Frank R. Chapman
Thomas R. Smith
CHAPMAN VALDEZ
PO Box 2710
Casper, Wyoming 82602
(307) 237-1983
(307) 577-1871 (fax)
ATTORNEYS FOR DEFENDANT

In The District Court

For the District of Wyoming

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Case No. 07-CR-32-B
	)	
NATHANIEL SOLON	)	
	)	
Defendant.	)	

MEMORANDUM IN SUPPORT OF MOTION TO DISMISS

This Memorandum is filed in support of Defendant Nathaniel Solon's Motion to Dismiss based upon denial of due process under the standards of *California v. Trombetta*, 467 U.S. 479 (1984).

Background

Defendant is charged in a single count indictment with possession of child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2). The charges stem from an investigation conducted through the Wyoming Internet Crimes Against Children (ICAC) Task Force in Cheyenne, Wyoming. Through investigations, Application and Affidavit were made for a search warrant filed September 15, 2006 (Case No. 06-N-185-B attached as Exhibit A). A Search Warrant was issued that same day by the Honorable William C. Beaman, United States Magistrate Judge (attached as

Exhibit B). The Application and Affidavit for Search Warrant, other than providing the basis for probable cause for issuance of the warrant, additionally include paragraphs of particular relevance for this motion. Paragraphs 15, 16 and 17 state the necessity of seizing not only parts of the computer but all computer items including hardware, software and storage media. Paragraph 16 testifies to maintaining a properly controlled environment in order to protect the integrity of the evidence in order to recover hidden, erased, compressed, password protected or encrypted files. Paragraphs 15, 16 and 17 are quoted as their importance is paramount:

> (15) Your Affiant knows from training and experience that searches and seizures of evidence from computers require agents to seize most of all computer items (hardware, software, passwords and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. Computer storage media to include but not limited to floppy disks, hard drives, tapes, DVD disks, CD ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography can store the equivalent of thousands of pages of information. Users may store information or images in random order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process renders it impractical to attempt this kind of data search on site.
>
> (16) Affiant knows from training and experience that searching computer systems for criminal evidence requires experience in the computer field and a properly controlled environment in order to protect the integrity of the evidence and recover even "hidden", erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources and from destructive code imbedded in the system as a "booby trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.
>
> (17) Affiant knows from training and experience that in order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the computer. In cases like this one where the evidence consists partly of graphics files, the input and

> output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media and the storage media are also essential to show the nature and quality of the graphic images which the system could produce. In addition the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) as well as documentation, items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized or to activate specific equipment or software.

(emphasis added).

The Search Warrant authorized the seizure of "All computers and peripheral equipment including, CPU's, monitors, keyboards, mice, scanners, printers, network communication devices, modems, external or connected devices used for accessing computer storage media, as well as hardware and software". Exhibit B. Thus, it seems without question that law enforcement recognized the importance of obtaining the complete computer system and not just components. They were authorized to do so by the Search Warrant.

Notwithstanding this recognized necessity and the authority granted to them in the Search Warrant, agents only seized a few items at the residence. These items are listed in the receipt provided to the Defendant (attached as Exhibit C). Only a few items were seized and certainly not the entire system.

The search warrant was executed on September 21, 2006. The Defendant was not arrested until January, 2007. During the time between the seizure of the hard drive and his arrest, the Defendant retained possession of the remainder of the computer components and eventually had another hard drive installed, as well as other work performed on it. Under information and belief, the

undersigned states that the computer has been used by the Defendant's daughter, her friends, his sister, and possibly others since the time of his arrest.

The charge against the Defendant is based upon digital images on the Maxtor hard drive seized (Item 400 on Exhibit C, and Indictment). The failure of the agents to seize the entire computer system prejudices the Defendant. Defendant contends that the failure to seize the system destroyed evidence.

Without the entire computer system, it cannot be ascertained, amongst other things, what images were actually viewable by the Defendant. Data could be stored on the hard drive without it being viewable. (Affidavit of Robert Reilly). Reilly's opinions about the possible non-viewability of stored data is the same as that of the government. See paragraph 17 of Affidavit, *supra*, (Seizure of most equipment "essential to show the nature and quality of the graphic images which the system could produce.")

If the data was not viewable on the Defendant's system, the Defendant could not have "knowingly" possessed the computer disk that contained child pornography, an element of the crime he is charged with.

Additionally, without the system as a whole, other evaluations are impossible. It is impossible to run a complete virus scan on the system. (See Affidavit of Greg Coffey) A virus in the hard drive can be an entirely different matter from a virus in the system.

Legal Analysis.

In *Trombetta*, *supra* and later in *Arizona v. Youngblood*, 488 U.S. 51 (1989), the United States Supreme Court discussed the standards for a defendant making a claim of denial of due process when evidence has been destroyed or not retained by the government. Because there are different standards, it is important to establish whether *Trombetta* or *Youngblood apply*. See, *U.S. v. Bohl*, 25 F.3d 904 (10th Cir. 1994) ("We must first determine whether *Trombetta* or *Youngblood* governs our analysis of [the] due process challenge. This inquiry turns on the import of the destroyed materials.")

Trombetta holds that any duty that the Constitution imposed must be limited to evidence "that might be expected to play a significant role in the suspect's defense. To meet this standard of constitutional materiality, evidence must both possess an exculpatory value that was apparent before the evidence was destroyed, and be of such of a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means." *Trombetta, supra*. 467 U.S. at 488-89. This case meets the *Trombetta* standard of constitutional materiality. The exculpatory value is recognized in the affidavit for the search warrant.

The second prong of the *Trombetta* standard is also met. This Defendant is unable to obtain comparable evidence by other reasonably available means. Defendant contends the U.S. should acknowledge this. The acknowledgment is likewise a part of the affidavit. (*e.g.*, . . . "computer evidence is extremely vulnerable." Paragraph 16).

In the present case, putting the system back together after these many months would not provide an accurate picture of the system at the time it was in Solon's possession. There has been no

reliable chain of custody. It is dubious whether any admissible evidence could be obtained putting the hard drive back into the system.

Defendant contends that the United States, through its own agent's affidavit, acknowledged the importance of maintaining the entire system for proper analysis. If proper analysis is important for prosecution, the exculpatory value is patent. The United States realized the evidentiary value of preserving the entire system, but, for some unknown reason, did not preserve the entire system. The evidence was not maintained. Failure to maintain the entire system destroyed much of the evidentiary value of what was seized. The digital images constitute the core of the Government's case. Defendant is denied the ability to defend himself properly by inability to have the entire system analyzed.

Appropriate Remedy.

This Court should choose between barring further prosecution or suppressing the Government's most probative evidence. *U.S. v. Bohl, supra,* 25 F. 3rd at 914, citing *Trombetta*. Because, there is no alternative to protecting this defendant's due process rights other than dismissal, defendant requests the Court dismiss the Indictment against him.

DATED this _____ day of April, 2007.

By: _____

Frank R. Chapman
Thomas R. Smith
CHAPMAN VALDEZ at
BEECH STREET LAW OFFICE
PO Box 2710
Casper, Wyoming 82602
(307) 237-1983
(307) 577-1871 (fax)
ATTORNEYS FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing document was served this _____ day of April, 2007, by U.S. Mail, addressed to:

Jim Anderson
U.S. Attorney=s Office
PO Box 668
Cheyenne, WY 82003-0668

_____
Cheryl L. Deere