ORIGINAL

FILED
U.S. DISTRICT COURT
DISTRICT OF WYOMING
APR 27 2007
Stephan Harris, Clerk
Cheyenne

JAMES C. ANDERSON
Assistant United States Attorney
Post Office Box 668
Cheyenne, WY 82003-0668
(307) 772-2124

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF WYOMING

UNITED STATES OF AMERICA	)	
	)	**Criminal No. 07-CR-0032-B**
Plaintiff,	)	
v.	)	
NATHANIEL SOLON,	)	
Defendant.	)	

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO DISMISS

COMES NOW, the United States of America, by and through its attorney, James C. Anderson, Assistant United States Attorney for the District of Wyoming, and hereby respectfully submits the following as the Government's response to the Defendant's Motion to Dismiss.

I. INTRODUCTION

The Defendant has been indicted by the Federal Grand Jury for the District of Wyoming with one count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). On April 13, 2007, the Defendant filed a motion seeking dismissal of the indictment herein based upon an alleged due process claim wherein he alleges the United States destroyed potentially exculpatory evidence. At best the Defendant's claim is based upon a complete misunderstanding of the proper techniques used by individuals qualified to conduct forensic examinations of computers. As the Defendant's motion has absolutely no basis in fact or any support in the applicable law it must be denied.

II. FACTS

As the result of an investigation relating to the trading of child pornography on Internet file sharing sites, Immigration and Customs Enforcement Special Agent Nicole Balliett identified a computer in Casper, Wyoming, offering to share child pornography with other computer users using a file sharing network. Through the use of administrative subpoenas Balliett was able to determine the computer was located at 439 Melrose, Casper, the residence of the Defendant, Nathaniel Solon. On

September 20, 2006, Balliett obtained a Federal search warrant authorizing the search of the Defendant's residence for items relating to child pornography. The search warrant was executed by Balliett and other members of the Wyoming Internet Crimes Against Children Task Force[1] on September 21, 2006. The Defendant was present during the search. When questioned about his use of file sharing networks the Defendant admitted he had downloaded adult pornography but no child pornography.

The search warrant issued by Magistrate Beaman authorized agents to seize any computers and/or computer systems within the residence. Agents did find a computer belonging to the Defendant but did not find it necessary to take the entire computer system. Rather the agents removed the computer's hard drive[2] from the computer and

---

[1]The Wyoming Internet Crimes Against Children Task Force(ICAC) is a law enforcement task force comprised of 5 Wyoming Division of Criminal Investigation agents, 1 Federal Bureau of Investigation agent, and 1 Immigration and Customs Enforcement Bureau agent (Balliett). ICAC is tasked with investigating crimes relating to the online exploitation of children. The task force leader, Flint Waters, has received both national and international recognition for his outstanding efforts in developing techniques to investigate these types of crimes.

[2] The term "hard drive" is actually short for "hard disk drive." The term "hard disk" refers to the actual disks inside the hard drive. However, all three of these terms are usually seen as referring to the same thing -- the place where data is stored within a computer, that is the locale within a computer system where files and folders are physically located. A typical hard drive in a desktop computer is only slightly larger than an adult's hand, yet can hold over 250 GB of data (approximately 80 million pages of data). The data is magnetically stored on a stack of disks that are mounted inside a solid encasement. These disks spin extremely fast (typically at either 5400 or 7200 RPM) so that data can be accessed immediately from anywhere on the disks within the

elected to leave the remainder of the system behind. The agents decided not to seize the entire system because upon their initial preview of the digital files contained on the hard drive of the computer did not reveal any images of child sexual abuse. This fact, coupled with the Defendant's insistence he was innocent of any wrongdoing, lead the agents to only take the hard drive from his computer.[3] However, a subsequent forensic exam of the hard drive did reveal images of child sexual abuse within unallocated space on the hard drive. This indicates the child pornography had been present on the hard drive in the form of individual files and the Defendant deleted those files. Approximately 8 to 10 viewable child pornography files were found by the examiner and all had been deleted on September 20, 2006, the day

---

drive. Because data is stored magnetically it stays on the hard drive disks even after the power supply is turned off. When a user saves data or installs a program on his/her computer, the information is typically placed on the hard disk. The hard disk is a spindle of magnetic disks, called platters, that record and store information. The hard drive transmits data back and forth between the central processing unit of the computer and the disk.

[3] The Government will introduce testimony that in some instances it is necessary for agents to seize an entire computer system to preserve the integrity of the digital evidence, but such was not the case in the instant case. Whether the entire computer system needs to be seized or just a hard drive often is dependent upon whether the computer is on and running at the time of the search and seizure. If a computer is on at the time of the search the BIOS system can be queried by the seizing agent to determine the accuracy of the system clock. If the computer is off then it may be necessary to seize the entire system to accurately verify the workings of the computer.

before the search.

The Defendant has filed a motion to dismiss claiming his due process rights have been violated because the Government failed to seize and preserve his entire computer system. According to the memorandum filed by the Defendant the Government's failure to seize his entire computer system "prejudices the Defendant." The Defendant contends that the failure to seize the entire system destroyed evidence. This is so, according to the Defendant, because without the entire system an examiner cannot ascertain "what images were actually viewable by the Defendant." *Defendant's Memordum*, at 4. In support of this motion the Defendant appended to his memorandum the declarations of two witnesses, neither of which appears to be a qualified forensic computer examiner, setting forth their opinions that the Government's actions has resulted in the destruction of evidence. The Government will introduce testimony and evidence at the hearing on this motion demonstrating that the seizure and examination of a hard drive, without the seizure of the entire operating system, does not alter, destroy, or otherwise impact the quality of the evidence relating to what data and files were present on the subject computer at the time of the seizure. Further, the Government will present testimony and evidence

establishing the procedures followed by the ICAC team in this matter were well withing the bounds of established practice and procedure by those who are qualified to forensically examine computers. Finally, the evidence will establish that the Defendant had custody and control of his computer system after the seizure of his hard drive and any alteration of the remaining system which could have altered or destroyed evidence relating to the computer was done by the Defendant, not the Government.

III. APPLICABLE LAW

In *California v. Trombetta*, 467 U.S. 479 (1984) the Court held that due process concerns require the government to preserve "evidence that might be expected to play a significant role in the suspect's defense." *Id.*, 467 U.S. at 488. This has been described by the Court as "a constitutionally guaranteed right to access evidence." *Id.*, at 485. The Court explained that a defendant's due process rights are violated when the government destroys such evidence where: 1) the evidence possesses an exculpatory significance that was "apparent before" its destruction; and 2) the defendant is unable to "obtain comparable evidence by other reasonably available means." *Id.*, 467 U.S. at 489. See also *United States v. Parker*, 72 F.3d

1444, 1451 (10th Cir. 1995) ("The mere possibility that lost or destroyed evidence could have exculpated a defendant is not sufficient to satisfy *Trombetta's* requirement that the exculpatory value be apparent to the police before destruction.") Evidence of such a nature is deemed to be "constitutionally material." *California v. Trombetta,* 467 U.S. 488-89. In *Arizona v. Youngblood*, the Court extended *Trombetta*, holding that where the government fails to preserve "evidentiary material of which no more can be said than it could have been subjected to tests, the results of which might have exonerated the defendant," then no due process violation occurs unless the defendant demonstrates the government acted in bad faith. 488 U.S. 51, 57 (1988). [M]ere negligence on the government's part in failing to preserve such evidence is inadequate for a showing of bad faith." *Id.* at 912.

In determining whether a law enforcement officer has acted in bad faith in destroying potentially useful evidence the Tenth Circuit has stated the inquiry must necessarily turn on the [police officer's] knowledge of the exculpatory value of the evidence at the time it was lost or destroyed." *United States v. Bohl,* 25 F.3d 904, 911 (10th Cir. 1994). The *Bohl* court stated a court should consider whether: (1) the government was on notice that the defendant believed the evidence potentially

exculpatory; (2) the defendant's assertion to the government the evidence possessed potential exculpatory value was merely conclusory or supported by objective, independent evidence, (3) the government still had possession of or the ability to control the disposition of the evidence at the time it received notice from the defendant of the evidence's potential exculpatory value, (4) the destroyed evidence was central to the government's case, (5) the government offers an innocent explanation for its failure to preserve the evidence, and (6) the destruction of the evidence was in accordance with standard procedure and the evidence was adequately documented prior to its destruction. *Id.* at 911-13.

IV. ANALYSIS

In the case at bar the investigating agents will testify that it is not unusual to only seize a hard drive during a search for digital evidence because the hard drive is the repository within a computer system where digital information is stored. Further, the Wyoming ICAC agents involved in this case will testify that in most instances a forensic exam of a computer to determine what data is stored within the computer simply doesn't require the entire computer system, just the hard drive. Such was the case here. So, by leaving the remainder of the Defendant's computer system in the

possession of the Defendant and only seizing his hard drive, the agents were not deliberately destroying or altering potentially exculpatory evidence as the Defendant erroneously claims. While the Defendant has appended the declarations of two individuals who claim that evidence has been destroyed by the ICAC agents it does not appear that either of these declarants possesses a background in the forensic examination of computer evidence. Further, their declarations simply demonstrate a profound misunderstanding of the forensic process and the requirements imposed upon a forensic computer examiner to maintain the integrity of seized evidence.

Importantly, the Wyoming ICAC agents will testify they have maintained the custody and integrity of the Defendant's hard drive since the day of its seizure and have not altered, changed, or otherwise tampered with the digital information contained on the hard drive. Pursuant to standard policy and procedure for conducting forensic examinations of digital evidence, the ICAC agents made an exact image of the Defendant's hard drive and examined the copy, not the original.[4] Thus, the evidence will establish the Government has not destroyed or altered any of the

[4] This is a procedure followed by the FBI, Secret Service, ATF, Department of Defense, ICE, and other Federal law enforcement agencies as well as the 46 ICAC teams within the United States.

digital evidence seized from the Defendant. If anyone has destroyed or failed to preserve evidence in this matter it was the Defendant, not the Government. See *United States v. Booth,* 309 F.3d 566, (9th Cir. 2002)(no due process violation when alleged exculpatory evidence not in possession of the government and accessible to the defendant). Moreover, whatever alterations or changes the Defendant has made to his computer system post-seizure are meaningless with respect as to whether he can examine and test the evidence the Government intends to introduce against him.[5]

Further, assuming *arguendo*, that the Government did destroy potentially exculpatory evidence (which the Government vigorously denies) there is simply no evidence whatsoever the agents acted in bad faith. On the contrary, the evidence will establish, as stated above, that the agents acted in conformity with established procedures and lacked any intent whatsoever to deny the Defendant with access to constitutionally material evidence. In fact, the Government has gone out of its way to comply with its obligation to provide discovery to the Defendant. The Government has provided complete discovery to the Defendant and defense counsel and his

[5]The Defendant has been free to examine the copy of his hard drive, which is at the ICAC offices, at any time simply by making an appointment with the investigating agents. To date Defense counsel and his "experts" have been to the ICAC offices on 2 occasions.

"experts" have been to the ICAC offices on two occasions to examine the digital evidence seized by the Government. Far from trying to deny the Defendant access to evidence the Government has attempted to be as transparent as possible allowing the defense access to the evidence gathered in this case. In fact, on April 26, 2007, defense counsel and his "experts" brought the Defendant's computer to the ICAC offices and inserted a copy of his original hard drive (supplied by the ICAC team) into the computer. The computer was then turned on and the digital information contained on the hard drive copy was viewed.

V. CONCLUSION

The Government would submit that absolutely no constitutionally material evidence in this matter has been altered, destroyed, or otherwise been rendered inaccessible to the Defendant. His motion to dismiss is specious at best and must be denied.

DATED this 27th day of May, 2007.

Respectfully submitted,

MATTHEW H. MEAD
United States Attorney

By: _____
JAMES C. ANDERSON
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that I served a true and correct copy of the foregoing **GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO DISMISS** upon the following by placing the same in the United States mail, postage prepaid and dated this 27th day of May, 2007:

Mr. Frank Chapman
Mr. Thomas Smith
Chapman Valdez
P.O. Box 2710
Casper, Wyoming 82602
Attorneys for the Defendant

_____