

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ALASKA**

UNITED STATES OF AMERICA,

Plaintiff,

v.

RANDY D. WINSLOW,

Defendant.

3:07-CR-00072-TMB-DMS

**ORDER REGARDING DEFENDANT'S  
MOTION FOR ORDER COMPELLING  
DISCOVERY OF COMPUTER-  
RELATED EVIDENCE SEIZED FROM  
RANDY D. WINSLOW  
[Doc. 31]**

**I. INTRODUCTION**

A computer was seized from Defendant Randy D. Winslow during the investigation of this matter. The defendant requests that a copy of the HP Pavillion hard drive seized from 109 East 5<sup>th</sup> Street, Tilton, Illinois, his home, be provided to defense counsel for review by a computer forensic expert. The Government contends that the hard drive contains images that constitute child pornography. The hard drive also allegedly contains evidence of on-line chats and emails between Winslow and an undercover officer, which are relied upon by the Government to prove a charge of attempted aggravated sexual abuse of a minor.

The defense requests that this discovery material be made available as it was in the past, pursuant to a detailed protective order that specified how the copied hard drive would be handled while in the possession of defense counsel for the purpose of discovery. (See U.S. v. Danny Michael Harvey, 3:07-CR-00103-RRB-DMS, Doc. 73-2, Affidavit of Bruce Johnson, Federal Public Defender Investigator, District of Alaska. The parties in this matter stipulated that the evidentiary record in Harvey on the issue of discovery could be incorporated into the record in

this matter. U.S. v. Winslow, Doc. 88, 90, 91). The precautions contained in the prior protective orders were taken to insure there was no further copying, viewing or distribution of the images, beyond that necessary to prepare the legal defense. The defense relies upon Fed. R. Crim. P. 16 and United States v. Hill, 322 F. Supp. 2d 1081 (C.D. Cal. 2004), in which the Court approved such a protective order.

The Government refuses to deliver the copy, arguing that the 2006 Adam Walsh Child Protection and Safety Act (hereafter the Walsh Act)—specifically 18 U.S.C. § 3509(m)—directs prosecutors and investigators in criminal cases to retain all child pornography in the Government’s care, custody and control. The Government argues that it will provide ample opportunity for the defense examination of the hard drive while in Government custody and, as a result, the Walsh Act prohibits the Court from ordering the Government to produce a copy of the hard drive for delivery to the office of defense counsel.

Winslow responds that 18 U.S.C. § 3509(m) is unconstitutional both facially and as applied in this case. He contends that he is entitled to copies of the hard drive under the Fifth Amendment’s Due Process clause and the Sixth Amendment’s Compulsory Process and Effective Assistance of Counsel clauses.

Other district courts around the country have considered whether this section of the Walsh Act is constitutional when applied to child pornography on a hard drive. No circuit courts have addressed the issue to date. Also, this Court has been unable to locate any precedent which addresses the constitutionality of Section 3509(m) of the Walsh Act when applied to a hard drive that contains not only child pornography but written emails and on-line chats from the defendant, which are relevant to a charge other than possession or distribution of child pornography.

## **II. STATEMENT OF FACTS**

In a superceding indictment August 24, 2007, Winslow was charged with attempted aggravated sexual abuse in violation of 18 U.S.C. § 2241(c) and distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1). Federal law enforcement agents arrested Winslow on May 4, 2007 in his Illinois home two weeks before he planned to travel to Alaska. Later that day, federal agents seized a computer and HP Pavillion hard drive from Winslow's Illinois home.

Prior to passage of the Walsh Act, in federal child pornography prosecutions in Alaska, the Government often provided the defense team with a copy of any computer hard drive which contained evidence considered to be child pornography, as long as an appropriate protective order was in place (Harvey Tr. 17, 76, Doc. 73-2, Johnson Affidavit). Since the passage of 18 U.S.C. § 3509(m), the Government no longer abides by this practice.

### **A. Discovery Procedures Prior to Enactment of the Walsh Act**

In Alaska prior to the Walsh Act, the Government provided mirrored hard drives to the defense attorney or expert (Harvey Tr. 107). The attorney and analyst signed an agreement in which the defense team agreed not to publish or distribute the material and to return the hard drive to the Government after the proceedings (Harvey Tr. 107). Agent Laws testified there was never a situation in Alaska when a defense attorney or computer analyst lost or distributed child pornography contained on a mirrored hard drive (Harvey Tr. 106). He was unaware of this ever happening nationwide. The single instance he knew of when a computer hard drive containing child pornography was lost, occurred when it was in the custody of the Government (Harvey Tr. 110-111).

The Federal Public Defender's criminal defense investigator, Mr. Bruce Johnson, stated that prior to the Walsh Act, the Government routinely provided copies of computer evidence to the Public Defender's Office, subject to appropriate protective orders and non-disclosure agreements (Harvey Doc. 73-2, Affidavit of Johnson at 2). Mr. Johnson maintained exclusive control of all computer evidence received and he placed such materials in a secure safe. He and the office administrator were the only two people with the key and security code to the safe, and he was the only person to ever access the safe (Harvey Doc. 73-2, Affidavit of Bruce Johnson at 3). Whenever he had to remove computer evidence from the safe, he documented the chain-of-custody and the date and time of its removal. He was the only person in the office who conducted analyses of the computer evidence, which ran in his secured office (Harvey Doc. 73-2, Affidavit of Bruce Johnson at 4). Upon completion of an analysis, he returned all computer evidence to the Government; permanently removed and deleted files and remnants of the hard drive from his office computer; and certified no copies had been made and all copies were returned (Harvey Doc. 73-2, Affidavit of Bruce Johnson at 5).

**B. Problems Presented when Defense Forensic Analysis is Required to Take Place at a Government Facility**

At the evidentiary hearing, Marcus Kenneth Lawson from Spokane, Washington testified as the defense computer forensics expert.<sup>1</sup> Mr. Lawson is the President of Global CompuSearch, LLC, which provides forensic computer investigations. Earlier in his career, Mr. Lawson worked for U.S. Customs as an agent specializing in child pornography computer forensic investigations

---

<sup>1</sup>As noted supra, the parties stipulated that the evidentiary hearing in U.S. v. Harvey on the issue of discovery of a hard drive in a prosecution for aggravated sexual abuse and possession of child pornography could be incorporated by reference in the record of this case. U.S. v. Winslow, Doc. 91. Lawson, who testified, is the defense forensic computer expert in both cases.

(Harvey Tr. 13). Mr. Lawson testified about the steps required for an effective analysis, including the need for specific equipment; access to the tools in his laboratory; access to his experienced colleagues; access to the Internet and access to defense counsel during the analysis.

The defense also relied upon the affidavits of Government agents filed in support of two search warrants in U.S. v. Harvey. The affidavits established the surroundings and circumstances necessary for an effective computer forensics exam (Harvey Doc. 42-3, Affidavit of Special Agent Skinner, Defendant's Exhibit C at the evidentiary hearing) and (Harvey Doc. 40-3, Affidavit of Special Agent Laws, Defendant's Exhibit B at the evidentiary hearing).

In his search warrant application and affidavit, Special Agent Kevin Laws of Immigration and Customs Enforcement (ICE) stated that reviewing data on a computer hard drive can take weeks or months; that it is impossible to attempt a computer review at the residence or office being searched; that searching computer systems for criminal evidence is very technical and requires a controlled environment. He added that it is difficult to know before a search what types of hardware and software are located on a computer, and therefore it is hard to know what type of experts and equipment are needed to analyze the computer and its data.

Special Agent Skinner of ICE stated in his affidavit that it is impossible to bring all of the technical manuals and specialized equipment necessary to conduct a thorough search to a search site; that a substantial amount of time is necessary to complete an analysis of a computer and a controlled environment is necessary. During the evidentiary hearing, Mr. Lawson agreed with the statements of both Agents Laws and Skinner (Harvey Tr. 19-22). Mr. Lawson stated that an on-site analysis, away from his laboratory, is difficult because running the required programs can take a long time and extend into the night (Harvey Tr. 22-23).

Mr. Lawson and his staff at CompuSearch, LLC have encountered the following problems when conducting computer analyses away from their office, at a Government facility (Harvey Tr. 19-43; Harvey Doc. 46-2, Affidavit of Lawson, incorporated by reference in evidentiary hearing Tr. 57):

1) Limited hours. Many times the Government will only provide limited hours to conduct an analysis. Government buildings have restricted hours—usually 9:00 a.m. to 5:00 p.m.—that prevent his team of experts from running a search or test after hours. Because various diagnostic programs frequently run into the night, if access is cut off at 5 p.m., the analysis can take much longer and may not be as effective.

2) Limited privacy. Frequently the Government will place an agent inside the room with defense experts. In these situations, defense experts are not able to have the requisite privacy and confidentiality needed to talk about the results with other experts and to talk with defense counsel about their findings. Also, the Government agents inside the room are often distracting and noisy, according to Mr. Lawson.

3) Limited contact. Often the Government will not provide phone access to the defense team. The rooms provided are often in the basement where there is no cell service and no telephone land lines (also referred to as fixed phone lines). This deficiency makes it difficult for the experts to consult with their colleagues and the attorneys.

4) No Internet access. Often an expert will need access to the Internet to conduct research to solve problems that occur during an analysis. The Government facilities provided to the defense team usually do not provide Internet access.

5) Inadequate preparation time. Because of the access limitations, both before and during

trial, the defense experts cannot be as prepared for trial as they would like to be and this deficiency is often exploited by the prosecution, who then make the defense experts appear unprepared or less knowledgeable about the evidence than the prosecution's experts, according to Mr. Lawson.

6) Damage to equipment. Transporting the expert's machines and tools often damage them and crucial time is spent fixing equipment instead of conducting the required analyses.

Mr. Lawson also testified that forensic computer analysis is crucial for the defense in any case involving child pornography or attempted aggravated assault on a child. Such analyses can reveal evidence of multiple users (Harvey Tr. 25); verify that any Internet chats reported by the Government are correct and presented in the proper context (Harvey Tr. 26, 28); profile the types of users in any chat rooms that may be at issue in the case (Harvey Tr. 28); determine the age of the people in any images involved in the case and whether or not the people in the images are real or virtual (Harvey Tr. 28, 30). It can also find evidence that reflects on whether or not the defendant intended to possess such child pornography (Harvey Tr. 53).

Mr. Lawson and defense counsel stressed that the biggest concern about 18 U.S.C. § 3905(m) is the effect it has on the defense at trial. Mr. Lawson testified that his team will often run tests and check data during a trial and after the trial has ended for the day (Harvey Tr. 33-38, 39). He said he often has associates stay late after a day of trial testimony to conduct tests and look up data (Harvey Tr. 75). According to Mr. Lawson, restrictive access to the copied hard drives during trial is an extreme handicap for the defense team (Harvey Tr. 36-38).

Mr. Lawson testified that since the passage of the Walsh Act, many forensic computer analysts will not work for a defense team because it is too difficult to conduct analyses in a

Government office, transporting their diagnostic equipment (Harvey Tr. 83-40). Despite the difficulties, Lawson's company still performs defense computer analyses (Tr. 40). His company has conducted forty to forty-five cases on the road since the passage of the Walsh Act (Harvey Tr. 72). According to Mr. Lawson, he believes that he and his staff did not do an adequate job when testifying in court because of the access limitations (Harvey Tr. 77).

Agent Laws testified as the Government's expert witness on computer forensics. He stated that, in his view, it is possible to do an effective defense forensic computer analysis at a Government office, notwithstanding his comments in his search warrant application about the difficulties of conducting a government forensic examination off-site. He testified that once the initial processing of a computer hard drive is complete, an expert then knows what tools and software will be necessary to complete the forensic analysis (Harvey Tr. 89). He said he did not believe it would give his adversaries insight into his work if the experts knew how often and how long he looked at the computer evidence (Harvey Tr. 103-104).

**C. Discovery Procedures to Date in Winslow Case**

While the Defendant's Motion for Order Compelling Discovery of All Computer-Related Evidence was pending, to expedite matters, the parties entered into a Stipulation Regarding Forensic Review Procedures Involving HP Pavillion Hard Drive Seized from Defendant (Winslow Doc. 85). The Government agreed to make two copies of a "true forensic, bit by bit E01 image of the HP Pavillion hard drive" available to the defense team to examine at the office of the Spokane Federal Bureau of Investigation (FBI). This was because expert Lawson's firm, Global CompuSearch, LLC, is located in Spokane. The stipulation stated:

The Spokane FBI Office will allow the defense team to install a stand-alone

defense forensics review workstation in an interview room monitored by Closed Circuit (CC) TV. The defense team lodges a standing objection to the camera while the forensic review is being conducted. While the non-audio feed will insure the integrity of FBI space and security of its occupants, the Plaintiff represents that the video feed will not be of sufficient detail or at an angle that would reveal defense strategy. The Plaintiff and its agents expressly agree that no attempt will be made to record any audio from the workstation and that no attempt will be made to observe the defense team's work product or computer monitor screen at any time. The defense expert may review the feed to ensure that their strategy is not being compromised at any time while conducting the forensic review.

(Winslow, Doc. 85 at 3).

In addition, the stipulation specifies that:

- The government will make a copy of the seized hard drive “reasonably available to the defendant and provide ample opportunity for the defense team to examine it . . . .”
- The defense team can review the evidence from 8 a.m. to 5 p.m. Monday through Friday. “The parties may approach the Court if there is a need for after hours access during the course of litigation in the event trial or motion hearings require additional forensic review.”
- The defense team will not make any copies of “alleged child pornography contraband.” The defense team is defined as the defense attorneys, defense investigator and defense forensic examiner. The word “contraband” is not defined.
- The defense team will not remove any contraband images from the government facility.

- The defense expert will be allowed to copy any file that is not contraband and compile a report without contraband images/videos on removable media at the discretion of the expert.
- The defense reserved all rights to object to the procedure and maintained a standing objection to the constitutionality of the Walsh Act.

U.S. District Court Judge Timothy M. Burgess entered a protective order, which adopted the stipulation (Doc. 87) on November 15, 2007.

On January 14, 2008, defense expert Lawson filed an affidavit with the Court, describing problems encountered during this discovery process. On January 4, 2008, an employee of Global CompuSearch went to the FBI office in Spokane, obtained the hard drive copies, set up her forensic station and attempted to view the media unsuccessfully. She reported that a forensic image “of what appeared to be a Compaq computer” was encrypted and required a password to open. A second forensic image entitled “other media” was also encrypted, and required a password to open. The examiner then returned the hard drive, broke down her forensic station, returned to Global CompuSearch and contacted the defense attorney. This process took one-half day (Doc. 102-2, Affidavit of Marcus K. Lawson).

Defense attorney McCoy then contacted Agent Laws about the matter. Agent Laws reported:

On or about January 7, 2008, I returned a telephone call to Kevin McCoy. Mr. McCoy inquired about some files on a hard drive sent to his computer expert in Spokane, Washington. Mr. McCoy said he was advised by his computer expert that some of the files on the hard drive were (sic) encrypted. I told Mr. McCoy that some of the files were

encrypted, that the hard drive contained items seized that were not included in the Stipulation and therefore I encrypted the files. I told Mr. McCoy that the hard drive also contained the “image” of several “CD’S” and at least one “media card” and these items where (sic) encrypted. I also told Mr. McCoy that his expert in Spokane was “looking at the files wrong” because the files covered in the court order—those involving the HP Pavillion hard drive—where (sic) in fact not encrypted.

(Winslow Doc. 106-2, Affidavit of Senior Special Agent Kevin J. Laws at 2).

Based upon this conversation, two Global CompuSearch experts again went to the Spokane FBI office on January 7 and repeated the process of obtaining the hard drive copies, setting up their forensic equipment and making screen captures of the encrypted media. This again took most of a morning (Winslow Doc. 102-2, Lawson affidavit at 3).

Further dialogue occurred with Agent Laws that permitted Mr. McCoy to ultimately forward the necessary passwords after receiving them from the Government on January 11. Mr. Lawson also reported that “the Spokane FBI Office has decided that it will no longer accommodate defense forensic examinations under 18 U.S.C. §3509(m) for cases originating outside of the Eastern District of Washington. Such examinations will be permitted only when there is an order by the district court requiring the Spokane FBI to permit the forensic evaluation on its premises.” (Winslow Doc. 102-2, Lawson affidavit at 4). Lawson concluded, stating, “. . . [T]he delay described in this affidavit illustrates and underscores the time consuming difficulties associated with performing a defense forensic examination of computer related media maintained in government controlled facilities.”

In its response to expert Lawson’s affidavit, the Government did not comment on the

assertion that the Spokane FBI office will no longer accommodate a defense forensic exam pursuant to the Walsh Act in the absence of a court order. It is also unclear from the present record whether the FBI is refusing the Global CompuSearch team access at the present time, or whether the Government views Judge Burgess' order enforcing the stipulation to require the FBI to cooperate.

### **III. ANALYSIS**

#### **A. Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure**

The Walsh Act became effective on July 27, 2006. Prior to that date, Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure governed whether or not the prosecution provided the defense team copies of hard drives containing alleged child pornography. Winslow asserts that under Rule 16(a)(1)(E), this Court can order the Government to produce a mirror-image of the hard drives, citing United States v. Hill, 322 F. Supp.2d 1081 (C.D. Cal 2004) for the proposition that it is not an abuse of discretion to order production of contraband such as child pornography with an appropriate protective order in place.<sup>2</sup> However, the Government asserts that Rule 16(a)(1)(E) is no longer controlling in child pornography cases since the passage of the Walsh Act.

Title 18 U.S.C. § 3509(m) states as follows:

**(m) Prohibition on reproduction of child pornography.--**

---

<sup>2</sup>Hill was decided by Judge Alex Kozinski of the Ninth Circuit, who was sitting as the district court judge by designation pursuant to 28 U.S.C. § 291(b). In that case, Judge Kozinski, rejected the Government's argument that the computer hard drives containing child pornography had to remain in the Government's offices. He ordered the hard drives be turned over to the defense team pursuant to a detailed protective order. Hill was decided prior to enactment of the Walsh Act.

(1) In any criminal proceeding, any property or material that constitutes child pornography (as defined by section 2256 of this title) shall remain in the care, custody, and control of either the Government or the court.

(2) (A) Notwithstanding Rule 16 of the Federal Rules of Criminal Procedure, a court shall deny, in any criminal proceeding, any request by the defendant to copy, photograph, duplicate, or otherwise reproduce any property or material that constitutes child pornography (as defined by section 2256 of this title), so long as the Government makes the property or material reasonably available to the defendant.

(B) For the purposes of subparagraph (A), property or material shall be deemed to be reasonably available to the defendant if the Government provides ample opportunity for inspection, viewing, and examination at a Government facility of the property or material by the defendant, his or her attorney, and any individual the defendant may seek to qualify to furnish expert testimony at trial.

Section 3509(m)(2)(A) clearly nullifies the copying requirements of Rule 16 as applied to child pornography.

**B. Constitutionality of 18 U.S.C. § 3509(m)**

Winslow challenges 18 U.S.C. § 3509(m) as it applies to computer evidence. He argues that in situations where computer evidence is involved, the statute violates a Defendant's Fifth

Amendment Due Process rights and Sixth Amendment Compulsory Process and Effective Assistance of Counsel rights.

To date, it appears no appellate court has reviewed the constitutionality of § 3509(m). However, district courts around the country have addressed the issue. All have ruled that the statute is constitutional. See United States v. Sturm, No. 06-CR-00342, 2007 WL 1453108 (D. Colo. May 17, 2007) (rejecting defendant's constitutional challenges to the Walsh Act, both facially and as applied, holding that the requirements of Subsections (2)(A) and (2)(B) of § 3509(m) are "consistent, if not coterminous, with the due process guarantee that [defendant] be afforded a 'fair opportunity to defend against the [Government's] accusations,'" and holding that because the defendant made no attempt to reach an accommodation with the United States, his as-applied challenge also fails); United States v. Doane, 501 F. Supp. 2d 897 (E.D. Ky. 2007) (finding that the case law does not support the defendant's position that requiring defense expert to examine a computer hard drive at a Government facility interferes with defendant's constitutional rights to investigate charges and to have assistance of counsel and due process because such access is "ample opportunity" under the statute); United States v. Renshaw, No. 05-CR-00165, 2007 WL 710239 (S.D. Ohio Mar. 6, 2007) (finding that although "Section 3509(m) may inconvenience trial counsel and [d]efendant's experts, it does not preclude defendant from preparing his case for trial" and because the statute provides a safety valve permitting the court to order the production of evidence where the Government does not make it reasonably available, there is no basis for a due process challenge and therefore the statute does not necessarily deny defendant a fair trial); United States v. O'Rourke, 470 F. Supp. 2d 1049, 1054-55 (D. Ariz. 2007) (rejecting defendant's constitutional challenges to the Walsh Act, both facially and as applied,

holding defendant was not deprived of due process by any Government refusal to give defense experts private access to the Internet when performing their analysis of the hard drive taken from defendant's computer); United States v. Knellinger, 471 F. Supp. 2d 640, 650 (E.D. Va. 2007) (noting that such an evaluation to compel duplication of materials should be made on a case-by-case basis, and holding that while the statute was constitutional, the Government had not given ample access to defense experts); United States v. Johnson, 456 F. Supp. 2d 1014, 1019-20 (N.D. Iowa 2006) (finding that the statute did not, as applied, unduly burden defendant's Fifth Amendment rights to due process and fair trial and Sixth Amendment right to effective assistance of counsel, and the statute did not unreasonably restrict defendant's access to services of computer forensic expert); United States v. Spivack, No. 05-CR-98, 2007 WL 4593475 (E.D.N.Y. Nov. 29, 2007) (finding the statute constitutional and holding that defendant provided no evidence that Government failed to provide ample opportunity); United States v. Battaglia, No. 07-CR-0055, 2007 WL 1831108 (N.D. Ohio June 25, 2007) (finding the statute constitutional and finding that Government provided ample opportunity); and United States v. Flinn, No. S-05-314, 2007 WL 3034932 (E.D. Cal. Oct. 16, 2007) (finding the statute constitutional and finding that defense had not presented any case-specific concerns to establish the lack of ample opportunity).

In the O'Rourke case, the court rejected the defendant's as applied and facial challenges to 18 U.S.C. § 3509(m). While the defendant challenged the statute under both the Fifth and Sixth Amendment, the court addressed the statute's constitutionality under the Fifth Amendment's due process framework, finding that the Fifth Amendment's Due Process clause provides broader protections for a fair trial than the Sixth Amendment. O'Rourke, 470 F. Supp. 2d at 1054, fn 2 (citing Pennsylvania v. Ritchie, 480 U.S. 39, 56 (1987)). The Court found that the statute does

not provide for an absolute denial of a defense team's possession of alleged child pornography. Instead, the court noted that § 3509(m)(2)(A) denies the defense team possession of the material only if the Government otherwise makes the material "reasonably available" to the defendant. O'Rourke, 470 F. Supp. 2d at 1055. The court noted that subsection 3509(m)(2)(B) provides that the material is "reasonably available" to the defendant if "the Government provides ample opportunity for inspection, viewing, and examination at a Government facility" of the material by the defense team. Id. Therefore, according to the court, if the Government does not provide "ample opportunity" to analyze the material at a Government facility, the court can order the Government to provide a copy to the defendant. Id. The court concluded that "ample opportunity" is coterminous with the requirements of due process because it requires the Government to provide defendants the same access to material that due process mandates, otherwise the court can order the Government to give the defense team a copy of the hard drive. Id. at 1055-56.

In Knellinger, the court applied similar reasoning and found that the term "ample opportunity" could be construed to, at a minimum, protect the constitutional rights of defendants. 471 F. Supp. 2d 640, 644 (E.D. Va. 2007). It therefore held that 18 U.S.C. § 3509(m) was facially constitutional. Id. at 645. The court also held that the statute would not be unconstitutional as applied either because the statute permitted the court to remedy insufficient "ample opportunity" through a court order, thus rendering any as-applied challenge moot. Id. at 646. Applying the facts, the court found that the defense needed digital video experts to establish the defense that the images on his computer were virtual and not real. Id. at 647. The digital video experts who testified in the Knellinger case noted that they do not move the equipment needed to run digital

video analysis and that it would be a great cost and effort to do so. They testified that they would not agree to service the defense team because their ability to do the job would be compromised. Id. at 646-48. The court ultimately found that the Government did not provide the defense team with an ample opportunity to inspect, view, and examine the child pornography because the experts needed to assert a “virtual-child” defense and could not conduct an analysis at a Government facility. Id. at 650. Therefore, the court ordered the Government to turn over a copy of the hard drive to the defense. Id.

In Sturm, the court adopted the reasoning of O’Rourke and Knellinger, and determined that 18 U.S.C. § 3509(m) is not facially unconstitutional. No. 06-CR-00342, 2007 WL 1453108 (D. Colo. May 17, 2007), at \*7. It also determined that the defense did not present with precision any actual or anticipated problems because the defense has not yet attempted to examine the images or work out an accommodation with the Government. Id. The court refused to rule for the defense based on hypothetical scenarios that could arise in any case, considering that witnesses suggested solutions to any hypothetical problems presented. Id. at \*7-\*8.

This Court finds the reasoning applied in O’Rourke, Knellinger, and Sturm persuasive. There is no indication of the purpose of § 3509(m) in the legislative history accompanying the Walsh Act.<sup>3</sup> See O’Rourke, 470 F. Supp. 2d at 1056 (citing 152 Cong. Rec. H676 (daily ed. Mar. 8, 2006) (statement of Rep. Conyers) and 152 Cong. Rec. H705-31 (daily ed. July 25, 2006)) (stating that § 3509(m) was added to the Walsh Act without consideration in committee and with virtually no explanation in the legislative history).

---

<sup>3</sup>There is a statement of purpose for the statute. However, there is no legislative history related to § 3509(m).

Nevertheless, it is the Court's responsibility to construe a statute to avoid a ruling of unconstitutionality, if possible. See Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Constr. Trades Council, 485 U.S. 568, 575 (1988) (citing Grenada County Supervisors v. Brown, 112 U.S. 261, 269 (1884)) (stating that a statute should be given a reasonable construction so that it is not ruled unconstitutional); United States v. Ray, 375 F.3d 980, 988-89 (9th Cir. 2004) (applying doctrine of constitutional avoidance); Abner J. Mikva & Eric Lane, An Introduction to Statutory Interpretation and Legislative Process 6-16, 23-27 (1997). Therefore, the term "ample opportunity" in 18 U.S.C. § 3509(m) must be read to at least include the same opportunity for inspection, viewing, and examination that is required by Fifth and Sixth Amendments of the Constitution. In other words, Winslow's opportunity to view, inspect, and examine the evidence must afford him a fair opportunity to defend against the Government's accusations as required by due process. If the Government is not providing a fair opportunity consistent with the Due Process clause, this Court can order the Government to turn over a copy of the evidence. This Court's ability to order the production of evidence and correct any situation that does not amount to "ample opportunity" renders any as-applied challenge moot. Instead, this Court must examine the facts to determine if the requisite access to the evidence will be provided to Winslow's defense team.

**C. Adequacy of Opportunity to Review Computer Hard Drive**

In this situation, expert Lawson testified that defense experts examining a hard drive in a Government facility encounter a number of problems that make inspection, viewing, and examination difficult, if not impossible. These problems involve limited hours to access the evidence; limited privacy; limited contact with colleagues and defense attorneys because of a lack

of phone reception; no Internet access to conduct research; inadequate preparation for trial, and possible damage to equipment when traveling. Winslow argues that because of these problems, when computer evidence is at issue, access to the computer at a Government facility is never going to amount to ample opportunity. The existence of these problems cause this Court concern about a defendant's right to a fair trial as encompassed in the Fifth and Sixth Amendments.

Winslow correctly argues that under constitutional jurisprudence he is entitled to access to evidence. See California v. Trombetta, 467 U.S. 479 (1984) (citing United States v. Valenzuela-Bernal, 458 U.S. 858, 867 (1982))(stating that to safeguard a criminal defendant's right to be afforded a meaningful opportunity to present a complete defense, the Court has developed "what might loosely be called the area of constitutionally guaranteed access to evidence").

Winslow also correctly argues that he has a right to the assistance of experts. See e.g., Ake v. Oklahoma, 470 U.S. 68, 83 (1985) (noting that indigent defendants have a right to receive the assistance of experts necessary for an adequate defense and holding that when sanity is to be an issue in trial, the state must assure the defendant access to a competent psychiatrist to conduct examinations and help prepare for the defense's preparation and presentation of the evidence).<sup>4</sup>

Underlying Winslow's argument as to why he does not have "ample opportunity" to view

---

<sup>4</sup>This right to expert assistance does not confer a constitutional right to choose a specific expert. Id. In this case, there is no evidence to suggest that Winslow will not be able to obtain an expert. In the Knellinger case, there was testimony from the digital video experts indicating that they would not take the case, leaving the defendant without expert assistance. 471 F. Supp. 2d at 647. In this case, while Lawson testified that many computer forensic experts are no longer taking cases similar to this one because of the restrictions imposed by 18 U.S.C. § 3509(m), he said his company still conducts computer analyses at Government facilities. In Knellinger, the digital video experts testified about the increased costs and impossibility of moving their equipment. 471 F. Supp. 2d at 647. According to the testimony of Lawson, his company has been moving equipment in order to conduct analyses off-site and nothing presented to this Court suggests that the equipment cannot be moved safely.

the hard drive is concern about the lack of privacy and the resulting disclosure of defense strategies and weaknesses. One of the questions presented by this case is whether the defense has a constitutional right to have defense experts view the evidence in private or whether it is acceptable for government agents to maintain video surveillance while discovery is underway. Here, the Government has conditioned access to the evidence upon an agreement that the experts remain under video surveillance. The Government promised that no audio recording would be made during discovery. No representation was made that the video images would not be recorded.

In United States v. Nobles, 422 U.S. 225 (1975), the Court considered the qualified work product privilege in the criminal context (ruling that the privilege protecting a defense investigator's report is waived if the investigator seeks to testify on behalf of the defendant.)

In describing the work product privilege, the Court stated:

‘Historically, a lawyer is an officer of the court and is bound to work for the advancement of justice while faithfully protecting the rightful interests of his clients. In performing his various duties, however, it is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel. . . .

\* \* \* \* \*

Although the work-product doctrine most frequently is asserted as a bar to discovery in civil litigation, its role in assuring the proper functioning of the criminal justice system is even more vital. The interests of society and the accused in obtaining a fair and accurate resolution of the question of guilt or innocence demand that adequate

safeguards assure the thorough preparation and presentation of each side of the case.

\* \* \* \* \*

. . . [T]he doctrine is an intensely practical one, grounded in the realities of litigation in our adversary system. One of those realities is that attorneys often must rely on the assistance of investigators and other agents in the compilation of materials in preparation for trial. It is therefore necessary that the doctrine protect material prepared by agents for the attorney as well as those prepared by the attorney himself.

United States v. Nobles, 422 U.S. 225, 238-9 (1975).

At least one district court has ruled that the Constitution requires that a defense expert be given private space to conduct a forensic examination of a hard drive allegedly containing child pornography. “Private space” was defined by the court as space where the expert “can conduct analyses of his choosing without purposeful or otherwise direct surveillance of those activities.”

United States v. Flinn, 2007 WL 3034932 at \*7 (E.D. Cal. Oct. 16, 2007)

The Government’s requirement that the discovery room remain under surveillance by closed circuit television, with the promise that the camera will not be trained on the computer monitor, does not provide “ample opportunity” to conduct discovery as required by the Constitution. Even without access to the final report of the expert, such surveillance can intrude upon the attorney work product privilege in meaningful ways. This is very troubling, particularly in light of the reason given by the Government for the surveillance. The stipulation of the parties states it is necessary “insure the integrity of FBI space and security of its occupants.” The Court is confident that the FBI can accomplish this important goal by means that do not impermissibly infringe upon the constitutional rights of the defendant.

The effective examination by defense experts is further hampered in this case because the Government did not make phone lines available in the room and no cell phone reception was possible (Harvey Tr. 32, 73). Also, no internet access was possible (Harvey Tr. 72, 73). This makes communication with defense counsel impossible without leaving the building and stopping the forensic examination, causing significant delay in completion of discovery (Winslow Doc. 102, Affidavit of Marcus K. Laws).

As noted supra, Agent Laws testified that prior to the Walsh Act, mirrored hard drives containing copies of child pornography were delivered to defense attorneys and experts for discovery purposes. With a protective order in place, there had never been an instance in Alaska's history when the contraband was copied or illicitly distributed (Tr. 106). He also testified he was unaware of any instance in the country when that occurred. The single time a hard drive with contraband on it disappeared, it had been in the custody of the Government, he said (Tr. 110-111).

The Walsh Act greatly increases the inconvenience, difficulty, and expense connected with both the prosecution and defense of child pornography offenses. In this matter, the Government perceives the statute to require the monitoring of the discovery room by closed circuit TV while defense experts examine the hard drive and prepare for trial—a process that can require days or weeks. Similarly, defense expert time is spent traveling to the Government facility and returning to his lab as needed for equipment and expert consultations. This drives up the cost for the parties. United States v. Flinn, No. S-05-314, 2007 WL 3034932, at \*5 (E.D. Cal. Oct. 16, 2007) (stating that the statute causes extra costs to be incurred). When a defendant is represented at taxpayer expense, the increased costs charged by the defense forensic examiner are ultimately paid by the taxpayer. See 18 U.S.C. § 3006A(e). When considering the new statute, one judge stated:

One could reasonably argue that §3509(m) is legislation by anecdote, and is an overreaction to an infrequent problem, the burdens of which outweigh the possible benefits. However, Congress gets to make its judgments on less than empirically perfect data. Except in the most arbitrary situations, concerns about the wisdom of legislation are to be raised before Congress.

Flinn, 2007 WL 3034932, at \*6.

In United States v. Harvey, 3:07-CR-00103-RRB-DMS, to accomplish discovery, the Government offered the defense a private room in a government facility, a basement room at Immigration and Customs Enforcement. The room was made available 24-hours a day both before and during trial, and phone access and internet access were provided. A government agent was posted outside the room but did not enter it. This Court ruled that these discovery conditions addressed all the significant problems set forth by defense expert Lawson, and provided ample opportunity to review the hard drive under circumstances coterminous with the constitutional requirements embodied in the Fifth and Sixth Amendments (Harvey, Doc. 104).

The same conclusion cannot be reached in the instant case. No phone or internet access is provided (Harvey Tr. 32, 72, 73). And, most importantly, privacy is not permitted. These restrictions impermissibly intrude upon both the defendant's Fifth and Sixth Amendment rights and are insufficient to "assure the thorough preparation and presentation of each side of the case" allowing for a "fair and accurate resolution of the question of guilt or innocence." U.S. v. Nobles, Id. As a result, this Court orders the Government to produce a copy of the hard drive to the defense team pursuant to the conditions described infra.

**D. Ability to Copy Non-pornographic Files on Hard Drive**

The hard drive in question also contains online chats and emails between Winslow and an undercover officer. This evidence is relevant to prove the charge of attempted aggravated sexual abuse. Defense expert Lawson testified that a forensic examination of such materials could reveal multiple users; determine whether the Internet chats reported by the Government were correctly reported and presented in the proper context; and profile the types of users in any chat rooms that may be at issue in the case.

In his motion, Winslow requests a copy of the computer files contained on the hard drive, which are not visual depictions of child pornography. See 18 U.S.C. §3509(m) (incorporating the definition of child pornography found at 18 U.S.C. §2256). The defense makes this request pursuant to Rule 16 of the Federal Rules of Criminal Procedure, United States v. Hill, 322 F. Supp. 2d 1081 (C.D. Call 2004), and the Fifth and Sixth Amendments to the Constitution.

It is unnecessary to resolve the question in the present case because the Court is directing that a copy of the hard drive be provided to defense counsel. Also, the stipulation of the parties states that the defense team can copy any file that is not contraband. If it is necessary for the expert to download copies of non-pornographic materials to complete his report, and this can be done without compromising the forensic integrity of the hard drive, this is permissible pursuant to Rule 16 and the Fifth and Sixth Amendments to the Constitution. There is nothing in the plain language of § 3509(m) to prohibit it.

In Flinn, the court considered the expert request to remove downloaded materials which were not child pornography from the custody of the Government facility. The Court ruled:

With the exception of materials which would be considered child pornography

under federal law, the expert may take off site that electronic or electronically derived information necessary for his examination or report; the expert will certify in writing that he has taken no materials which would be considered child pornography under federal law; and that he has not caused any such child pornography to be sent off site. . . .

Flinn, 2007 WL 3034932, at \*6.

#### **IV. CONCLUSION**

This Court finds that the conditions for review offered by the Government in this case do not meet the Constitutional requirements of due process and a fair trial. The conditions also intrude on the defendant's Sixth Amendment rights. Thus, ample opportunity for review pursuant to 18 U.S.C. § 3509(m) has been denied. Therefore, Defendant Winslow's Motion for Order Compelling Discovery of All Computer-Related Evidence Seized from Randy D. Winslow is **HEREBY GRANTED**.

In light of the Government's failure to provide ample opportunity to review the hard drive, this Court orders that a copy of the HP Pavillion hard drive seized from the home of the defendant be immediately provided to defense attorney Kevin McCoy under the following terms and conditions:

- 1) The hard drive copy will be delivered to and remain in the exclusive control of defense investigator Bruce Johnson and will be maintained in a secure safe at the Federal Public Defender Agency in Anchorage.
- 2) Whenever the evidence is removed from the safe, the chain-of-custody will be documented and the date and time of its removal. Any analysis of the hard drive will occur in a locked,

secure room. Only the defense attorney, investigator and expert may have access.

- 3) Any individual who handles or views any portion of the hard drive must sign a non-disclosure agreement, agreeing to refrain from copying or publishing any material which would be considered child pornography under federal law.
- 4) With the exception of materials which would be considered child pornography under federal law, the defense investigator and/or expert may download files or portions of files as long as the forensic integrity of the hard drive is not altered. He may take off site that electronic or electronically-derived information necessary for his examination or report; the expert will certify in writing that he has kept no materials which would be considered child pornography under federal law and that he has not caused any child pornography to be sent off site.
- 5) Upon completion of the hard drive examination, the hard drive will be returned to the Government.
- 6) The defense expert and/or investigator will certify that, upon completion of the hard drive examination, all files and remnants of the hard drive are permanently removed and deleted from the defense computer equipment.

DATED this 28<sup>th</sup> day of January, 2008, at Anchorage, Alaska.

/s/ Deborah M. Smith  
DEBORAH M. SMITH  
United States Magistrate Judge