16 February 2017

IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES, *Appellee*,	)	FINAL BRIEF ON BEHALF OF THE UNITED STATES
v.	)	USCA Dkt. No. 16-0727/AF
Lieutenant Colonel (O-5), JAMES W. RICHARDS, IV, USAF, *Appellant.*	)	Crim. App. No. 38346

FINAL BRIEF ON BEHALF OF THE UNITED STATES

MARY ELLEN PAYNE, Major, USAF
Appellate Government Counsel
Air Force Legal Operations Agency
United States Air Force
1500 Perimeter Road, Suite 1190
Joint Base Andrews NAF, MD 20762
(240) 612-4800
Court Bar No. 34088

GERALD R. BRUCE
Associate Chief, Government Trial and
Appellate Counsel Division
Air Force Legal Operations Agency
United States Air Force
1500 Perimeter Road, Suite 1190
Joint Base Andrews NAF, MD 20762
(240) 612-4800
Court Bar No. 27428

KATHERINE E. OLER, Colonel, USAF
Chief, Government Trial and
Appellate Counsel Division
Air Force Legal Operations Agency
United States Air Force
1500 Perimeter Road, Suite 1190
Joint Base Andrews NAF, MD 20762
(240) 612-4815
Court Bar No. 30753

INDEX

TABLE OF AUTHORITIES

Page(s)

SUPREME COURT CASES

COURT OF APPEALS FOR THE ARMED FORCES

COURTS OF CRIMINAL APPEALS

FEDERAL CIRCUIT AND DISTRICT COURT CASES

STATUTES

OTHER AUTHORITIES

16 February 2017

IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES, *Appellee*,	)	FINAL BRIEF ON BEHALF OF THE UNITED STATES
v.	)	USCA Dkt. No. 16-0727/AF
Lieutenant Colonel (O-5), JAMES W. RICHARDS, IV, USAF, *Appellant.*	)	Crim. App. No. 38346

TO THE HONORABLE, THE JUDGES OF THE
UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES:

ISSUE PRESENTED

WHETHER THE 9 NOVEMBER 2011 SEARCH AUTHORIZATION WAS OVERBROAD IN FAILING TO LIMIT THE DATES OF THE COMMUNICATIONS BEING SEARCHED, AND IF SO, WHETHER THE ERROR WAS HARMLESS.

STATEMENT OF STATUTORY JURISDICTION

The Air Force Court of Criminal Appeals (AFCCA) reviewed this case pursuant to Article 66, UCMJ. This Court has jurisdiction to review this case under Article 67(a)(3), UCMJ.

STATEMENT OF THE CASE

Appellant's Statement of the Case is generally accepted.

STATEMENT OF FACTS

On 22 April 2011, the Air Force Office of Special Investigations (AFOSI) at Tyndall Air Force Base, Florida received notification from the National Center for

Missing and Exploited Children that Appellant had been accused of child molestation. (J.A. at 171, 755-56.) Specifically, one of Appellant's former "little brothers" from the Big Brothers of America organization, J.P., had alleged that Appellant sexually assaulted him approximately 10 times when J.P. was between the ages of 9 and 13. (J.A. at 171, 756.) AFOSI initiated an investigation into Appellant and discovered that Appellant had been dismissed from the local Big Brothers program for violations of their visitation policy. (J.A. at 756.) AFOSI then began physical surveillance of Appellant, which included, among other things, placing a GPS tracker on Appellant's car. (J.A. at 757.) Data from this GPS tracker revealed that Appellant, who lived on Tyndall Air Force Base, had been stopping at the base visitors' center at odd hours of the day. (Id.) AFOSI discovered that Appellant had been signing a minor male, A.P., onto base. (J.A. at 233, 758.)

On 9 November 2011, the Bay County Sheriff's Office (BCSO) interviewed A.P., who was then 17 years old. (J.A. at 483.) A.P. stated that he had known Appellant "for about a year and a half to two years," and that their relationship had begun online. (Id.) The two texted with one another and talked online, and the online talk was almost always of a sexual nature. (J.A. at 483-84.) In late February 2011, A.P. and Appellant met in person. (J.A. at 484.) While A.P. was still sixteen years old, A.P. and Appellant's relationship became sexual. (J.A. at

484-85, 490.) A.P. estimated that he and Appellant had had oral or anal sex 25 times. (J.A. at 486-87.) Sometimes Appellant would come to A.P.'s school to pick him up and then take him to Appellant's house. (J.A. at 488.) Appellant told A.P. that if anyone asked about their relationship, A.P. should say that Appellant was his uncle. (J.A. at 489.)[1]

Based on the information revealed by A.P. in his interview, SA Sara Winchester of AFOSI prepared an AF IMT 1176 search authorization and accompanying affidavit. (J.A. at 270-72.) The search authorization allowed for the search of Appellant and his residence and the seizure of "all electronic media and power cords for devices capable of transmitting or storing online communications." It further explained the magistrate was "satisfied from the matters presented that the said property . . . is evidence which will aid in the apprehension or conviction of the persons(s) who committed the offense being investigated, or . . . has been used . . . as the means of committing the criminal offense being investigated . . ." (J.A. at 270.)

The search authorization listed "Florida Statute Section 847.0125 Computer Pornography; Traveling to meet a minor" as the offense being investigated. (Id.)

[1] Later, on 16 November 2011, A.P. recanted his claims that he and Appellant had engaged in sexual relations, but he did not recant his allegations that he and Appellant had engaged in sexual conversations online. (J.A. at 190, 776.) This recantation occurred soon after A.P. had spoken with Appellant on the phone about his interview with BCSO. (J.A. at 190, 501.)

Florida Statute Section 847.0125 (2010) makes it a crime to travel any distance or cause another to travel any distance, in, to, or from the state of Florida, for the purpose of engaging in illegal sexual conduct with a child[2] "after using a computer online service, Internet service, local bulletin board service, or any other device capable of electronic data storage or transmission to seduce, solicit, lure, or entice . . . a child to engage in" such illegal sexual conduct.

The accompanying affidavit described the information that A.P. had related to the BCSO during his 9 November 2011 interview, including that Appellant and A.P. had "engaged in sexually explicit conversations" online for approximately a year prior to starting their physical relationship in April 2011. (J.A. at 271.) It related that Appellant had given A.P. "a cover story should he ever be questioned about their relationship." (Id.) The affidavit further stated that SA Winchester had coordinated with the Tyndall Air Force Base legal office, where an attorney agreed that "probable cause existed to conduct a search to obtain all electronic media and power cords for devices capable of transmitting or storing online communications related to the matter being investigated against [Appellant]." (J.A. at 271-72.) The affidavit used the same language as the search authorization in identifying the crime being investigated and the items to be seized. (J.A. at 271.) The magistrate gave verbal authorization to search Appellant's residence on 9 November 2011.

[2] Florida law defines a "child" as being any person under the age of 18 years. Florida Statute Section 827.01 (2010).

(J.A. at 272.) The magistrate signed the AF IMT 1176 the next day. (J.A. at 270.)

In accordance with the authorization, AFOSI searched Appellant's residence on 9 November 2011, and seized, among other devices, four loose hard drives: a Western hard drive, a Toshiba hard drive, a Gateway hard drive, and a Maxtor hard drive.[3] (J.A. at 241, 658, 697.)

The following day, on 10 November 2011, Appellant was arrested at the Panama City, Florida Airport. (J.A. at 458-59.) Pursuant to an additional search authorization dated 10 November 2011, electronic devices on Appellant's person, including cell phones and Appellant's personal HP Pavilion laptop, were seized and ultimately transferred to AFOSI. (J.A. at 218, 257-58, 459.) The 10 November 2011 search authorization and supporting affidavit were nearly identical in language to the 9 November 2011 authorization and affidavit, except that they allowed a search of Appellant himself, rather than his residence. (J.A. at 327-29.)

AFOSI sent the devices seized from Appellant on 9-10 November 2011, including the four loose hard drives and Appellant's personal HP Pavilion laptop computer, to the Defense Computer Forensic Laboratory (DCFL) for analysis.

[3] To assist the Court, the United States has created a chart at Appendix A summarizing the evidence seized from Appellant as described in this *Statement of Facts.* The chart is not a comprehensive list of all devices seized from Appellant, but includes the devices and evidence most relevant to the granted issue. Where the source of the information in the chart is not clear from the body of the *Statement of Facts,* additional citations to the record have been included in the chart.

(J.A. at 429.) AFOSI requested that DCFL analyze, among other things, "all pictures, videos, chat logs, times of access and use, and any other historical or current use information relevant to the matter being investigated." (J.A. at 368.)

In December 2011, DCFL made mirror images of some of Appellant's devices and returned a Forensic Data Extraction (FDE) drive to AFOSI containing the mirrored data. (J.A. at 459.) This particular FDE (FDE #1) was received by AFOSI on 23 December 2011 and contained data from two of the loose hard drives (the Western and the Maxtor) and from the hard drive from Appellant's personal HP Pavilion laptop.[4] (J.A. at 234, 459, 507.) As SA Shane Nishioka of AFOSI explained in an affidavit, "DCFL simply dumped all the pictures and on-line chats from these drives onto one big drive for review." (JA at 507.)

When SA Nishioka plugged this FDE in to AFOSI's stand-alone computer, a graphical user interface or "GUI" opened up, which displayed "standard windows and folders" that were arranged in categories such as photos, videos, and chats. (J.A. at 464, 760-61.) SA Winchester, who had prepared the affidavit and search authorization, was also present and demonstrated how to use the FDE. (J.A. at 773.) SA Nishioka began reviewing the FDE by opening the first folder on the list,

[4] The Toshiba hard drive and Gateway hard drive seized on 9 November 2011 were damaged and were eventually received back at AFOSI in a separated FDE (FDE #2) on 12 March 2012 after the hard drives had been repaired. (J.A. at 218-20, 234, 237, 464.) (Comparing the first and fourth columns of J.A. at 393-94 with J.A. at 577 reveals which devices were contained on which FDE.)

which was "Pictures." (J.A. at 761.) He explained that he started from the top of the list on the FDE and worked his way down, including reviewing subfolders. (Id.) SA Nishioka found several photos of A.P., including a picture of A.P. that looked like a screenshot of a Skype chat. (J.A. at 521-22, 761.)

After finding these pictures of A.P., SA Nishioka continued to search for evidence on the FDE in pictures subfolders that were labeled as "unallocated." (J.A. at 762, 773.) In one of those "unallocated" subfolders, SA Nishioka saw child pornography.[5] (J.A. at 773.) SA Nishioka immediately stopped, notified his supervisor, notified the legal office, and obtained another search authorization from the magistrate to search all of the devices in AFOSI's possession for child pornography. (J.A. at 762.) This search authorization was obtained on 3 January 2012. (J.A. at 242, 382.) SA Nishioka did not continue his search of Appellant's electronic devices until he had received this additional search authorization. (Id.)

[5] Appellant asserts in his brief that the files in unallocated space that SA Nishioka was reviewing when he first discovered child pornography came from the Toshiba hard drive and the Gateway external hard drive, and were likely deleted in 2007 and 2006, respectively. (App. Br. at 23.) However, the record makes clear these were not the same files that SA Nishioka was searching through in January 2012 when he first encountered the child pornography. The Toshiba hard drive and the Gateway external hard drive were contained on the second FDE sent to AFOSI on 13 March 2012. (J.A. at 237, 393-94, 577) The record indicates that there were also images of child pornography found in unallocated space on the Maxtor hard drive and the HP Pavilion laptop, which would have been contained on the first FDE received by AFOSI on 23 December 2011. (J.A. at 393-94, 577.) There does not appear to be any information in the record as to whether the image of child pornography SA Nishioka initially found in unallocated space on the first FDE had any dates or times associated with it.

Pursuant to the 3 January 2012 search authorization, SA Nishioka discovered thousands of images of child pornography on Appellant's media devices. (J.A. at 234, 237.) Some of these images of child pornography, found later on the Toshiba and Gateway hard drives, depicted a boy, N.R., whose brother Appellant had mentored through the Big Brothers Program. (J.A. at 237, 396.) Analysis by DCFL revealed that the images of N.R. had been taken with an HP Photosmart digital camera on various dates from 2005 to 2007. (J.A. at 208, 550-65.) These images of N.R. comprised Prosecution Exhibits 32-37 and formed the basis for Charge I, Specifications 2-6 (indecent acts committed against N.R.) (J.A. at 103, 544-64, 644.)

Approximately 100 files of child pornography found on the HP Pavilion laptop, the Maxtor hard drive, the Toshiba hard drive, and the Gateway hard drive were admitted at trial under Mil. R. Evid. 404(b) as Prosecution Exhibits 39 and 40. (J.A. at 103, 538-39.)

The discovery of child pornography on Appellant's devices formed part of the basis for probable cause determinations in subsequent search authorizations obtained by AFOSI on 12 March 2012 and 2 April 2012. (J.A. at 243-44, 395-397.) The 12 March 2012 search produced an HP Photosmart digital camera which was eventually entered into evidence against Appellant as Prosecution Exhibit 41. (J.A. at 103, 238, 243-44.) Subsequent analysis showed this was

indeed the camera used to take the pornographic pictures of N.R. found on Appellant's hard drives. (J.A. at 565.)

The 2 April 2012 search produced a Western Digital My Passport external hard drive that contained thumbnail images of child pornography that were entered into evidence against Appellant as Prosecution Exhibit 38 in support of Charge I, Specification 1 (possession of child pornography). (J.A. at 393.)

At trial, Appellant moved to suppress the evidence seized as a result of the 9 November 2011 and all derivative evidence on several grounds, including that the search authorization was overbroad. (J.A. at 115-117.) The military judge denied Appellant's motion to suppress and found that the 9 November 2011 search authorization was not overbroad because "it was written with enough particularity to sufficiently guide and control the agent's judgment in selecting what to seize and search. And the category of items to be seized was appropriate under the circumstances." (J.A. at 640.) In the alternative, the military judge found that the good faith exception to the exclusionary rule applied. (Id.)

During a motions hearing at trial, Mr. Frederick Kleeh, a forensic examiner from DCFL, testified about his analysis of Appellant's electronic devices. (J.A. at 650-712.) Mr. Kleeh testified that when a file is deleted from a computer it actually stays on the computer in "unallocated space" until that space is overwritten by a new file. (J.A. at 660, 662.) He explained that files in

unallocated space are not necessarily written over in the order they are deleted, and therefore he could not specify how long it would take for a file in unallocated space to be written over. (J.A. at 662.) Due to the way deleted files are stored in unallocated space, a file may exist in unallocated space, but "the dates and times from the file system" may be lost. (J.A. at 663, 698.) For example, Mr. Kleeh testified about 13 images found on Appellant's Western Digital My Passport hard drive for which there was no date or time information or any other metadata. (J.A. at 670, 674.)

Mr. Kleeh further asserted that when DCFL makes a mirror copy of a media device, they do not filter the data by specific dates. (J.A. at 702.) He explained that when creating the FDE drive, DCFL could theoretically screen out the data by date, but this would only capture files that actually had metadata associated with them. (J.A. at 703.)

SUMMARY OF THE ARGUMENT

The 9 November 2011 search authorization was not overbroad in failing to limit the dates of the communications being searched. The search authorization already contained an implicit limitation on the dates to be searched, because it only authorized a search for evidence that Appellant had violated a particular Florida statute, and Appellant did not move Florida until mid-2010. Even so, the Fourth Amendment's specificity and particularity requirements do not mandate that search

authorizations contain any specific search methodology or protocol. The nature of computer searches, in fact, dictates against imposing date limitations in search authorizations, because such limitations could cause law enforcement agents to miss incriminating evidence that has been hidden or mislabeled, or that is located in unallocated space. In this particular case, where Appellant could have deleted or attempted to hide evidence of his relationship with A.P., a date limitation on the search authorization would have unreasonably restricted the AFOSI agents' search for incriminating evidence.

Even assuming the 9 November 2011 search authorization was overbroad, the AFOSI agents relied on it in good faith. No controlling authority requires all search authorizations to contain date limitations, and therefore, the search authorization was not so facially deficient that the AFOSI agents could not have reasonably presumed it to be valid. Moreover, the agents were searching in folders that they reasonably believed were covered by the warrant when they discovered child pornography, and then further demonstrated their good faith by stopping their search to obtain a new search authorization. This reasonable and prudent law enforcement conduct does not warrant the application of the exclusionary rule to the seized evidence.

Finally, even if the search authorization had contained date limitations, the evidence of child pornography would have been inevitably discovered by AFOSI.

Even operating under a date limitation, it would still have been reasonable for AFOSI to search in the unallocated pictures folder where the child pornography was ultimately found. Since the search authorization was not overbroad, and, in the alternative, the good faith exception to the exclusionary rule and the inevitable discovery doctrine would apply, the military judge did not abuse his discretion by denying Appellant's motion to suppress.

ARGUMENT

THE 9 NOVEMBER 2011 SEARCH AUTHORIZATION PROPERLY LIMITED AFOSI AGENTS TO SEARCHING ONLY FOR EVIDENCE FOR WHICH THERE WAS PROBABLE CAUSE; THEREFORE, IT WAS NOT OVERBROAD. EVEN IF THE SEARCH AUTHORIZATION WAS OVERBROAD, BOTH THE GOOD FAITH EXCEPTION TO THE EXCLUSIONARY RULE AND THE INEVITABLE DISCOVERY DOCTRINE WOULD APPLY.

Standard of Review

This Court reviews a military judge's denial of a motion to suppress for an abuse of discretion. United States v. Clayton, 68 M.J. 419, 423 (C.A.A.F. 2010). In doing so, this Court views the evidence in the light most favorable to the prevailing party below. United States v. Hoffmann, 75 M.J. 120, 124 (C.A.A.F. 2016). This Court reviews the military judge's findings of fact for clear error, and his conclusions of law de novo. Id. Whether a search authorization is overly broad is a question reviewed de novo. United States v. Maxwell, 45 M.J. 406, 420

(C.A.A.F. 1996).

Law and Analysis

The Fourth Amendment[6] provides that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Evidence directly obtained through a violation of the Fourth Amendment as well as evidence that is the "fruit" of such a violation may be subject to exclusion at trial. Wong Sun v. United States, 371 U.S. 471, 488 (1963). The touchstone of the Fourth Amendment is "reasonableness." Florida v. Jimeno, 500 U.S. 248, 250 (1991).

The Supreme Court has asserted:

> The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory search the framers intended to prohibit.

Maryland v. Garrison, 480 U.S. 79, 84 (1987).

1. The 9 November 2011 Search Authorization was not overbroad.

The military judge correctly ruled that the 9 November 2011 search authorization was not constitutionally overbroad. As the Ninth Circuit Court of Appeals has explained, "[s]earch warrants must be specific. 'Specificity has two

[6] U.S. Const. amend. IV.

aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based.'" United States v. Hill, 459 F.3d 966, 973 (9th Cir. 2006). Similarly, the First Circuit has described two problems in assessing the validity of warrants: "whether the warrant supplies enough information to guide and control the agent's judgment in selecting what to take and "whether the category as specified is too broad in the sense that it includes items that should not be seized." United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999).[7]

The level of specificity required in a warrant "varies depending on the circumstances of the case and the type of items involved." Hill, 459 F.3d at 973 (internal citations omitted). Furthermore, "[t]he requirement of particularity must be assessed in terms of practicality." United States v. Summage, 481 F.3d 1075, 1079 (8th Cir. 2007). In determining whether a warrant is sufficiently specific, a court should consider "whether it was reasonable to provide a more specific description of the items at that juncture of the investigation." United States v.

[7] The First Circuit Court of Appeals has further acknowledged that courts have at times "been unclear [in their opinions] on the difference between particularity and overbreadth," but that they "remain two distinct parts of the evaluation of a warrant for the Fourth Amendment purposes." United States v. SDI Future Health, Inc., 568 F.3d 684, 702 (9th Cir. 2009).

Richards, 659 F.3d 527, 541 (6th Cir. 2011) (citing United States v. Meek, 366 F.3d 705, 716 (9th Cir. 2004)).

There is no binding precedent in the military or in federal courts that states all search authorizations must contain a date limitation. As Appellant acknowledges, temporal limitations may be a relevant consideration in evaluating a warrant's validity, and analysis on case-by-case basis is appropriate. (App. Br. at 21.) However, the absence of a time or date limitation does not render a warrant *per se* invalid. *See* United States v. Bucuvalas, 970 F.2d 937, 942 (1st Cir. 1992) ("Temporal delineations are *but one* method of tailoring a warrant description to suit the scope of the probable cause showing") (emphasis added).

a. The search authorization was not overbroad because, for all practical purposes, it already contained an implicit date limitation.

In determining whether the 9 November 2011 search authorization was overbroad, this Court must determine whether it adequately limited AFOSI to searching for only evidence for which there was probable cause to search. *See* United States v. Leary, 846 F.2d 592, 605 (10th Cir. 1988) ("a search warrant is also impermissibly overbroad if it authorizes the search and seizure of evidence that is not supported by probable cause.") First and foremost, the 9 November 2011 search authorization already imposed an implicit date limitation on the agent's search. The search authorization allowed AFOSI to search for and seize online communications that were evidence of Appellant's violation of Florida

Statute 847.0135. In order to violate this statute, Appellant would either have to travel within Florida, to Florida, or from Florida, or cause another to do so. The record indicates that Appellant moved to Tyndall Air Force Base, Florida from Travis Air Force Base, California sometime between April and July 2010. (J.A. at 187, 424, 611.)

Since the AFOSI agents were restricted to looking for online communications that showed Appellant violating Florida law, they were also effectively restricted to searching for communications that took place between mid-2010 and 9 November 2011.[8] This time period coincided with the time period during which A.P. told investigators he had been communicating with Appellant online, from approximately April 2010 until 9 November 2011. Given the facts and circumstances of this case, the inclusion of the Florida statute in the warrant already limited the agents to searching only for evidence for which there was probable cause. This is not a situation where the search authorization "authorized a broader search than was reasonable given the facts in the affidavit supporting the warrant." *See* United States v. Ford, 184 F.3d 566, 576 (6th Cir. 1999).

Appellant cites Ford, 184 F.3d at 576, for the proposition that "failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad." However, although the Court in Ford

[8] There is no evidence in the record that Appellant was engaging with minors in Florida at any time before he moved there in mid-2010.

invalidated one portion of the warrant on that basis, it held that another portion of the warrant was still valid despite the lack of a time limitation because the warrant's "subject matter limitation . . . fulfills the same function as a time limitation would have done, by limiting the warrant to evidence of the crimes described in the affidavit." Id. at 578. As in Ford, the reference to the Florida statute in the 9 November 2011 search authorization fulfilled the same function as a date limitation would have done: it only allowed AFOSI to search for crimes with a nexus to Florida, which naturally limited the time frame to events occurring after Appellant moved there in mid-2010. Under the facts of this case, an explicit limitation on dates on the face of the warrant would not have changed the scope of what the agents were authorized to search for. In other words, date limitations would not have made the search authorization narrower than it already was.

The Tenth Circuit has indicated that "warrants for computer searches must affirmatively limit the search to evidence of specific federal crimes *or* specific types of material." United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005) (emphasis added). The search authorization in this case already accomplished both of these requirements by restricting the agents to searching for "online communications" that violated Florida Statute 847.0135, Traveling to Meet a Minor. That SA Nishioka understood the limited nature of the search authorization is evidenced by the fact that immediately upon finding child pornography, *he*

suspended his original search and obtained another search authorization. As such, this was not a search authorization that allowed a limitless exploratory rummaging through Appellant's electronic devices for anything the agents desired to find. The search authorization was not overbroad.

b. The Fourth Amendment does not require that search authorizations contain any specific search methodology or protocol.

As a general proposition, this Court should note that "[f]ederal courts . . . have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers, because criminals can -- and often do -- hide, mislabel, or manipulate files to conceal criminal activity such that a broad, expansive search of the computer may be required." United States v. Bass, 785 F.3d 1043, 1049 (6th Cir. 2015) (internal citations omitted); *see also* United States v. Grimmett, 439 F.3d 1263, 1269 (10th Cir. 2006) ("we have adopted a somewhat forgiving stance when faced with a 'particularity' challenge to a warrant authorizing the seizure of computers.")

The granted issue also raises the question of whether a search authorization should restrict law enforcement agents to using a certain *search methodology* to ensure they only view evidence within a certain date range for which there is probable cause. However, as the Sixth Circuit has recognized, "the majority of federal courts have eschewed the use of a specific search protocol, and, instead, have employed the Fourth Amendment's bedrock principle of reasonableness on a

case-by-case basis." Richards, 659 F.3d at 538 (citing United States v. Stabile, 633 F.3d 219, 238-39 (3d Cir. 2011); United States v. Mann, 592 F.3d 779, 785-86 (7th Cir. 2010); United States v. Burgess, 576 F.3d 1078, 1092, 1094 (10th Cir. 2009); United States v. Khanani, 502 F.3d 1281, 1290 (11th Cir. 2007); Hill, 459 F.3d at 977; United States v. Adjani, 452 F.3d 1140, 1149-50 (9th Cir. 2006); United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005); Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001); Upham, 168 F.3d at 535.)

Federal courts do not require warrants to include search protocols for the same reason they reject particularity challenges to warrants: an expansive search of an electronic device may be wholly necessary to uncover evidence of crimes contained within. "Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent." Hill, 459 F.3d at 978.

As one court has noted, enforcing too stringent terms on searching a computer "would give criminals the ability to evade law enforcement scrutiny." United States v. Graziano, 558 F.Supp. 2d 304, 315 (E.D.N.Y. 2008). "In today's technological age, a computer should not be a safe-haven for criminals to hide evidence of their criminal activities by unnecessarily limiting law enforcement's ability to search only certain files/documents on a computer with a certain name or term, or located in a certain area of the computer hard drive." Id.

Similarly, the Tenth Circuit has acknowledged that "[i]t is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods -- that process must remain dynamic." Burgess, 576 F.3d at 1093. "It is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objective." Id. at 1094. *See also* Adjani, 452 F.3d at 1149-50. ("[t]o require such a pinpointed computer search, restricting the search to an email program or to specific search terms, would likely have failed to cast a sufficiently wide net to capture the evidence sought.")

Due to the nature of computer searches, there is always a possibility that, in conducting their search, law enforcement agents might encounter nonresponsive or irrelevant files. However, this possibility does not render a search authorization overbroad or the ensuing search unreasonable. "So long as the computer search is limited to a search for evidence explicitly authorized in the warrant, it is reasonable for the executing officers to open the various types of files located in the computer's hard drive in order to determine whether they contain such evidence." Richards, 659 F.3d at 540; *see also* Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976). ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized"); Guest, 255 F.3d at 325 ("Although

there were presumably communications on the computers that did not relate to the offenses [specified in the warrant] a search does not become invalid merely because some items not covered by a warrant are seized").[9]

As the Tenth Circuit has concluded, "in the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files." Burgess, 576 F.3d at 1094.

c. In general, warrants authorizing computer searches should not be required to include dates limitations.

There are two compelling reasons why law enforcement agents conducting computer searches should not be limited to searching for files within a certain date range. First, as some courts have noted, file dates on a computer may be manipulated or unintentionally changed. In United States v. Loera, 59 F.Supp. 3d. 1089, at *1153 (D. N.M. 20 October 2014), the court asserted, "[g]iven the ease with which an individual may change the file dates on his or her computer . . . [the warrant] could not have imposed a date restriction without running the risk of losing a significant amount of relevant data." Thus, searching for files by date alone may not yield incriminating evidence that is nonetheless present on a device.

[9] The Fourth Circuit has gone so far as to assert that due to the likelihood of mislabeled or concealed files, "a computer search must, by implication, authorize at least a cursory review of each file on the computer." United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010).

Likewise, in United States v. Will, 2015 U.S. Dist. LEXIS 79887 at *21 (N.D. W.Va. 19 July 2015), the district court rejected the argument that law enforcement should have restricted their search to files dated on or after the occurrence of the underlying crime, "because the designation or labeling of files on a computer can easily be manipulated." Id. quoting Williams, 592 F.3d at 522.

Second, a search restricted by a date range may not reveal incriminating evidence located in unallocated space on a computer. As Mr. Kleeh explained in his testimony, files found in unallocated space on a computer often do not have dates, times, or other metadata associated with them. (J.A. at 663, 698.) Moreover, if DCFL filtered files by date before sending the FDE back to AFOSI for review, files without metadata would not be captured. (J.A. at 703.)

In United States v. Otero, 563 F.3d 1127, 1131 (10th Cir. 2009), a law enforcement agent conducting the search of a computer pursuant to a warrant found incriminating evidence in unallocated space on the defendant's hard drive. The agent indicated that "a date restriction could not have been used in a search of unallocated space." In conducting a good faith exception analysis of the search, the Tenth Circuit found that the search methodology used by the agent was appropriately limited to searching for the items for which there was probable cause, even though the search methodology did not include a date restriction. Id. at 1135. The Court recognized that "a date restriction . . . would have been

impossible to apply in the search of the unallocated space where the two pertinent documents were found, and even in other portions of the hard drive and disks we do not know how effective the restrictor would have been." Id.

If appellate courts begin requiring date limitations in warrants for computer searches, it would unreasonably impede legitimate law enforcement investigations supported by probable cause. Furthermore, such a ruling would put child pornographers and other criminals on notice that they need only take the simple step of manipulating the dates of incriminating files to avoid being caught.

d. There was no compelling reason to apply a date restriction to the 9 November 2011 search authorization in this case.

Not only should date restrictions not be required for computer searches in general, a date restriction should not have been imposed in Appellant's case in particular. In this case, the evidence available to the law enforcement agents showed that Appellant had been communicating online with A.P. for approximately a year and a half to two years. It is reasonable to believe that in that time period Appellant might have deleted some evidence of online communications with A.P., either to attempt to conceal his criminal activities, or simply because of the general passage of time. This evidence may nonetheless still have been recoverable in unallocated space on Appellant's electronic devices. But, as Mr. Kleeh explained in his testimony during motions, there was a significant chance that a specific date and time would no longer be associated with such files.

(J.A. at 663, 698.) In addition, the affidavit related that Appellant gave A.P. a "cover story" to attempt to hide the true nature of their relationship. As such, it was reasonable to believe that Appellant would also try to hide evidence of their relationship on his electronic devices. Limiting the agents to searching only for files with certain dates or times could have caused the agents to miss incriminating evidence of Appellant's illicit online communications with A.P.

At the time they applied for the search authorization, the AFOSI agents had no way of knowing for certain whether Appellant had deleted evidence of his online communications with A.P., if evidence had been hidden and mislabeled, or if evidence still remained in allocated space on his computer. Therefore, at that juncture in the investigation, the 9 November 2011 search authorization could not have reasonably or practically been more specific in directing the agents to search only for files containing a certain date. *See* Richards, 659 F.3d at 541; Bass, 785 F.3d at 1049 (warrant not overbroad where officers could not have known where evidence was located on device or in what format). In conducting his search, SA Nishioka was searching for and found pictorial evidence of Appellant's online communications with A.P. Thus, it was reasonable for SA Nishioka to continue to open files in the unallocated "pictures" folder on the FDE in order to determine whether they contained similar evidence.

In short, a date restriction on the 9 November 2011 search authorization could have caused the agents to miss incriminating evidence of Appellant's communications with A.P. that was otherwise within the scope of the search authorization, and it was reasonable for the magistrate not to impose one.[10] Since the search authorization was not overly broad, the search of Appellant's hard drives which ultimately led to the discovery of child pornography was entirely lawful.[11]

---

[10] This Court should note that the affidavit accompanying the search authorization did specifically inform the magistrate of the relevant time frame of Appellant's alleged crimes. Nonetheless, it was well within the magistrate's discretion to issue a search authorization without a date limitation. *See* Clayton, 68 M.J. at 423 ("resolution of doubtful or marginal cases should be largely determined by the preference for warrants and close calls will be resolved in favor of sustaining the magistrate's decision.")

[11] Although not directly encompassed by the granted issue in this case, the United States notes that SA Nishioka was reasonably and appropriately conducting a search within the scope of the search authorization when he discovered the child pornography. SA Nishioka's initial discovery of child pornography was covered by the plain view doctrine because (1) SA Nishioka was lawfully searching Appellant's computer within the scope of the search authorization when the first image of child pornography was in plain view; (2) the incriminating nature of the image was immediately apparent; and (3) based on the search authorization, SA Nishioka had lawful right of access to the image itself. Horton v. California, 496 U.S. 128, 136-37 (1990). After discovering the first image of child pornography, SA Nishioka immediately stopped his search and obtained another search authorization allowing him to continue to search for child pornography. These concepts are also relevant to the discussion of the good faith exception, and will be addressed in greater detail below.

2. The Good Faith Exception to the Exclusionary Rule Applies

In this case, the military judge correctly determined that even if the 9 November 2011 search authorization was overbroad, the good faith exception to the exclusionary rule applied.

Mil. R. Evid. 311(b)(3) provides that:

> Evidence that was obtained as a result of an unlawful search or seizure may be used if:
>
> (A) The search or seizure resulted from an authorization to search, seize or apprehend issued by an individual competent to issue the authorization under Mil. R. Evid. 315(d) or from a search warrant or arrest warrant issued by competent civilian authority;
>
> (B) The individual issuing the authorization or warrant had a substantial basis for determining the existence of probable cause; and
>
> (C) The officials seeking and executing the authorization or warrant reasonably and with good faith relied on the issuance of the authorization or warrant. Good faith shall be determined on an objective standard.

Mil. R. Evid. 311(b)(3), which is the military's "good faith exception" to the exclusionary rule, incorporated the Supreme Court's decisions in United States v. Leon, 468 U.S. 897 (1984) and Massachusetts v. Sheppard, 468 U.S. 981, 988 (1984).[12] United States v. Carter, 54 M.J. 414, 421 (C.A.A.F. 2001). This Court has indicated that Mil. R. Evid. 311(b)(3) is not intended to be a more stringent

[12] Sheppard holds that the good faith exception can be applied to warrants that violate the particularity requirement of the Fourth Amendment.

rule for the military than Leon and Sheppard, and therefore, the Rule should be construed "in a manner consistent with those decisions." Carter, 54 M.J. at 421.

In Leon, the Supreme Court determined that there were four circumstances under which the good faith exception does not apply: (1) a false or reckless affidavit; (2) a "rubber stamp" judicial review; (3) an affidavit so deficient in probable cause that a reasonable officer could not rely on it; and (4) a warrant so facially deficient – i.e., in failing to particularize the place to be search or the things to be seized – that the executing officers cannot reasonably presume it to be valid. Leon, 486 U.S. at 914-15.

a. None of the four prongs of Leon dictate against the application of good faith exception in this case.[13]

Appellant alleges that the affidavit accompanying the 9 November 2011 search authorization fails the third prong of Leon because there was no probable cause in the affidavit to support a conclusion that Appellant had committed any offense prior to April 2010. (App. Br. at 24-25.) In advancing this argument, Appellant appears to be conflating the affidavit and the search authorization. If there was a deficiency in one of the documents, it was with the search authorization, not the affidavit. By recounting the details of A.P.'s interview with law enforcement, the affidavit clearly established probable cause to believe that

[13] Appellant does not allege that either of the first two prongs of Leon is at issue in this case.

evidence of Appellant's illicit online communications with A.P. might be found on Appellant's electronic devices. The affidavit also did, in fact, establish a time frame for Appellant's crimes, stating that that Appellant and A.P. had been communicating for approximately one year prior to April 2011. (J.A. at 271.) The affidavit itself was not deficient in establishing probable cause to search Appellant's electronic devices for online communications in violation of Florida Statute 847.0135. The AFOSI agents could have reasonably relied on it in executing the search authorization.

Appellant next complains that the search authorization fails the fourth prong of Leon because it permitted examination of all electronic devices found in Appellant's home, irrespective of the dates of the files contained therein. (App. Br. at 25.) Even assuming that the search authorization was overbroad in failing to contain date limits, it was not so facially deficient that the AFOSI agents could not have reasonably presumed it to be valid. There is no binding law in the military or the Supreme Court that requires all search authorizations to contain date limitations or that even establishes when date limitations would be required. Therefore, a reasonably trained officer would not have "known that the search was illegal despite the magistrate's authorization." Leon, 468 U.S. at 922, n.23. *See also* United States v. Buck, 813 F.2d 588, 592-93 (2d Cir. 2009) (applying the good faith exception where the law in the jurisdiction was unsettled and ambiguous as to

the particularity requirements at the time officers obtained the warrant). As further evidence of the AFOSI agents' intention to comply with the Fourth Amendment, SA Winchester also sought the opinion of the legal office in obtaining the 9 November and 10 November search authorizations, and was assured that probable cause existed to search Appellant's electronic devices for online communications. *See* Otero, 563 F.3d at 1134.

b. AFOSI confined its search to places it was reasonable to believe were covered by the 9 November 2011 search authorization.

The good faith exception assumes "that the officers properly executed the warrant and searched only those places and for those objects that it was reasonable to believe were covered by the warrant." Id. at 918, n.19. In this case, SA Nishioka initially limited his search to places it was reasonable to believe were covered by the search authorization. In his interview, A.P. did not specify all the means of online communications in which he and Appellant engaged. However, due to the nature of online communications in the 2010-2011 time period, it was reasonable to believe that Appellant and A.P. might have exchanged pictures online or that there might be picture evidence of their communications. As Mr. Kleeh testified at trial, certain online chat programs will store pictures that are transferred between users. (J.A. at 690.) *See also* United States v. Crespo-Rios, 645 F.3d 37, 44 (1st Cir. 2011) ("a chat transcript, which begins as text, could be converted into an image and saved as an image file.")

Thus, searching in a folder and subfolders labeled "pictures" was well within the scope of the search authorization. The reasonableness of SA Nishioka's decision to search in the "pictures" folder is reinforced by the fact that, in doing so, he found a screenshot of a Skype chat between Appellant and A.P. This was exactly the type of evidence of "online communications" between Appellant and A.P. that was contemplated by the search authorization.

Appellant contends that the good faith exception should not apply because SA Nishioka testified at the Article 32 hearing that during his December search of the FDE, he was "only looking for communications between Appellant and A.P. or the little brothers." (App. Br. at 25.) Appellant is correct in asserting that the 9 November 2011 affidavit did not established probable cause to search for evidence of crimes against the other little brothers.

However, SA Nishioka's testimony does not change the fact that when he found the child pornography, he was still searching in a location (a folder of "pictures" from unallocated space) where it was objectively reasonable to search for evidence related to A.P. "[A]n investigator's subjective intent is not relevant to whether a search falls within the scope of a search warrant." Stabile, 633 F.3d at 240 (citing Garrison, 480 at 84). *See also* Horton, 496 U.S. at 138 ("The fact that an officer is interested in an item of evidence and fully expects to find it in the course of a search should not invalidate its seizure if the search is confined in an

area and duration by the terms or a warrant or a valid exception to the warrant requirement.) Since SA Nishioka only searched in folders reasonably encompassed by the search authorization, under Leon, the good faith exception is still available.

c. AFOSI demonstrated good faith by seeking a second search authorization after finding evidence they believed to be outside the scope of the original authorization.

As a final indicator of AFOSI's good faith in executing the search authorization, this Court should consider that upon finding evidence of child pornography, SA Nishioka immediately suspended his search, consulted the legal office and sought another search authorization. This demonstrates that SA Nishioka knew he was not allowed to exceed the scope of the search authorization, and was determined not to do so. *Compare* United States v. Walser, 275 F.3d 981, 987 (10th Cir. 2001) (commenting that agent "showed restraint by returning to the magistrate for a new warrant before commencing a new search for evidence of child pornography") *with* United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) (evidence of child pornography suppressed where agents exceeded the scope of the original warrant and failed to obtain a second warrant), and United States v. Osorio, 66 M.J. 632 (A.F. Ct. Crim. App. 2008) (same); *see also* Riccardi, 405 F.3d at 864 (by consulting the prosecutor about the scope of the warrant, the officers "showed their good faith in compliance with constitutional requirements.")

d. The deterrent effect of applying the exclusionary rule in this case would not outweigh the substantial costs to the justice system of suppressing this evidence.

Ultimately, the exclusionary rule "cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity." Leon, 468 U.S. at 918-19. "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." Herring v. United States, 129 S.Ct. 695, 702 (2009); *see also* Hudson v. Michigan, 547 U.S. 586, 595 (2006) (recognizing that "the exclusion of relevant incriminating evidence always entails . . . the risk of releasing dangerous criminals into society"). "When police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs." Davis v. United States, 564 U.S. 229, 238 (2011). On the other hand, "when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way." Id.

In this case, the AFOSI agents sought the counsel of the legal office, obtained a search authorization from the base magistrate, confined their search to the terms of the search authorization as written, and stopped when they found

evidence outside the scope of the search authorization to obtain a second search authorization. This was not a deliberate, reckless, or grossly negligent disregard for Appellant's Fourth Amendment rights. This was good, reasonable, and prudent law enforcement activity and not the type of "flagrant or deliberate violation of rights" that the exclusionary rule was intended to deter. *See* Otero, 563 F.3d at 1134 (citing Herring, 129 S.Ct. at 702). The costs of imposing the exclusionary rule in this case would mean a convicted child molester and possessor of child pornography would be released back into society. Even if the search authorization was deficient in failing to include date limitations, the costs of applying the exclusionary rule heavily outweigh any deterrent effect that suppression of the evidence would have.

3. Assuming the search authorization contained the date limitations Appellant claims are required, the child pornography on Appellant's devices would have been inevitably discovered.

Even if the 9 November 2011 search authorization had limited AFOSI to searching for online communications between April 2010 and 9 November 2011, SA Nishioka would have inevitably discovered child pornography on Appellant's electronic devices through the lawful execution of that search authorization. The inevitable discovery doctrine is an exception to the exclusionary rule that provides for "admission of evidence that, although obtained improperly, would have been obtained by another lawful means." Hoffmann, 75 M.J. at 124 (internal citations

omitted); Mil. R. Evid. 311(c)(2). In order for the inevitable discovery doctrine to apply, the government must establish by a preponderance of the evidence that "when the illegality occurred, the government agents possessed or were actively pursuing, evidence or leads that would have inevitably led to the discovery of the evidence and that the evidence would inevitably be discovered in a lawful manner had not the illegality occurred." Hoffmann, 75 M.J. at 124-25 (internal citations omitted).

The Court of Appeals for the First Circuit has applied the inevitable discovery doctrine under circumstances similar to those found in Appellant's case. In Crespo-Rios, 645 F.3d at 39, the defendant engaged in online sexual chats with an undercover agent who was posing as a twelve-year-old girl. On a government appeal, the Court considered whether there had been probable cause to search the defendant's computer for child pornography. Id. at 41. The Court found it unnecessary to decide that question because the child pornography ultimately found on the defendant's electronic devices would have been inevitably discovered. Id. at 42. The Court reasoned that agents *did* have probable cause to search the computer for chats between the defendant and undercover agent and would have certainly pursued a warrant and a search for that evidence. Id. at 42. "When searching digital media for 'chats' and other evidence of enticement, government agents cannot simply search certain folders or types of files for key

words." Id. at 43. The search for such evidence had to account for mislabeled or concealed files, and thus "forensic experts would have thoroughly combed through files and would have inevitably discovered the child pornography that Crespo now seeks to suppress." Id. at 44."

Like in Crespo-Rios, the agents in this case still had probable cause to search for online communications between Appellant and A.P, which they believed to have occurred between April 2010 and November 2011. There is every indication in the record that the AFOSI agents were actively pursuing this investigation, and would have continued to seek a search authorization until one was granted. Assuming the agents were confined to searching for files within a certain date range, it would have still been reasonable and lawful for SA Nishioka to search in a folder of pictures labeled "unallocated" since those files likely no longer had dates associated with them. In combing through the "unallocated" image files, the AFOSI agents would have inevitably discovered Appellant's child pornography. Since the inevitable discovery doctrine applies, the evidence of child pornography and the fruits of any subsequent searches need not be suppressed.

The United States acknowledges that the evidence of child pornography from the Western Digital My Passport hard drive and the pictures of N.R. formed the basis of the all of the specifications of Charge I. Had it been error to admit that evidence, then Appellant would have been prejudiced. However, for the reasons

discussed above, the United States strongly contends that the initial search and all subsequent searches of Appellant's electronic devices were lawful because the 9 November 2011 search authorization was not overbroad, and, in any event, both the good faith exception to the exclusionary rule and the inevitable discovery doctrine would apply. There was no reason for the military judge to suppress these pieces of evidence, and Charge I and all of its specifications should be affirmed.

In sum, the military judge did not abuse his discretion by denying Appellant's motion to suppress. The Air Force Court of Criminal Appeals likewise correctly upheld the military judge's ruling. This Court should affirm AFCCA's decision below.

CONCLUSION

WHEREFORE the Government respectfully requests that this Honorable Court affirm the findings and sentence in this case.

MARY ELLEN PAYNE, Major, USAF
Appellate Government Counsel
Air Force Legal Operations Agency
United States Air Force
(240) 612-4800
Court Bar No. 34088

GERALD R. BRUCE
Associate Chief, Government Trial and
Appellate Counsel Division
Air Force Legal Operations Agency
United States Air Force
(240) 612-4800
Court Bar No. 27428

KATHERINE E. OLER, Colonel, USAF
Chief, Government Trial and
Appellate Counsel Division
Air Force Legal Operations Agency
United States Air Force
(240) 612-4815
Court Bar No. 30753

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the foregoing was delivered to the Court, to civilian appellate defense counsel, and to the Appellate Defense Division on 16 February 2017.

MARY ELLEN PAYNE, Major, USAF
Appellate Government Counsel
Air Force Legal Operations Agency
United States Air Force
(240) 612-4800
Court Bar. No. 34088

COMPLIANCE WITH RULE 24(d)

1. This brief complies with the type-volume limitation of Rule 24(d) because:

☒ This brief contains 8,810 words,

2. This brief complies with the typeface and type style requirements of Rule 37 because:

☒ This brief has been prepared in a monospaced typeface using Microsoft Word Version 2013 with 14 characters per inch using Times New Roman.

/s/_____
MARY ELLEN PAYNE, Major, USAF
Attorney for USAF, Government Trial and Appellate Counsel Division

Date: 16 February 2017

APPENDIX A

Summary of relevant evidence seized from Appellant

Date of Search Authorization	**Device Seized**	**Forensic Data Extraction(FDE)#/ Date FDE received by AFOSI**	**DCFL Identifier[1]**	**Relevant Evidence Found[2]**
9 Nov 11 (FL Statute 847.0135) (3 Jan 12 search authorization allowed search of these devices for CP)	Toshiba HD	FDE #2 (12 Mar 12)	Tag9_ItemB_HD_001	- Photos of N.R. offered in support of Charge I, Specs 2-6 **(Pros. Exs. 32-37)** - Images of CP in unallocated space offered under MRE 404(b) **(Pros. Ex. 40.)**
	Gateway HD	FDE #2 (12 Mar 12)	Tag9_ItemC_HD_001	- Photos of N.R. offered in support of Charge I, Specs 2-6 **(Pros. Exs. 32-37)** - Images of CP in unallocated space offered under MRE 404(b) **(Pros. Ex. 40.)**
	Western HD	FDE #1 (23 Dec 11)	Tag9_ItemA_HD_001	
	Maxtor HD	FDE #1 (23 Dec 11)	Tag9_ItemD_HD_001	- Images of CP in unallocated space offered under MRE 404(b) **(Pros. Ex. 40.)**
10 Nov 11 (FL Statute 847.0135) (3 Jan 12 search authorization allowed further search of this device for CP)	HP Pavilion Laptop	FDE #1 (23 Dec 11)	Tag2A_HD_001	- Photos of A.P. and screenshot of A.P. Skyping with Appellant[3] - Images of CP in unallocated space offered under MRE 404(b) **(Pros. Ex. 39.)**
12 Mar 12	HP Photosmart Digital Camera	FDE #3 (4 Apr 12)[4]	Tag7_MC_001	- Camera entered into evidence **(Pros. Ex. 41.)** - Analysis shows this was the camera used to take photos of N.R.
2 Apr 12	Western Digital My Passport HD	FDE #4 (6 Jul 12)[5]	Tag2_HD_001	- 13 thumbnail images of CP offered in support of Charge I, Spec 1. **(Pros. Ex. 38.)**

Abbreviations: CP = child pornography; HD = hard drive; DCFL = Defense Computer Forensic Laboratory; FL = Florida

[1] (J.A. at 241, 243-44, 257-58, 262, 577, 592.)
[2] (R. at 466-70; 532-33,540.)
[3] (J.A. at 521-22, 571, 761.)
[4] (J.A. at 208, 238.)
[5] (J.A. at 239, 581.)

APPENDIX B

UNITED STATES OF AMERICA, Plaintiff, v. DUANE DAVID WILL, Jr., Defendant.

CRIMINAL NO. 5:15-CR-6

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF WEST VIRGINIA

2015 U.S. Dist. LEXIS 79887

June 19, 2015, Decided
June 19, 2015, Filed

PRIOR HISTORY: *United States v. Will, 2015 U.S. Dist. LEXIS 79883 (N.D. W. Va., Apr. 29, 2015)*

COUNSEL: [*1] For Duane David Will, Jr., Defendant: Patrick E. McFarland, LEAD ATTORNEY, Patrick E. McFarland, PLLC, Parkersburg, WV.

For USA, Plaintiff: Stephen L. Vogrin, LEAD ATTORNEY, U.S. Attorney's Office - Whg, Wheeling, WV.

JUDGES: JOHN PRESTON BAILEY, UNITED STATES DISTRICT JUDGE.

OPINION BY: JOHN PRESTON BAILEY

OPINION

ORDER ADOPTING REPORT AND RECOMMENDATIONS

On this day, the above-styled matter came before this Court for consideration of the Report and Recommendation ("R & R") of the United States Magistrate Judge James E. Seibert [Doc. 22]. Pursuant to this Court's Local Rules, this action was referred to Magistrate Judge Seibert for submission of an R & R. An evidentiary hearing was held on April 14, 2015. The R & R was filed on April 29, 2015, wherein Magistrate Judge Seibert recommends that this Court deny the defendant's Motion to Suppress [Doc. 13]. The defendant timely filed his objections on May 13, 2015 [Doc. 23].[1] Pursuant to *28 U.S.C. § 636(b)(1)(C)*, this Court will review those portions of the R & R to which objections were made under a *de novo* standard of review. The remaining portions will be reviewed for clear error. After reviewing the record, for the reasons set forth below, this Court adopts the Report and Recommendations.

1 [*2] This Court notes the defendant submitted an Amended Objection [Doc. 24] on May 14, 2015, which does not make any substantive changes, but rather seeks to correct typographical errors as the originally submitted Objection was discovered to be a rough draft. To the extent the defendant seeks this Court's leave to amend his objections, the same is hereby GRANTED.

I. BACKGROUND

On February 4, 2015, the defendant was named in a one count indictment plus forfeiture allegations charging him with possession of child pornography, in violation of *18 U.S.C. §§ 2252(a)(5)(B), (b)(2)*. [Doc. 1]. The defendant moves this Court to suppress all evidence seized by officers during the execution of the April 29,

2014, search warrant. [Doc. 13]. The search warrant authorized a search of the defendant's home to seize "[a]ny and all computers, hard drives, cell phones, digital media storage devices located on the property." Def. Ex. 2 [Doc. 21-1].

For the most part, the defendant agrees with the Findings of Fact contained in the R & R. This section will discuss the factual findings set forth in the R & R and also the facts not mentioned in the R & R, upon which the defendant relies.

A. Facts Supporting Search Warrant

On April 15, 2014, Deputy Shawn [*3] Mayle of the Marshall County, West Virginia Sheriff's Department was stationed at John Marshall High School as a resource officer. That day, Deputy Mayle was approached by a female student from the high school. Mayle Aff., Apr. 29, 2014 [Doc. 21-1]. The student advised Deputy Mayle that, on April 9, 2014, Defendant Will, a teacher at John Marshall High School, put his arms around the student and attempted to kiss her. *Id.* During Deputy Mayle's investigation of this alleged incident, he interviewed other potential witnesses. As a result of his investigation, Deputy Mayle filed a criminal complaint of misdemeanor battery[2] against Will and sought a search warrant for certain electronic devices in Will's home. Def.'s Ex. 1, 2 [Doc. 21-1]. Deputy Mayle's affidavit stated:

> On April 15, 2014, I Deputy Shawn Mayle the resource officer at John Marshall High School was made aware of a battery that had taken place at John Marshall High School. I spoke with the victim [redacted], she is a student at John Marshall High School. [Redacted] was assigned to go and take photo's for the yearbook, she was advised by the yearbook teacher to go to room 321 and take some pictures. [Redacted] felt uncomfortable [*4] going to this room because it belonged to Mr. Will, she advised me that earlier in the year when she won homecoming queen she was contacted by Mr. Will on face book and twitter and she said things that made her feel very uncomfortable and she has spent most of the year trying to avoid contact with him. [Redacted] asked her sister [redacted] to escort her to Mr. Will's room because she didn't know if there were students in there and she didn't want to be alone with him. When they got to his room they could see that there were other students in the room so they went in. [Redacted] said that Mr. Will approached them and stated "what do you need beautiful, and that I've missed you." [Redacted] stated she was embarrassed by his words and tried to ignore his comments and attempted to take some pictures of the class, Mr. Will continued and approached [redacted] and put his arms around her, trying to embrace her, as she pulled away Mr. Will attempted to kiss her, not knowing if he was trying to kiss her on the lips or not, [redacted] turned her head and his kiss landed on her cheek. Mr. Will's actions embarrassed, insulted, and made both girls feel very uncomfortable, [redacted] and her sister [*5] left the room feeling that [redacted] had been assaulted, and the actions of Mr. Will was very inappropriate, and in no way justified. This attack occurred on April 9th, 2014 at John Marshall High School, since then Mr. Will has attempted to contact [redacted] via face book and twitter, she advised me that she has not replied to any of his attempts and continues to ignore him. Mr. Will has been reported to the Board of Education by the administration at John Marshall High School for another incident that occurred at school, and since then Mr. Will has deactivated his face book account and the messaging has stopped for now.

Id. Officer Mayle then went to the Marshall County, West Virginia, magistrate to obtain the warrant. Based on the criminal complaint and attached affidavit, on April 29, 2014, a Marshall County Magistrate signed an arrest warrant and authorized a search of Will's home to seize "[a]ny an all computers, hard drives, cell phones, digital media storage devices located on the property." *Id.*

2 Battery, under *West Virginia Code § 61-2-9*, is defined as "[a]ny person who unlawfully and intentionally makes physical contact with force

> capable of causing physical pain or injury to the person of another or unlawfully [*6] and intentionally causes physical pain or injury to another person . . .."

That same day, officers traveled to Will's home to arrest him for battery and to execute the authorized search warrant. During the suppression hearing, Deputy Zachary Allman testified that he was the ranking officer during the execution of Will's arrest warrant and search warrant. At Will's home, officers knocked on the door, and, once Will answered, Deputy Allman informed him that he had a warrant for his arrest and a search warrant for his house. DVD Audio of Search Warrant, Apr. 29, 2014, Pl.'s Ex. 1 [Doc. 21-2].

During the execution of the search warrant, Deputy Allman explained to Will that:

> Apparently there was some correspondence, through the internet or text messages, or whatever. So what will happen with that stuff is basically we'll [inaudible] Facebook. Facebook keeps record of every message it's sent for like a year or so. And they'll extract basically every text message that you've sent and received for the past month, or however many months, even belated ones. Because your phone is like a little computer, you know? They extract all that information using what's called a "shell break." And the same [*7] thing with your other computers. And then they'll go through . . . each email and text and all that stuff one at a time to see if there's anything in there that's inappropriate or whatever.

Id. Officers seized the following items from Will's home: (1) an Apple iPhone 4; (2) an HP Pavilion DV6000 PC; (3) an Amazon Kindle; (4) an Apple iPad; (5) a Dell Inspiron "X16-96072"; and (6) a Dell Inspiron 537. Def.'s Ex. 4 [Doc. 21-1].

On April 30, 2014, officers downloaded content from Will's iPhone and iPad, and, subsequently, created a digital copy of the downloaded material. On May 15, 2014, officers downloaded content from Will's computers and provided hard drives to West Virginia State Trooper Matthew Scott Adams. Hr'g Tr. 21, Def.'s Ex. 5 [Doc. 21-1]. Deputy Allman testified that he gave Trooper Adams a "synopsis of the case and explained what exactly we were looking for." *Id.* Trooper Adams began his forensic examination of July 22, 2014. Def.'s Ex. 6. Trooper Adams conducted his analysis on "duplicate images of the original" hard drives provided by officers. *Id.* After his analysis, Trooper Adams turned over evidence to officers found on the hard drives along with a report. *Id.* Based on [*8] the evidence collected on the three hard drives, Will was charged with possession of child pornography on February 4, 2015.

B. Suppression Hearing Testimony

During the hearing, the Government asked Officer Mayle why a search of Will's home for computers was justified. Specifically, Officer Mayle was asked "[w]hy were you seeking to search and seize certain computer-type equipment?" Officer Mayle replied, "[a]fter speaking with the victim, it was -- I was advised that Mr. Will attempted to contact my victim through social media, so I was -- just for my investigation purposes, wanted to see if that information was still in the computers, just for my -- to make my case for battery stronger." Hr'g Tr. 11, April 14, 2015. Officer Mayle also testified:

> At the time of the search warrant, Mr. Will was not at work, and that's where most computers are kept, or at home in a home office, or if it's a laptop or something mobile. He was not at work at that time, so he would not have had anything in his a search of his classroom. It would have been at his residence.

Id.

Based upon the hearing testimony, there is no evidence that law enforcement limited their search of Will's computers and cell phone to Facebook and [*9] Twitter accounts or Will's web browsing history accessing those social media sites. Deputy Allman testified as to the process used to examine the computer files obtained during the search. The Marshall County Sheriff's Department created digital copies of the contents of Will's iPhone. *Id.* at 20. Then, Deputy Allman gave Trooper Adams the hard drives of the items seized. Deputy Allman testified that he gave Trooper Adams a "synopsis of the case and explained what exactly we were

looking for." *Id.* at 21. However, Deputy Allman testified "[a]cutally when we -- when Sergeant Adams does the download, he just does the download. It really doesn't vary much as to what -- exactly what documents we're looking for. He does an image of the hard drives pretty much the same in every case that I've worked where we've had to download a phone or a computer." *Id.* at 22.

Deputy Allman testified that officers attempted to obtain a search warrant from Facebook, however, Will's account had been deleted and officers "had not preserved the account, which means . . . there was nothing." *Id.* at 26. Nevertheless, Deputy Allman testified that there was a likelihood that relevant evidence could still be on the hard drives of Will's computers, agreeing that [*10] "just because the Facebook account was deleted with Facebook doesn't mean it was deleted on the particular person's computer." Deputy Allman also agreed that "it would be relevant to the investigation to get communications before and after an alleged battery between the victim and a potential suspect." Further, Deputy Allman testified that social media messages are often saved as images by the user taking a screen shot of the message. Hr'g Tr. 26.

II. DISCUSSION

The defendant makes several objections to the R & R. The defendant argues that the warrant is void for two reasons: 1) it lacked probable cause and 2) it was unconstitutionally general. The defendant argues that the insufficiency of the warrant precludes the invocation of the good faith exception. Defendant also argues that, even if the warrant was valid, the officers exceeded the scope of the warrant. The following section will discuss each argument in turn.

A. Validity of Warrant

Will attacks the validity of the warrant on two grounds. First, he argues that it lacked probable cause because it failed to identify a nexus between the designated crime of battery to the search of Will's home. Second, Will contends that the warrant [*11] did not describe the place to be searched with particularity. The *Fourth Amendment's* requirement that warrants "particularly describ[e] the place to be searched, and the persons or thing to be seized" is closely tied with the probable cause requirement because probable cause requires law enforcement show the magistrate that the items to be searched are connected with criminal activity.

The first issue presented is whether the magistrate acted properly in issuing the warrant for the search of computers inside Will's home. Although the defendant argues that there was no factual basis to support a nexus between the defendant's home and the alleged offense of battery, this Court disagrees.

The issuing magistrate is charged with determining, based on the totality of the circumstances, whether there is a "fair probability that contraband or evidence of a crime will be found in a particular place." ***Illinois v. Gates****, 462 U.S. 213, 238, 103 S. Ct. 2317, 76 L. Ed. 2d 527 (1983).* As the R & R discusses, "the task of a reviewing court is not to conduct a *de novo* determination of probable cause, but only to determine whether there is substantial evidence in the record supporting the magistrate's decision to issue the warrant." ***Massachusetts v. Upton****, 466 U.S. 727, 728, 104 S. Ct. 2085, 80 L. Ed. 2d 721 (1984).*

"[R]esidential searches have been upheld only where some information links the criminal [*12] activity to the defendant's residence." ***United States v. Lalor****, 996 F.2d 1578, 1583 (4th Cir. 1993)* (citing ***United States v. Williams****, 974 F.2d 480, 481-82 (4th Cir. 1992)).* Magistrate Judge Seibert found that a sufficient nexus between the alleged crime of battery and the defendant's home existed. He based this finding on several facts laid out in the supporting probable cause affidavit:

> (1) Will allegedly attempted to 'put his arms around [the victim], tr[ied] to embrace her, . . . [and] attempted to kiss her' before the victim turned her head away; (2) the victim was 'embarrassed' and 'insulted' by the incident and felt as if she 'had been assaulted;' (3) subsequent to this incident, Will attempted to contact the victim via social media; (4) the victim has refused to reply to any of Will's messages 'and continues to ignore him;' and (5) at the time of the executed search warrant, Will was on administrative leave and not working at John Marshall High School.

Because the affidavit stated that the defendant used social media to contact the victim, information from the defendant's computers was relevant to the prosecution for battery. Officer Mayle testified to the relevancy of the social media communications between the defendant and

victim, stating he "wanted to see if that information was still in the computers, [*13] just for my -- to make my case for battery stronger." Hr'g Tr. 11.

Defendant relies on persuasive authority that can be distinguished on the facts. In the instant case, the victim's statement that Will used social media to contact her created a nexus between the crime and the items to be searched (computers and electronic devices). *See* ***United States v. Shanklin****, No. 2:12CR-l62, 2013 U.S. Dist. LEXIS 161947, 2013 WL 6019216, at *8 (E.D. Va. 2013)* (holding that search of computers was not supported by probable cause because none of the supporting evidence "implicate[d] any multimedia device use . . .."); *see also* ***Dougherty v. City of Covina****, 654 F.3d 892, 898 (9th Cir. 2011)* (holding that probable cause for charges of sexual molestation did not authorize a search of the defendant's home for child pornography on defendant's computers because "[t]he affidavit contains no facts tying the acts of [the defendant] as a possible child molester to his possession of child pornography.").

Further, this Court finds that the issuing magistrate could reasonably infer that these devices may be found at the defendant's home. *See* ***United States v. Anderson****, 851 F.2d 727, 729 (4th Cir. 1988)* (holding reasonable inference that a suspect will keep firearms in home). In light of ***Anderson***, the issuing magistrate's inference that a person would typically use and [*14] keep computers at either their home or work is reasonable, and this Court will not disturb it. *See* ***Massachusetts v. Upton****, 466 U.S. 727, 733, 104 S. Ct. 2085, 80 L. Ed. 2d 721 (1984)* ("A deferential standard of review is appropriate to further the *Fourth Amendment's* strong preference for searches conducted pursuant to a warrant.").

Even if the warrant lacked probable cause, the good faith exception precludes the use of the exclusionary rule. The ***Leon*** Court "established a good faith exception to the exclusionary rule under which evidence obtained pursuant to a search warrant issued by a neutral magistrate does not need to be excluded if the officer's reliance on the warrant was objectively reasonable.'" ***United States v. Doyle****, 650 F.3d 460, 467 (4th Cir. 2011)* (internal quotations and citations omitted). The ***Leon*** Court identified four situations where the good faith exception would not apply:

> (1) if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth;
>
> (2) if "the issuing magistrate wholly abandoned his judicial role in the manner condemned in ***Lo--Ji Sales, Inc. v. New York****, 442 U.S. 319, 99 S.Ct. 2319, 60 L.Ed.2d 920 (1979)*";
>
> (3) if the affidavit supporting the warrant is "so lacking in indicia of probable cause as to render official belief in its existence [*15] entirely unreasonable;" and
>
> (4) if under the circumstances of the case the warrant is "so facially deficient--i.e., in failing to particularize the place to be searched or the things to be seized--that the executing officers cannot reasonably presume it to be valid."

United States v. DeQuasie*, 373 F.3d 509, 519-20 (4th Cir. 2004)* (quoting ***Leon****, 468 U.S. at 923*) (internal quotation marks omitted).

As stated above, Will argues the present case falls under situations 3 and 4. "When considering the application of the good faith exception, courts 'should examine the totality of the information presented to the magistrate in deciding whether an officer's reliance on the warrant could have been reasonable.'" ***Doyle****, 650 F.3d at 471*. The good faith exception will not endorse a search that is wholly unrelated to the crime designated in the warrant. ***Id.*** *at 472-73* (holding good faith exception not applicable when warrant sought permission to search for evidence of child pornography, but evidence in affidavit only supported child molestation). *Cf.* ***United States v. Lalor****, 996 F.2d 1578, 1583 (4th Cir. 1993)* (although insufficient probable cause, upheld search of home for drugs under the good faith exception when no evidence affidavit prepared in bad faith).

This Court agrees with the R & R that the good faith exception saves any defect in the warrant. [*16] Here, the issuing magistrate was presented with an affidavit that stated a teacher (defendant) battered a student at school. This student told Deputy Mayle that the teacher contacted her via Facebook or Twitter. Deputy Allman testified that relevant computer data is generally found on the suspect's

person or in their home. There are no allegations that the affidavit was prepared in bad faith or that the underlying information was unreliable.

Likewise, Will's argument that the warrant was "unconstitutionally general" also fails. Will argues that the warrant's authorization of "any and all computers, hard drives, cell phones, digital medial storage devices . . .." was overbroad because the probable cause supported only the search for social media messages sent by Will on or after April 9, 2014. Objections 9 [Doc. 23].

The *Fourth Amendment* requires "a particular description of the things to be seized. This particularity requirement is fulfilled when the warrant identifies the items to be seized by their relation to designated crimes and when the description of the items leaves nothing to the discretion of the officer executing the warrant." ***United States v. Williams***, *592 F.3d 511, 519 (4th Cir. 2010)* (internal citations and quotations omitted). As discussed above [*17] and in the R & R, the supporting affidavit[3] and warrant complies with these requirements.

> 3 The affidavit was incorporated into the search warrant. [Doc. 21-1].

B. Scope of Warrant / Plain View Doctrine

Finally, Will argues that, even in the event the search was lawful by either a valid warrant or under the good faith exception, law enforcement exceeded the scope of the warrant's authorization.[4] Will argues that the search warrant only authorized a limited search of his computers to social media messages sent by Will on or after April 9, 2014--not a search for child pornography. Objections 9 [Doc. 23].

> 4 Although closely related to Will's previous argument that the warrant fails for its lack of particularity, this issue will be examined separately because the good faith exception will not save a warrant that is improperly executed. *See* ***United States v. Angelos***, *433 F.3d 738, 746 (10th Cir. 2006).*

"A search conducted pursuant to a warrant is limited in scope by the terms of the warrant's authorization." ***United States v. Phillips***, *588 F.3d 218, 223 (4th Cir. 2009)*. Yet, courts consistently hold that "a search warrant is not to be assessed in a hypertechnical manner." ***United States v. Srivastava***, *540 F.3d 277, 289 (4th Cir. 2008)* (holding that law enforcement did not exceed scope of warrant after seizing personal records when warrant identified only business [*18] records).

This Court finds that ***United States v. Williams***, *592 F.3d 511 (4th Cir. 2010)*, is dispositive. In ***Williams***, after a church received several e-mail messages discussing molestation of boys that attended the church, the police investigated and determined the source of at least one email. ***Id.*** *at 515*. A detective submitted an affidavit for a warrant to search the defendant's home, which contained a description of the emails and stated that he believed probable cause existed for violations of two state crimes, including 1) prohibiting threatening communications to persons at elementary schools and 2) harassment by computer.[5] The magistrate judge issued the warrant that authorized the search and seizure of "[a]ny and all computer systems and digital storage media . . .." ***Id.*** The search of the computers revealed several images of child pornography. Child pornography was also found on a dvd seized from the home. ***Id.*** *at 516*.

> 5 For simplicity, this Court has abbreviated the names of the state laws.

The ***Williams*** Court addressed two issues: "(1) whether the government's search for and seizure of child pornography fell within the scope of the warrant's authorization; and (2) whether the evidence of child pornography was in any event properly seized under the plain-view [*19] exception to the warrant requirement." ***Id.*** *at 519*. The ***Williams*** Court upheld the search and seizure under both.

"Whether seized evidence falls within the scope of the warrant's authorization must be assessed solely in light of the relation between the evidence and the terms of the warrant's authorization." ***Id.*** *at 520- 21* (internal citations omitted). The Fourth Circuit held that law enforcement in ***Williams*** acted properly, reasoning that "[w]hile the warrant did not explicitly authorize a search for child pornography, it did authorize a search for instrumentalities for computer harassment . . .."

Will argues that the scope of the warrant was limited to a search related the designated offense-- battery. Unlike ***Williams***, the connection between the designated offense of battery and child pornography is more attenuated. In ***Williams***, the designated offense required the Government to prove the defendant used the

computer to harass the victim. Here, the only connection between the alleged battery and the defendant's computer was the use of a device to contact the victim via social media. Officer Mayle testified that Will's computer and other devices would have contained only limited relevant evidence to battery:

> Q. And [*20] you said that he Mr. Will contacted the alleged victim through Twitter or Facebook?
>
> A. She was unclear. She said one of the two.
>
> Q. I understand. But it was either Facebook or Twitter?
>
> A. Social media, yes, sir.
>
> Q. So there was no reason to look for anything relating to a battery charge or anything other than Facebook or Twitter, correct?
>
> * * *
>
> Q. I said if you were just trying to substantiate the charge of battery and that he may have had some contact with her over Facebook or Twitter, that's all you really needed to look to substantiate those charges of battery, correct?
>
> A. Social media, yeah.
>
> * * *
>
> Q. And so there would be no evidence of the crime of battery prior to April 9 of 2014, would there?
>
> A. I don't believe so.

Hr'g Tr. 14.

Although the connection between images for child pornography and the designated offense is not as strong as in ***Williams***, this Court further finds that, the search of the defendant's computers for images of child pornography falls under the plain view exception to the warrant requirement. In addition to holding that the execution of the warrant was valid, the ***Williams*** Court also held that the search and seizure of the images fell within the plain view exception.

Will [*21] argues that law enforcement should have restricted their search to files dated April 9, 2014, or later. Yet, this argument fails "because the designation or labeling of files on a computer can easily be manipulated to hide their substance." ***Williams****, 592 F.3d at 522*. As in ***Williams***, the three requirements for the plain view exception are met. As explained above, law enforcement was authorized to search Will's computers and other devices; thus, law enforcement was authorized to "open and cursorily view each file." Third, "when the officer comes upon child pornography, it become 'immediately apparent' that its possession by the computer's owner is illegal and incriminating." ***Id.*** (citing ***Horton v. California****, 496 U.S. 128 136, 110 S. Ct. 2301, 110 L. Ed. 2d 112 (1990))*.

III. CONCLUSION

For the foregoing reasons, this Court adopts the Report and Recommendation **[Doc**. **22]**. The defendant's Objections **[Docs. 23, 24]** are **OVERRULED** and the defendant's Motion to Suppress **[Doc. 13]** is **DENIED**.

It is so **ORDERED**.

The Clerk is directed to transmit copies of this Order to all counsel of record herein.

DATED: June 19, 2015.

/s/ John Preston Bailey

JOHN PRESTON BAILEY

UNITED STATES DISTRICT JUDGE