UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

JAMES JOHNSTON,

Defendant.

_____/

NO. CR. S-07-00425 KJM

ORDER

Defendant James Johnston is charged in a superseding indictment filed May 19, 2011, with (1) conspiracy to produce visual depictions of minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2251(c) and (e); (2) receipt of visual depictions of minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(2); (3) possession of one or more matters containing depictions of minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(4)(B); and (4) conspiracy to travel with intent to engage in illicit sexual conduct in violation of 18 U.S.C. § 2423(b) and (e). (ECF 75.)[1]

On February 27, 2012, defendant filed several motions, including a motion to suppress that the court has not previously resolved. The government filed an opposition to the motion to suppress on March 19, 2012. The court heard argument on the motion on March 28,

[1] The original indictment, filed on September 20, 2007, charged defendant with possession of one or more matters containing depictions of minors engaged in sexually explicit conduct, in violation of 18 U.S.C. § 2252(a)(4)(B). (ECF 1.)

2012, and then set the matter for an evidentiary hearing, which occurred on April 3, 2012. At the conclusion of the evidentiary hearing, counsel made closing arguments. At all proceedings on the motion to suppress, defendant has been represented by Tom Johnson and defendant has personally appeared, out of custody; the government has been represented by Kyle Reardon.

For the reasons that follow, the court DENIES defendant's motion to suppress.

I. Factual Background

A. Documentary Record

In October 2005, federal investigatory agents located an illegal child pornography website identified by the name "Illegal CP." (ECF 92-1 at 20.) On December 23, 2005, a United States District Judge in New Jersey authorized the interception of communications pertaining to the Illegal CP website. (*Id*. at 23.) On or about February 12, 2006, the operator of the e-mail account brestogen@yahoo.com sought a subscription to the Illegal CP website, listing his name as that of the defendant, James Johnston. (*Id*. at 29-30.) On February 13, 2006, ICE agents intercepted an e-mail message to brestogen@yahoo.com informing the recipient of access to the Illegal CP website. (*Id*. at 31.) After confirming that the e-mail address brestogen@yahoo.com belonged to a James Johnston, and otherwise confirming information related to Johnston including his residential address, (i*d*. at 31-33), agents sought and obtained a warrant to search defendant's residence, which they did on September 6, 2006. The search warrant, issued by a U.S. magistrate judge on September 5, 2006, authorized seizure of "evidence of violations of 18 U.S.C. 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography, and violations of 18 U.S.C. 2252(a)(2) and 2252A(a)(2), which make it a crime to receive child pornography in interstate commerce by computer." (*Id*. at 3.) Specifically, the warrant identified the following items for seizure, among others: "[computer] hard drive, any other computer-related operation equipment," "correspondence pertaining to the possession, receipt, distribution, or advertisement of visual depictions of minors engaged in sexually explicit conduct . . . transmitted or received using a computer," "electronic mail, chat logs, and electronic messages, offering to transmit . . . visual depictions of minors engaged in sexually explicit conduct," and "records evidencing occupancy or ownership of the premises [to

be searched]" and "ownership or use of computer equipment found in the . . . residence." *Id.* at 41-42.

During execution of the search warrant, agents found two computers; on one an agent located fifteen video clips depicting minors engaged in sexually explicit conduct. (ECF 92-2 at 1.) Agents also found information related to travel documents and money order receipts. (ECF 106-2.) Before concluding the search, agents seized the computer and created a copy of the hard drive. (*Id.*) Agents conducted a first search of a mirror image of the hard drive between September 15, 2006, and October 23, 2006, searching for "images depicting minors engaged in sexually explicit conduct." (ECF 92-2 at 2.) During this first search, Special Agent Brian A. Cardwell found seven still photographic images and 304 video clips depicting minors engaged in sexually explicit conduct. (*Id.* at 2-3.) He also found 302 videos of the same kind in the computer's recycle folder. (*Id.* at 3.) A search for e-mails containing images or videos depicting minors engaged in sexually explicit conduct yielded no results, but some "emails of interest" and chat logs were located; the agent created a CD copy of the chat logs but did not review them in detail at the time. (*Id.* at 4.) Based on this information, on September 20, 2007, the government filed an indictment against defendant, charging possession of one or more matters containing depictions of minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(4)(B). (ECF 1.)

A second search of a mirror image of defendant's computer was completed between April 18 and June 14, 2011. (ECF 92-4.) During this search, Agent Cardwell discovered 80 thumbnail images containing child pornography, and 285 link files, several of them containing child pornography. (*Id.* at 5.) A search for the e-mail address brestogen@yahoo.com resulted in 97527 hits,[2] including a copy of a webpage at which

[2] During the evidentiary hearing, defense counsel referenced a report by Agent Cardwell based on the second search, which incorporates a different number, namely 1156827 hits. The defense had its copy of the report marked as an exhibit for reference and provided a copy to the court following the hearing. The court has carefully reviewed the two different reports based on Agent Cardwell's second search, the first signed by the agent on May 21, 2011, and the second signed by him on June 14, 2011. Apart from the different number of hits

(continued...)

defendant had used the "brestogen" e-mail address to book a flight from Sacramento to Bangkok; no year for the flight was evident. (*Id*. at 6.)

Agent Cardwell also completed a third search, of a mirror image of defendant's computer, on July 21, 2011. (ECF 106-2.[3]) During this search, the agent reviewed the CD of the chat logs he had created during the first search in 2006, as well as e-mails and internet history files. He also reviewed e-mails, internet activity and used keyword searches to look "for further evidence pertaining to child pornography." During this search, the agent located chat logs of internet chats between the person using the screen name "brestogen" and a person using the screen name "switlass_69," identified as Kim Lacson. (*Id.* at 2.) The chats reflect, among other things, Lacson asking if her correspondent wanted "young" women and saying she had a friend who was a 15 year old "virgin"; "brestogen" responded "sure" and asked for a picture of the virgin or her vagina. Other chats also involve discussions of young women, including a "12 year old beauty," and defendant's desire to meet them and see photos of them first. (*Id.* at 3.)

B. Evidentiary Hearing Testimony

At the evidentiary hearing, Agent Cardwell testified regarding the method of searching he used during his examinations of defendant's computer. He said he was present during execution of the search warrant at defendant's residence on September 6, 2006; in preparation for that search he reviewed the warrant and developed a procedure to determine whether evidence pertaining to child pornography was located on any computer that might be

---

[2](...continued)
appearing in one line of the reports, the court finds there are no material differences between them. The earlier report in fact does include a separate paragraph, on page 7, describing a search of the "brestogen" e-mail, which yielded 97527 hits. The earlier report also includes the additional report of an email netted by this search, sent from another of defendant's e-mails to his "brestogen" account, and indicates a copy is provided with the report as "attachment 1-11." No such attachment is identified, however, in the index of attachments included in this report on page 9, and the court has not located such an attachment in the record. While the government has offered no explanation for the discrepancy between the two reports based on the second search, it also has not indicated it plans to rely on any email sent from defendant to himself at his "brestogen" account and so the court does not consider any such email as the subject of the pending motion to suppress.

[3] The first page of this report is not included in the document filed on the court's electronic docket, but it was provided by the parties at the evidentiary hearing.

found during the search. On one computer, located downstairs in the residence, the agent did locate videos of child pornography, at which point he immediately turned off the computer and took steps to seize the computer for further off site forensic analysis. In conducting his first analysis, beginning on September 15, 2006, Agent Cardwell first used a forensic software product to create a mirror image of the computer, confirming to a 99% measure of accuracy that the image was a true copy of the computer. He then used the software to look for images, including videos, of child pornography. He also conducted word searches, of the words "child porn" and other words he knows are commonly used by those who view child pornography. He reviewed e-mails, chat logs and internet search history. In reviewing e-mails, Agent Cardwell perused all the e-mails captured through a search of the e-mail addresses identified in the search warrant, and found some e-mails that contained images of child pornography. The agent clarified that his primary purpose in searching the e-mails, however, was capturing defendant's e-mail accounts based on information provided in the warrant. He also saved chat logs identified through his searching as potentially relevant because persons who view child pornography often chat about their viewing activities on line. The agent described this first search as a "triage" search during which he did not review a lot of information. Rather once he found a relatively small amount of evidence he provided it to the prosecuting attorney. Based on his experience, the evidence he provided was equivalent to the evidence that in most cases supports the prosecutor's filing of charges and that also results in an early guilty plea.

During his second search beginning on April 18, 2011, Agent Cardwell testified that he found the same information located during his initial search. But at the request of the prosecutor, he conducted a more thorough search of internet history and e-mail correspondence, and he also looked at files to see if images had been opened. He specifically searched for the credit card number and e-mail address associated with the subscription to the child pornography website identified in the original search warrant application. Agent Cardwell testified at all times that his purpose was to look for child pornography.

During his third search of defendant's computer on July 21, 2011, Agent Cardwell again looked for child pornography, and prepared a detailed analysis of the chat logs he

had previously saved to a CD. He isolated relevant chats and reviewed their content. During this search he located evidence related to child pornography; in response to the prosecutor's questioning he said that some of this evidence was intermingled with evidence of other crimes. During the third search, the agent again conducted word searches. While he did not recall the specific words searched, he said he assumed he used the words he typically uses for these types of searches, such as "child porn," "lolita," "baby j," "pedo" and "hussyfan." He said he also conducted followup searches based on information turned up during his searches, including the nickname "lollipop." When asked if he ever searched for information other than that related to child pornography, the agent said no.

During cross-examination, Agent Cardwell testified that he saved only chat logs and not e-mails to a CD. He said he understood he was authorized to review all e-mails and chats line by line for the purpose of determining if they contained or referenced child pornography. He did in fact review some but not all chat logs line by line. While at one point the agent testified he understood it was acceptable for him to provide a copy of the CD containing every chat log to the lead agent on the case, and to the prosecutor, he also said he did not seize or provide anything to the prosecutor that did not pertain to child pornography. Agent Cardwell confirmed he could not recall exactly which search terms he used during any given search, and conceded he did not create a detailed log or day-to-day report to document every step of his analysis of defendant's computer. Regarding information on air travel retrieved during his search, the agent said that the flight information itself "did not mean anything" to him; rather the information was retrieved through searching for the user i.d., e-mail and date of birth information contained in the search warrant application.

II. The Parties' Arguments

In closing argument following the evidentiary hearing, defendant argued, in essence, that the searches that turned up the "emails of interest" and other material unrelated to receipt and possession of child pornography exceeded the scope of the search warrant and so this material should be suppressed. He also argued that the lack of detail in the examining agent's reports is fatal to the government's position; because it is not possible to reconstruct exactly

what the agent did, in what order, it is not possible to determine clearly that the agent acted only within the bounds laid out by the warrant's terms. Defendant also argues that the CD containing all of the chat logs and provided during discovery, without any segregation of material beyond the scope of the warrant, is proof of the government's "rummaging" indiscriminately through defendant's computer in violation of the Fourth Amendment.

In response, the government takes the position that all of the searches carried out fell within the scope of the original warrant, in that they all were targeted to locate images of child pornography that were possessed or received, material related to the Illegal CP website, subscription information, e-mail address, credit card number, and other information expressly set forth in the warrant application and providing probable cause to search defendant's residence in the first place. To the extent any material located during the searches does not qualify strictly as evidence of receipt or possession of child pornography, the government argues it was discovered in "plain view" during the course of those authorized searches, and that it was intermingled in such a way that "parsing" by the examining agent was not practical or required.

III. Legal Standards

The warrant clause of the Fourth Amendment requires "probable cause, supported by Oath or affirmation" to justify the issuance of a search warrant. U.S. Const. amend. IV. In addition, the Fourth Amendment requires a particular description of the items to be seized in connection with the execution of the warrant. *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). If a search conducted based on a warrant exceeds the scope of that warrant, the search violates the Fourth Amendment. *Horton v. California*, 496 U.S. 128, 140 (1990).

When the results of a warrant-based search are challenged in a motion to suppress, the defendant bears the burden of demonstrating that the search is unreasonable under the Fourth Amendment. *See United States v. Ankeny*, 502 F.3d 829, 836 (9th Cir. 2007); 6 Wayne LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 11.2(b) (4th ed. 2004) ("if the search or seizure was pursuant to a warrant, the defendant has the burden of proof; but if the police acted without a warrant the burden of proof is on the prosecution").

/////

The Ninth Circuit has considered suppression in the context of computer searches for child pornography, in a case relied on by both parties. In *United States v. Giberson*, 527 F.3d 882, 884 (9th Cir. 2008), the defendant appealed the district court's denial of his motion to suppress evidence of child pornography found on his personal computer, which led to his conviction for receipt and possession of child pornography. Giberson had been pulled over by an officer for expired license plates. *Id*. When the officer discovered he had three outstanding arrest warrants and no valid driver's license, a search incident to arrest was conducted. *Id*. It was later discovered that Giberson failed to make child support payments, and a warrant to search his home was issued. *Id*. Prior to execution of the warrant, agents did not know that Giberson owned a computer. *Id*. When agents found a computer at Giberson's home, they obtained a separate search warrant for it, to search for information pertaining to fake I.D. cards they had found sitting next to the printer. *Id*. at 884-85. While searching Giberson's computer an agent "discovered images he believed to be child pornography." *Id*. at 885. The agent immediately stopped the search, and then was directed by his supervisor to continue searching only for items related to the creation of fake I.D.s; however, if the agent came across more child pornography, he was told to print it out. *Id*. Agents then obtained a third warrant to search for information pertaining to child pornography; the search based on this warrant located more than 700 images, and led to the child pornography charges being filed against Giberson. *Id*. Giberson challenged the seizure of his computer and the search of his hard drive, arguing the evidence of child pornography should be suppressed. *Id*. at 886. The Ninth Circuit disagreed, explaining that, "'in the age of modern technology . . . [a] warrant could not be expected to describe with exactitude the precise form the records would take.'" *Id*. at 887 (quoting *United States v. Reyes*, 798 F.2d 380, 383 (10th Cir. 1986)). The court, noting that "a search warrant authorizing the seizure of materials also authorizes the search of objects that could contain those materials," held "where there was ample evidence that the documents authorized in the warrant could be found on Giberson's computer, the officers did not exceed the scope of the warrant when they seized the computer." *Id*. at 886-87. The court further explained that the officers' "actions were particularly appropriate because the agents merely secured the computer while

they waited to get a second warrant that would specifically authorize searching the computer's files." *Id*. at 889. Finally, the court found it important that "after discovering the pornographic images, [the agent] continued his search for evidence of fake I.D. documents and only inadvertently came across more child pornography. The government only searched for pornographic files after obtaining the third search warrant." *Id*. at 890.

In the later case of *United States v. Payton*, 573 F.3d 859, 863 (9th Cir. 2009), the Ninth Circuit explained the *Giberson* holding as relying on the legitimacy of the first warrant to search the computer, based "quite specifically on the documents found next to the printer . . . indicating a likelihood that they were created on and printed from the computer." In *Payton*, the search warrant authorized a search for items related to the sale of methamphetamine; it did not authorize searching information on a computer. *Id*. at 862. During the search, officers found a computer with the screen saver on, and without obtaining a second warrant, moved a mouse to click open a file. There was nothing analogous to the evidence in Giberson, sitting next to the computer, that would have justified a computer search or "any attempt to secure the computer and seek a second warrant." *Id*. at 864. In reversing the district court's denial of a motion to suppress evidence of child pornography found during that search, the Ninth Circuit concluded "the search of Payton's computer without explicit authorization in the warrant exceeded the scope of that warrant and did not meet the Fourth Amendment standard of reasonableness illustrated by *Giberson*." *Id*.

Other, earlier Ninth Circuit authority emphasizes the point made in *Payton*, namely the importance generally of a warrant specifying with particularity the material that may be seized. *See Center Art Galleries-Hawaii, Inc. v. United States*, 875 F.2d 747, 749 (9th Cir. 1989), *superseded by statute on other grounds as noted in J.B. Manning Corp. v. United States*, 86 F.3d 926, 927 (9th Cir. 1996) (warrant allowing seizure of items constituting "evidence of violations of criminal law" did not satisfy the Fourth Amendment's specificity requirement); *United States v. Kow*, 58 F. 3d 423, 427 (9th Cir. 1995) (warrant authorizing seizure "of virtually every document and computer file" lacked Fourth Amendment specificity). But to the extent material falling within a search warrant's scope is intermingled with other material on a

computer, seizure of the other material is not impermissible. "As long as an item appears, at the time of the search, to contain evidence reasonably related to the purposes of the search, there is no reason absent some other Fourth Amendment violation to suppress it. The fact that an item seized happens to contain other incriminating information not covered by the terms of the warrant does not compel its suppression, either in whole or in part." *United States v. Beusch*, 596 F.2d 871 (9th Cir. 1979) (citation omitted; conclusion rests on seizure of noncomputerized "single files and single ledgers" constituting "one volume or file folder" and may not apply to "sets of ledgers or files"). This principle extends to searches of computers and other electronic storage media, during which officers are entitled to seize all such media for later examination. *See United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) ("It is true that all items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search."). *See also United States v. Hill*, 322 F. Supp. 2d 1081, 1089 (C.D. Cal. 2004) (*citing United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000)). Because "[t]he difficulties of examining and separating electronic media at the scene are well known," a warrant's authorizing "seizure of intermingled materials that are difficult and time-consuming to separate on-site" is reasonable and permissible. *Hill*, 231 F.3d at 1090. The intermingled nature of materials, however, does not justify a detailed examination of the entire content of those materials in the form of "an investigatory dragnet." *Tamura*, 694 F.2d at 595; *see also United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1170 (9th Cir. 2010).

To the extent that certain materials located during a search are outside the scope of the warrant, to avoid suppression those materials must have been located in plain view during a search faithful to the terms of the warrant. Specifically, "(1) the officer must be lawfully in the place where the seized item was in plain view; (2) the item's incriminating nature was 'immediately apparent;' and (3) the officer had 'a lawful right of access to the object itself.'" *United States v. Wong*, 334 F.3d 831, 838 (9th Cir. 2003) (applying test to find that in searching graphics files for evidence of murder as authorized by a warrant, officers' discovery of child pornography deemed to be in plain view). "There is no rule. . .that evidence turned up while

officers are rightfully searching a location under a properly issued warrant must be excluded simply because the evidence found may support charges for a related crime. . . not expressly contemplated in the warrant." *United States v. Adjani*, 452 F.3d 1140, 1151 (9th Cir. 2006) (reversing suppression of e-mails that supported extortion conspiracy charge not identified in warrant, given that e-mails were discovered during search that complied with warrant).

Defendant cites no authority, and the court has found none, for the proposition that the lack of precise detail in Agent Cardwell's investigative reports explaining exactly what he searched for and what he found at each step along the way is fatal to the government's opposition to the motion to suppress, because it makes it impossible to know whether the searches were within the scope of the warrant.

IV. Analysis

Here, the search warrant that authorized Agent Cardwell's search of defendant's computer specified with sufficient particularity the material to be seized, by making clear it needed to pertain to possession or receipt of child pornography, and by identifying the list of items that could be seized. By authorizing the seizure of defendant's computer hard drive, the warrant also authorized the targeted search of the hard drive; by authorizing seizure of electronic correspondence offering to transmit visual depictions of minors, including e-mails and chat logs, the warrant allowed for the search of e-mail and chat log histories that could contain such correspondence. Agent Cardwell's description of the investigatory steps that led to his discovering emails and internet information related to foreign travel, and to internet chats with "switlass_69," demonstrates that any information his searches returned that was not limited precisely to possession or receipt of images of child pornography was located by searching only for this kind of material. As in *Giberson*, although the government here did not seek an additional warrant after the agent discovered the travel information and the chats, the agent continued his search by looking only for evidence of child pornography. There is no indication that he ever diverted his search to areas of inquiry outside the scope of the warrant, conducting the kind of "investigatory dragnet" operation that would violate the Fourth Amendment. Although the government concedes it provided the defense with a CD containing all of the chat

logs saved from defendant's computer, Agent Cardwell's testimony explains the CD is a copy of what he saved during his initial search of the hard drive; the steps he took to search the CD for material authorized by the warrant are not consistent with the kind of indiscriminate rummaging that would support suppression.

Certain material the defendant's motion targets also satisfies the plain view doctrine as clarified in *Wong*. Agent Cardwell was searching the computer hard drive as authorized by the warrant, and specific areas of the hard drive authorized by the warrant as well, when he came upon the chat logs and foreign travel information. The incriminating nature of chat logs referencing sexual relations with young women of the ages of 12 and 15 was immediately apparent. The travel reservation information was returned in the agent's searching for information to confirm the identity of the computer's owner, and the person who subscribed to the Illegal CP website. It is not disputed that Agent Cardwell had a lawful right of access to the hard drive and its contents.

Defendant's briefing raised questions regarding whether the search of defendant's computer was carried out in a manner faithful to the terms of the search warrant, and those questions warranted an evidentiary hearing. Agent Cardwell's testimony under oath has provided sufficient, credible detail to support the conclusion that he carried out his searches within the warrant's bounds. On the record before the court, defendant has not met his burden of demonstrating the search of his computer violated the Fourth Amendment.

Accordingly, IT IS HEREBY ORDERED that defendant's motion to suppress is DENIED.

DATED: April 16, 2012.

UNITED STATES DISTRICT JUDGE