. Israel, Criminal Procedure, § 3.4(f) at 229 (1984). In such cases, only those items confiscated under the overbroad portion of the warrant are suppressed. George, 975 F.2d at 79.

Id. at 1077-78 (footnotes omitted). "To make [Brown's] severability doctrine applicable the valid portions of the warrant must be sufficiently particularized, distinguishable from the invalid portions, and make up the greater part of the warrant." United States v. Naugle, 997 F.2d 819, 822 (10th Cir. 1993).

The court finds that, other than paragraph 8, the remaining disputed paragraphs of the warrant are sufficiently particularized, that they are easily distinguished from paragraph 8, and that they make of the greater part of the warrant, thereby satisfying the test articulated in Naugle. Therefore, the court finds that either of two redaction methods would make paragraph 8 valid under the Fourth Amendment. First, the court strikes the word "all" that immediately precedes "electronic media," and the word "all" that immediately precedes the word "data" in paragraph 8. With those modifications, paragraph 8 would even more clearly be construed as merely authorizing a particular method of searching electronic media for the items

described elsewhere in the warrant, and specifically in paragraphs 3 and 6. Alternatively, the court would strike paragraph 8 in its entirety. With that modification, paragraph 1 would still authorize seizure of computers that could be used for receipt, distribution, or possession of child pornography, and paragraphs 3 and 6 would authorize a search of those computers and other electronic media for evidence of child pornography.

Under any of the three approaches described above, the warrant would authorize the government to search defendant's computers for child pornography; and, under any of those approaches, the warrant would satisfy the Fourth Amendment's particularity requirement. Defendant's motion to suppress is accordingly denied on this point.[5]

3. New Arguments Raised in Defendant's Supplemental Brief

In his supplemental brief, defendant asserts that the government violated the Fourth Amendment when it "intercepted" communications between stevedragonslayer and Vanlandingham from a chat session on Yahoo!. (Doc. 36 at 3.) However, defendant misrepresents the facts on this point. The uncontroverted account of how the contents of this communication fell into the hands of law enforcement shows that Vanlandingham provided a transcript of the chat to Pennsylvania police officers. (Doc. 35 exh. D at 4-5.)

---

[5] In paragraph 12 of his motion to suppress, defendant also makes a particularity argument regarding the search warrant affidavit's failure to allege that defendant and Vanlandingham were logged onto Yahoo! at the relevant time. (Doc. 30 at 7-8.) This fact has nothing to do with the Fourth Amendment's particularity requirement. The Fourth Amendment merely requires that a warrant specify with particularity the places to be searched and the things to be seized. Facts regarding whether these two users were logged into Yahoo! at the same time are irrelevant to a determination of whether the warrant was sufficiently particular.

It is well settled that when a party to a conversation shares the contents of that conversation with police officers, the Fourth Amendment is not implicated. United States v. White, 401 U.S. 745, 749, 91 S. Ct. 1122, 1125, 28 L. Ed. 2d 453 (1971); Hoffa v. United States, 385 U.S. 293, 303, 87 S. Ct. 408, 414, 17 L. Ed. 2d 374 (1966); United States v. Longoria, 177 F.3d 1179, 1182-83 (10th Cir. 1999); United States v. Salisbury, 662 F.2d 738, 740 (11th Cir. 1981). Indeed, "[i]f a person knowingly exposes statements to the plain view of outsiders, such statements are not protected under the Fourth Amendment because the speaker has not exhibited an intention to keep them to himself;" and, "the Fourth Amendment offers no protection for a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." Longoria, 177 F.3d at 1182-83 (internal quotation marks omitted).

Under these principles, defendant bore the risk that Vanlandingham would reveal the contents of the Yahoo! chat to law enforcement. Any expectation of privacy defendant had in this communication was not objectively reasonable, and the Fourth Amendment provides him no relief on this point.

Much of the balance of defendant's supplemental brief is aimed at suppressing the identifying information obtained from Yahoo! and Cox. However, as already noted, the court finds that defendant had no objectively reasonable expectation of privacy in his subscriber information, thereby foreclosing remedies under the Fourth Amendment; and, the court finds that suppression is not an available remedy under Chapter 121 of Title 18 of the United States Code.

Besides his argument regarding his subscriber information,

defendant also asserts yet another new argument in his supplemental brief, and this despite the fact that the court directed that no new arguments should be set forth therein. (Doc. 33 at 3.) Nevertheless, since the government continues to disclose important evidence in bits and pieces, and since, for the first time in its supplemental brief, the government finally disclosed the affidavits supporting the applications for search warrants for defendant's residence, the court finds that defendant is entitled to challenge those warrants. Accordingly, the court will consider defendant's arguments.

Defendant argues that the warrants issued to search his residence (and a warrant issued by the same Kansas state court to Yahoo!) were supported by affidavits that failed to establish probable cause. (Doc. 36 at 11.) Defendant claims that the computer logs originally obtained from Yahoo! failed to show that stevedragonslayer was logged in on September 2, 2005 at the time Vanlandingham reported his chat with stevedragonslayer. Thus, defendant argues, Vanlandingham's veracity was placed in question to the point that his statement was not sufficient to support a conclusion that defendant was ever involved in such a conversation. Id. at 12-14.

In considering whether probable cause existed to justify issuance of a search warrant, the court begins with the following principles:

> If the search and seizure was done pursuant to a warrant, we review the issuing judge's finding of probable cause with great deference: we look to ensure that the judge "had a 'substantial basis' for concluding" that the affidavit in support of the warrant established probable cause. United States v. Cusumano, 83 F.3d 1247, 1250 (10th Cir. 1996). The issuing judge's task "is simply to make a practical, common sense decision whether,

> given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." Id.

Grimmett, 439 F.3d at 1268.

> A reviewing court is to interpret search warrant affidavits in a common sense and realistic fashion. United States v. Ventresca, 380 U.S. 102, 108, 85 S. Ct. 741, 13 L. Ed. 2d 684 (1965). The issuing judge is entitled to go beyond the averred facts and draw upon common sense in making reasonable inferences from those facts. United States v. Rowland, 145 F.3d 1194, 1205 (10th Cir. 1998). A reviewing court should uphold the warrant as long as the issuing judge had a "substantial basis for . . . conclud[ing] that a search would uncover evidence of wrongdoing." Illinois v. Gates, 462 U.S. 213, 236, 103 S. Ct. 2317, 76 L. Ed. 2d 527 (1983) (internal quotation marks omitted).

Id. at 1270.

In this case, the facts in the affidavit show that Vanlandingham not only reported his conversation with stevedragonslayer, but also provided police with a transcript of that chat. In addition, Vanlandingham affirmatively reported that stevedragonslayer broadcast to him multiple videos containing child pornography. This was enough to establish probable cause to believe that someone with the Yahoo! screen name "stevedragonslayer" possessed and distributed child pornography.

The fact that the Yahoo! logs fail to show that stevedragonslayer was logged in on September 2, 2005 at the relevant time is of no moment. A review of the logs shows that they simply do not go back that far in time. The earliest entry is for October 9, 2005. (Doc. 36 exh. H at 5.) It is unclear why the log stops here. Perhaps it is because the data is only retained as far back as that

date. Whatever the reason, the mere fact that these logs do not go back as far as September 2, 2005, does nothing to undermine the fact that Vanlandingham says the encounter occurred, and Pennsylvania authorities saw a transcript of the chat. Defendant's claim that inclusion of the Yahoo! logs would have resulted in a finding of no probable cause is accordingly rejected.

Having established probable cause to believe that stevedragonslayer was distributing child pornography, the affidavit next chronicles the efforts that linked that screen name with an IP address at Cox Communications that was associated with defendant's account. Cox also provided the subscriber information for that account, which included the address of defendant's residence in Wichita, Kansas. The affidavit further noted that defendant had a previous conviction for sexual exploitation of a child. (Doc. 35 exh. D at 5.) The court finds that this was enough to establish probable cause to believe that defendant possessed and distributed child pornography, and that evidence of this crime might be found on computers and related equipment at his home, and in his e-mail account.

Finally, defendant argues that the affidavits in support of the Kansas warrants failed to establish probable cause because some of the information contained in those affidavits was over three months old when the police applied for the search warrant. Accordingly, defendant argues, this information was too stale to support a finding of probable cause. (Doc. 36 at 13-14.)

"Whether information is stale depends on the nature of the criminal activity, the length of the activity, and the nature of the

property to be seized." United States v. Riccardi, 405 F.3d 852, 860-61 (10th Cir. 2005). However, a conclusion that once depended on statements in a search warrant application for support have now become so well-established in case law as to be appropriate for judicial notice: pedophiles are commonly known to hoard and retain their child pornography for long periods of time. See id. at 861 (collecting cases); see also United States v. Zimmerman, 277 F.3d 426, 434 (3d Cir. 2002) ("pedophiles rarely, if ever, dispose of child pornography"); United States v. Hay, 231 F.3d 630, 636 (9th Cir. 2000) (information six months old not stale when related to computer-based child pornography). The court finds that, although a three month delay might make information stale in certain types of cases, it was not such a long delay in the area of internet child pornography. It is well known that once information is placed on a computer, that information can remain there for a long time. See Grimmett, 439 F.3d at 1267 (search of computer hard drive revealed child pornography that had been produced over 18 months earlier). Indeed, in this very case defendant has expressed grave concerns that he might be prosecuted for possessing images of child pornography that were placed on his computer over three and a half years before his computer was seized in December of 2005. (Doc. 16 at 2.) Several of the counts in this case center around possession and distribution of child pornography over the internet. This process is highly dependent on computers, and there was no reason to believe that some evidence of this crime would not be found on the computers so involved when only three months had passed since the last known incident. Having disposed of this last argument, defendant's motion to suppress is therefore DENIED in its

entirety.

Based on the foregoing conclusions, the court finds no need for another evidentiary hearing. Therefore this case is set for trial beginning May 30, 2006 at 9:00 A.M.

IT IS SO ORDERED.

Dated this 18th day of May 2006, at Wichita, Kansas.

s/ Monti Belot
Monti L. Belot
UNITED STATES DISTRICT JUDGE