NO. _____

IN THE SUPREME COURT

OF THE UNITED STATES

MICHAEL HUNTOON,

Petitioner

vs.

UNITED STATES OF AMERICA,

Respondent

ON PETITION FOR WRIT OF CERTIORARI TO THE

UNITED STATES COURT OF APPEALS - NINTH CIRCUIT

PETITION FOR WRIT OF CERTIORARI

THE LAW OFFICES OF STEPHANIE K. BOND, P.C.
STEPHANIE K. BOND, ESQ
Attorney for Petitioner-CJA counsel,
Appointed under 18 U.S.C. § 3006A
177 North Church Avenue, Suite 611
TUCSON, ARIZONA 85701
(520) 624-2636

QUESTIONS PRESENTED FOR REVIEW

1. Whether or under what circumstances is this Court's ruling in Jacobsen applicable to computers in that a person loses any reasonable expectation of privacy contained on a computer, including private non-contraband, such that once it is seized by one agency pursuant to a warrant, it can be searched again for different contraband and private non-contraband by another agency years later without obtaining a new warrant?

2. Whether the lower court can interpret the meaning of words to determine probable cause existed in a search warrant without the false information when the issuing magistrate was not provided the information when determining whether or not to issue the warrant and then deny a Frank's Hearing?

TABLE OF CONTENTS

APPENDIX

TABLE OF CASES AND AUTHORITIES

CASES

STATUTES

RULES AND AUTHORITIES

PETITION FOR A WRIT OF CERTIORARI

Petitioner Michael Huntoon respectfully petitions for a writ of certiorari to review the judgement of the U.S. Court of Appeals for the Ninth Circuit in case number 18-10277.

OPINIONS BELOW

The Memorandum Opinion, issued December 16, 2019, of the Ninth Circuit Court of Appeals is unpublished and can be found at 18-10277. Pet. App. 1a. The relevant trial court proceedings and orders are unpublished and can be found at CR 16-00046-001-TUC-DCB. Pet App. 2a & 3a. The Judgement from the District Court issued July 24, 2018. App. 4a. Another relevant proceeding was State of Arizona v. Michael Huntoon, Pinal County Superior Court, Case No. CR201503282.

JURISDICTION

The opinion of the U.S. Court of Appeals for the Ninth Circuit was issued on December 16, 2019. Pet. App. 1a. This Court's jurisdiction is invoked under 28 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL PROVISION

The Fourth Amendment states in relevant part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause."

STATEMENT OF THE CASE

On December 15, 2014, the Tucson Police Department ["TPD"] began an investigation by using law enforcement software called "Torrential Downpour" ["TD software"] to download files from a peer-to-peer software network called "BitTorrent."[1] The TD software automatically connects to the BitTorrent network to look for certain "hash values" to find people who are sharing those "hash values." The TD software then reports the internet protocol [hereinafter "IP"] address of the computer, makes a connection to the other computer on the BitTorrent network, and then attempts to download files from that computer.[2]

On December 15, 2014, the TD software connected with IP address 67.1.114.24 and downloaded four files containing child pornography. The account holder for IP address was T.H. living on East Polly Drive, in Hereford, Arizona.[3] T.H. is the father of Huntoon. The IP address was outside TPD jurisdiction so the case file was transferred to Homeland Security Investigations ["HSI"].[4] HSI

---

[1]TT1, 63, 68-69. "CR" refers to the Clerk's Record, followed by the document number(s). "MH" refers to the Reporter's Transcript of the Motion Hearing followed by the date and page number(s); "TT" refers to the Trial Transcript followed by the day of Trial (1, 2, or 3) and page number(s).

[2]TT1, 73-74.

[3]TT2, 38, 144.

[4]TT1, 88; TT2, 144.

requested a search warrant for the residence which was served on November 16, 2015.[5]

When the search warrant was served, T.H. was the only resident.[6] During the search, a Sony USB flash drive ["the flash drive"] was seized from a desk in the detached garage.[7] The forensic analysis on the flash drive revealed nine deleted videos of adolescent females in various states of undress.[8]

On January 6, 2016, Huntoon was indicted on two charges: Distribution of Child Pornography in violation of 18 U.S.C. §2252(a)(2) and (b)(1); Knowing Access of Child Pornography in violation of 18 U.S.C. §2252A(a)(5)(B) and (b)(2). On March 21, 2018, a supervening indictment was filed charging Huntoon with an additional charge of Possession of Child Pornography in violation of 18 U.S.C. §2252A(a)(5)(B) and (b)(2).[9]

In unrelated investigations, the Chandler Police Department ["CPD"] and the Phoenix Police Department ["PPD"] had both intercepted files of child pornography from IP address 173.25.7.226 using TD software in August of 2015. These files were different files than the ones intercepted by TPD. PPD determined the IP

---

[5]TT2, 146.

[6]TT2, 49, 147.

[7]TT2, 46, 48, 150.

[8]TT2, 150-155.

[9]CR 121.

address was registered to C.F. ["Cheryl"] at a residence on Cedar Drive, in Apache Junction, Arizona, utilizing Mediacom Communications.[10]

PPD checked the Pinal County Assessor's records which identified Cheryl as only being associated with a residence on Smythe Drive in Apache Junction.[11] The relevant portion of the Search Warrant Affidavit ["SW Affidavit"] obtained by PPD on October 7, 2015 stated that Cheryl lived on Cedar Drive and MVD records indicated Huntoon, who was a registered sex offender, also resided there.[12] On October 20, 2015, at the request of PPD, Detective Southwick of the Apache Junction P.D. Sex Offender Notification Unit, ["AJPD"] went to the Smythe Drive residence and determined Cheryl resided there with her two grandchildren.[13] They also determined that Huntoon and his wife lived on the property in a fifth wheel.

The SW Affidavit further stated:

> Cheryl told Detective Southwick that she gets her internet in the home and that Michael Huntoon uses an Ethernet cable and runs it from the 5th wheel RV into her home and into the router. This cable connects Michael's laptop to the internet. Detective Southwick also met with Michael Huntoon and Michael stated that he and his wife reside in the 5th wheel at 1404 S. Smythe and he accesses the internet from the Ethernet cable from the RV to the house. He and his wife Courtney are not allowed into the home at 1404 S. Smythe if the children are there without Cheryl. All the residents access the mobile RV also parked on the property at the north end of the

---

[10]TT2, 107, 126-128.

[11]TT2, 127-128, 130-131.

[12]CR 100, SW Affidavit, 97.

[13]CR 100, SW Affidavit, 97.

lot.[14] (Emphasis Added)

PPD contacted Mediacom on October 22, 2015 and confirmed the only user under the account was Cheryl and that Mediacom could not determine where the modem was actually located.[15]

The following information was presented as evidence at a hearing on June 20, 2017, held in State of Arizona v. Michael Huntoon[16] but was not contained in the SW Affidavit. Detective Jeansonne of SJPD covertly made a video recording of their trip to the property in an effort to provide site intelligence to the search warrant team. The relevant portion of the recorded conversation between Southwick and Cheryl is as follows:

> Southwick: So do you have a router and a modem and all that?
> Cheryl: I don't honestly know.
> Southwick: He doesn't have his own connection out there as far as the hardware for a media account?
> Cheryl: No he's got it connected on mine.
> Southwick: He's got it connected to yours, alright.[17]

Southwick then went to the fifth wheel where Courtney and Huntoon resided and spoke with both of them.[18] Southwick and Huntoon did not discuss his internet connection. Also, not contained in the SW Affidavit was that PPD attempted to

---

[14]CR 100, SW Affidavit, 97.

[15]CR 100, SW Affidavit, 98.

[16]Pinal County Superior Court, Case No. CR201503282.

[17]CR 100; "Cheryl Video," 1.

[18]CR 100; "Cheryl Video," 1.

verify the MAC address on the Modem in order to confirm the IP address was correct.[19] PPD was not successful because, when he asked Cheryl, she did not know what a modem was and could not identify the modem even with a description and help over the phone. On multiple occasions she referred to "the black box."[20]

A search warrant was execute on the Smythe Drive property on October 28, 2015.[21] In a recorded interview of Huntoon, conducted while the search was taking place, Angel confirmed there was no ethernet cable linking Cheryl's house and his fifth wheel.[22] During the search, Huntoon's Toshiba laptop ["the laptop"] was located in the master bedroom inside the fifth wheel and seized.[23]

The SW authorized the Detective or the PPD to retain all evidence as provided by A.R.S. 13-3920.[24] The SW was returned on October 29, 2015.[25] In June of 2016, computer forensic examiner for PPD conducted a forensic exam of the laptop by making a forensic image file of the internal storage of the laptop and then examining it for images, videos, user accounts and different user activity.[26]

---

[19]MH 6/20/17, 62, 102.

[20]MH 6/20/17, 102-104, 106-107.

[21]TT2, 113-114.

[22]EH 6/20/17, 64.

[23]TT2, 114, 118.

[24]CR 100; SW, 87.

[25]CR 100; SW, 88.

[26]TT1, 53, 55-56.

At the request of Government, in January of 2018, PPD sent a copy of the laptop's hard-drive to HSI to conduct their own investigation.[27] HSI found the files downloaded by TPD in the recycle bin and in subfolders within the download folder.[28] HSI also found the deleted files on the flash drive in the download folder and subfolder.[29] HSI also determined that the standard settings under the "Torch" program were changed or modified and located several files containing personal information and correspondence.[30] HSI went back and examined the copy of the hard-drive again in 2018, three weeks prior to trial.

Prior to trial, Huntoon filed a Motion to Suppress Illegal Search and a supplemental motion.[31] As is pertinent here, Huntoon argued that the search of his computer by the Government violated the Fourth Amendment because it was conducted without a warrant and without any exigency otherwise justifying the search. Huntoon also argued that he was entitled to a Frank's hearing because the search warrant contained false information and when the false information was removed, no probable cause existed. The District Court denied the Motions and ruled "[t]here was a good state warrant. The feds then confined their search to what was covered by that warrant, and only with respect to any images on that computer,

---

[27]TT1, 56, 156.

[28]TT2, 156, 176.

[29]TT2, 176-177.

[30]TT2, 178.

[31]CR 66, 79, 80, 97, 100, 102.

and I don't think there's any privacy interest in the contraband that was found on that computer."[32] As is relevant here, the District Court relied on Supreme Court case United States v. Jacobsen, 466 U.S. 109 (1984) to support its holding.

A jury trial commenced on on April 17, 2018 and lasted three days.[33] The jury found Huntoon guilty of Distribution of Child Pornography in violation of 18 U.S.C. §2252(a)(2) and (b)(1) and Knowing Access of Child Pornography in violation of 18 U.S.C. §2252A(a)(5)(B) and (b)(2).[34] Huntoon was sentenced to 220 months incarceration on each count running concurrently, lifetime supervised release, and a $200 special assessment.[35]

Huntoon appealed his conviction to the U.S. Court of Appeals for the Ninth Circuit. On December 16, 2019, the Ninth Circuit denied Huntoon's appeal and upheld his conviction. The Ninth Circuit held, "it is well settled that "once an item in an individual's possession has been lawfully seized and searched, subsequent searches of that item, so long as it remains in the legitimate uninterrupted possession of the police, may be conducted without a warrant. United States v. Johnson, 820 F.2d 1065, 1072 (9th Cir. 1987) (quoting United States v. Burnette, 698 F.2d 1038, 1049 (9th Cir. 1983)." In reference to the issue regarding the search

---

[32]CR 142; RT 4/9/18, 20.

[33]CR 148-150.

[34]CR 154, 156; TT3, 107-108.

[35]CR 173.

warrant and denial of a Frank's hearing, the Ninth Circuit held that the detective had a "good faith belief that there was a 'hard wire' . . . connection . . ." and that "even without the allegedly false statements," there was probable cause. Pet. App. 1a.

REASONS FOR GRANTING THE WRIT

I. The Lower Courts Erroneously Applied Jacobsen to the Search of Huntoon's Laptop Claiming That a Person Loses Any Reasonable Expectation of Privacy Contained on a Computer Such That Once it Is Seized by One Agency Pursuant to a Warrant, it Can Be Searched Again for Different Contraband and Private Non-contraband by Another Agency Years Later Without Obtaining a New Warrant.

The Ninth Circuit and the District Court relied on Illinois v. Andrea, 463 U.S. 765 (1983) and United States v. Jacobsen, 466 U.S. 109 (1984) to support its holding claiming no "search" occurred because Huntoon no longer had a reasonable expectation of privacy in the laptop.

This Court should use this case to clarify if Jacobsen is applicable to computer searches and to provide guidance to the lower courts and the police regarding computer searches. Jacobsen was decided in 1984 when computers were just beginning to be used. In 1984, this Court could not have fathomed the extent to which the Jacobsen decision would be applicable. Jacobsen involved FedEx employees that opened a damaged package, found bags of white powder inside, and gave the package to the government. Id. at 111, 104 S.Ct. 1652. The DEA opened the package, examined the substance and conducted a chemical test which

confirmed it was cocaine. Id. at 111–12, 104 S.Ct. 1652. This Court held that no "search" within the Fourth Amendment occurred because there was a "virtual certainty" that the government could not have discovered anything else of significance in the package nor learned anything beyond what it had "already ... been told" by FedEx. Id. at 119, 104 S.Ct. 1652.

However, Huntoon's case is different. The privacy interests in a person's storage devices such as computers and cell phones have been recognized by this Court in that they "place vast quantities of personal information literally in the hands of individuals." Riley v. Cal. United States, 134 S.Ct. 2473, 2485, 189 L.Ed.2d 430 (2014) (cell phones). Computers, like Huntoon's laptop, contain "vast quantities of personal information" which is not contraband.

Courts across the country are attempting to apply Jacobsen but encountering problems as it relates to personal storage devices. These problems have caused a split in the Circuits regarding the applicability of Jacobsen as discussed in the Tenth Circuit's decision in United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016). Ackerman discussed two significant cases, United States v. Place, 462 U.S. 696, 103 S.Ct. 2637, 77 L.Ed.2d 110 (1983) and Walter v. United States, 447 U.S. 649, 100 S.Ct. 2395, 65 L.Ed.2d 410 (1980). In United States v. Place, this Court held that when a "well-trained narcotics detection dog" sniffed luggage, it did not offend the Fourth Amendment since the luggage was not opened and the "sniff" only suggested the presence or absence of contraband. Id. at 707, 103 S.Ct. 2637 (quoted in Jacobsen, 466 U.S. at 124, 104 S.Ct. 1652). However, in Walter v. United States,

447 U.S. 649, 100 S.Ct. 2395, 65 L.Ed.2d 410 (1980), this Court held the Fourth Amendment was violated when the police projected and viewed the films when the previous private search was much narrower and involved only an inspection of the labels on the outside of the film boxes. See Id. at 656–60, 100 S.Ct. 2395. According to the Ackerman Court, "[a]s interpreted by the Court in Jacobsen, the analytical thread stitching together these results and its own is the question whether 'the governmental conduct could [have] reveal[ed] nothing about noncontraband items'." Ackerman, 831 F.3d at 1308. Specifically, the Ackerman Court determined that in Place and Jacobsen, the government's conduct could not have revealed any information "about noncontraband items, so no 'search' took place within the meaning of the Fourth Amendment." Id. In contrast, the government's conduct in Walters could have revealed previously unknown information about noncontraband items, so a "search" occurred within the meaning of the Fourth Amendment. See, Id. Ackerman held, similar to Walters, that "opening the email and viewing the three other attachments—was enough to risk exposing private, noncontraband information that AOL had not previously examined" so a "search" occurred. Id. at 1306-7.

The Fifth Circuit used a similar analysis as Ackerman in United States v. Reddick, 900 F.3d 636 (5th Cir. 2018). Reddick found no "search occurred" when the detective opened the computer files because he "merely confirmed that the flagged file was indeed child pornography, as suspected." 900 F.3d at 639. The Reddick Court claimed the detective did not search any files other than "those

flagged as child pornography." Id.

The Ninth Circuit and the District Court did not apply the analysis found in Walters, Ackerman or Reddick so there appears to be a split among the circuits regarding the applicability of Jacobsen to computers and private information. In Huntoon's case, the Government did not search only for child pornography and they expanded the search conducted by PPD into Huntoon's private documents. The Government's Forensic exam[36] showed that the Government searched Huntoon's private documents to include his correspondence regarding the Estate of James P. Fine, Huntoon's resume, Huntoon's Oracle Ridge Mine identification, correspondence applying for a job, correspondence regarding his move to Pima County, a photo of Huntoon's social security card, Huntoon's electronic signature, and Huntoon's personal photographs. None of these documents involved child pornography. The Government's search was not limited to the search conducted by PPD nor was it limited to child pornography. Additionally, the report authored by PPD, dated October 20, 2016, did not include these additional private files with one exception: the list of "Torrent Active Transfers" lists a "resume;" however, there was no indication that PPD actually opened the file title "resume."[37] Therefore, the Government's search was not the same as PPD's search, it was not limited to child pornography and it examined private non-contraband items without a warrant.

In United States v. Adjani, the Ninth Circuit claimed "[t]he contours of [the

[36]CR 131, Ex 1.

[37]CR 131, Ex. 2.

Fourth Amendment's] protections in the context of computer searches pose difficult questions." 452 F.3d 1140, 1152 (9th Cir., 2006). "Computers are simultaneously file cabinets (with millions of files) and locked desk drawers; they can be repositories of innocent and deeply personal information, but also of evidence of crimes.... As society grows ever more reliant on computers ... courts will be called upon to analyze novel legal issues and develop new rules within our well established Fourth Amendment jurisprudence." Id. Additionally, this Court previously stated, "[w]he a person cannot know how a court will apply a settled principal to a recurring factual situation, that person cannot know the scope of his constitutional protection, nor can a policeman know the scope of his authority." New York v. Belton, 453 U.S. 454, 459-60 (1981). Consequently, this Court should accept Writ and determine if Jacobsen applies and if it does, are the Fifth Circuit and the Tenth Circuit correct in that an exception exists when the "search" exposes private, non-contraband items like in Huntoon's case.

The facts of this case would allow this Court to consider different variations on computer searches and deliver guidance. Here, the Government searched the laptop for the files discussed in the Federal Indictment which were not any of the listed files that were the subject of the State's search warrant. The Government searched the laptop for connections to the flash drive. They also searched for private documents and private photographs as discussed earlier herein. HSI also testified in detail about the changes Huntoon made to the "Torch" program and the personalization of the program. HSI searched the laptop's hard-drive twice.

Here, the Government displayed callous disregard for Huntoon's Fourth Amendment rights. No warrant was obtained and no exception to the warrant requirement was applicable. Although the Government had the opportunity to secure a warrant, it appears that it simply chose not to. Almost three years later, the Government elected to search Huntoon's laptop by other means in violation of Huntoon's Fourth Amendment Right.

Additionally, PPD did not have a lawful right to access the laptop and copy the hard-drive for purposes of giving it to HSI or any other agency. See e.g., U.S. v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1102 (9th Cir., 2008). In this case, the SW authorized the Detective or the PPD to retain all evidence as provided by A.R.S. 13-3920. [38] A.R.S. §13-3920 states, "All property or things taken on a warrant shall be retained in the custody of the seizing officer or agency which he represents, subject to the order of the court in which the warrant was issued, or any other court in which such property or things is sought to be used as evidence."[39] The Government did not possess such an order. The plain language of the search warrant excluded any one other than the Detective or PPD to have a copy.

Not only was providing a copy to HSI and/or the government not permitted under the search warrant, but it is also unreasonable under the Fourth Amendment. The Government's behavior in requesting a copy of the hard-drive without first obtaining its own warrant was egregious. The Government had a copy

[38]CR 100; Search Warrant, 88.

[39]CR 97, 6.

of the issuing judge's search warrant and SW Affidavit prior to requesting the evidence to know that they were not entitled to it under the original search warrant. The Government lacked a lawful right to seize a copy of the hard-drive and search it.

According to the doctrine of the "fruit of the poisonous tree," evidence may not be used if "`granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint.'" Wong Sun, 371 U.S. at 488 (citation omitted).

II. The Lower Courts Erred in Interpreting the Meaning of Words to Determine Probable Cause Existed in a Search Warrant Without the False Information When the Issuing Magistrate Was Not Provided the Information and to Deny a Frank's Hearing.

The Ninth Circuit and the District Court improperly applied this Court's rulings in Elkins v. United States, 364 U.S. 206, 80 S.Ct. 1437 (1960) and Franks v. Delaware, 438 U.S. 154 (1978) to Huntoon's case. This Court should use this case to provide guidance to the lower court's regarding the applicability of these important cases and if the lower court can interpret the meaning of the words to determine probable cause existed when the issuing magistrate was not provided the information in determining whether or not to issue the search warrant.

This Court determined in Elkins v. United States, " . . .that evidence obtained by state officers during a search which, if conducted by federal officers, would have violated the defendant's immunity from unreasonable searches and seizures under the Fourth Amendment is inadmissible . . . in a federal criminal

trial." 364 U.S. 206, 223 (1960). The ". . . federal court must make an independent inquiry, whether or not there has been such an inquiry by a state court, and irrespective of how any such inquiry may have turned out. The test is one of federal law . . ." Id. at 223-224.

A. The Lower Courts Erred in Finding Probable Cause Existed When it Determined the Meaning of Words That Were Not Presented to the Judge Who Issued the Search Warrant.

"[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment subject only to a few specifically established and well-delineated exceptions." Arizona v. Mincey, 437 U.S. 385, 390 (1978) (quoting Katz v. United States, 389 U.S. 347, 357 (1967); U.S. Const. amend. IV.; See also Riley v. Cal. United States, 134 S.Ct. 2473 (2014). "[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.' " Riley, 134 S.Ct. at 2483 quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006). "... reasonableness generally requires the obtaining of a judicial warrant." Id., quoting Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653 (1995).

Generally, a magistrate's finding of probable cause to issue a search warrant will not be overturned unless it is clearly erroneous. However, this rule does not apply when a trial court reviews an affidavit that was submitted to the magistrate and later found to have been supported by false statements. Elliott, 893 F.2d at 222. To determine if the affidavit sufficiently supports a finding of probable cause, the totality of the circumstances standard is used. Illinois v. Gates, 462 U.S. 213 (1983). A reviewing court must set the affiant's false statements to one side and

then determine whether the remaining content is sufficient to establish probable cause. See Franks v. Delaware, 438 U.S. 154, 156, (1978). If the affidavit is not sufficient, the warrant must be voided and the evidence suppressed. See Id.

In Huntoon's case, the defense showed that PPD included false statements in the SW Affidavit and the District Court agreed.[40] Specifically, PPD's Affidavit falsely stated that "Cheryl told Detective Southwick that she gets her internet in the home and that Michael Huntoon uses an Ethernet cable and runs it from the 5th wheel RV into her home and into the router."[41] The Affidavit further falsely stated that "this cable connects Michael's laptop to the internet." Lastly, the Affidavit falsely stated that "Detective Southwick also met with Michael Huntoon and Michael stated that . . . he accesses the internet from the Ethernet cable from the RV to the house."[42]

The SW Affidavit created a fictitious connection between Huntoon's residence and the router in Cheryl's residence via a fictitious ethernet cable. Cheryl never said Huntoon used her internet; instead, she agreed that Huntoon used her "media account." Furthermore, her actual statement to the detective on the phone demonstrated she did not understand if there was a modem or router in her house. Also, neither Cheryl nor Huntoon said what was stated in the SW Affidavit.[43]

---

[40]CR 142, 8-9.

[41]CR 100; SW Affidavit, 95.

[42]CR 100; SW Affidavit, 97.

[43]CR 100; MH 6/20/17, 41-42.

Southwick did not observe "any unique connections, any wire or cables coming from the fifth wheel."[44] He also did not put anything in his report about whether or not Huntoon had access to the internet.[45]

The District Court acknowledged that the statements in the SW Affidavit was false but claimed the false information did not affect probable cause.[46] The District Court incorrectly assumed that Huntoon was connected to Cheryl's internet service in some capacity. The District Court erroneously claimed "it is undisputed that the Defendant's laptop computer was connected to . . . [Cheryl's] internet service having the IP address corresponding to the search warrant."[47] However, the laptop's connection to the IP address was not determined until the forensic search was conducted several days after the search; therefore, this information should not be considered for purposes of probable cause. It is also disputed that PPD or SJPD, knew Huntoon's laptop was connected to the IP address prior to obtaining the SW. Southwick was the individual who spoke to Cheryl and Huntoon prior to PPD obtaining the SW. Southwick testified that he had not met the PPD detective prior to testifying in the State court hearing on June 20, 2017.[48] He also did not recall if he spoke to the PPD Detective about his contact with Cheryl and Huntoon or

---

[44]CR 100; MH 6/20/17, 44.

[45]CR 100; MH 6/20/17, 30-32.

[46]CR 142, 9-10.

[47]CR 142, 9.

[48]CR 100; MH 6/20/17, 43-44.

another detective.[49] Additionally, Cheryl actually said Huntoon was connected to her "Media account."[50] Southwick agreed that he did not use the word "internet" when speaking to Cheryl and asked her if Huntoon had "his own connection out there as far as the hardware for a media account?"[51] Southwick also acknowledged that he is not certain exactly what Mediacom connects but assumed it was internet and possibly television and telephone.[52]

"An officer has probable cause to conduct a search if a reasonably prudent person, based upon the facts known by the officer, would be justified in concluding that the items sought are connected with the criminal activity and that they would be found at the place to be searched." Gates, 462 U.S. at 213 (emphasis added). PPD falsely told the issuing judge an elaborate story about how exactly Huntoon was accessing the internet, when Southwick did not ask if or how Huntoon was accessing the internet.

The district court set aside part of the false statements but erred in attributing a fact (ie: that Huntoon was accessing the internet wirelessly) when that was presumably not known to PPD. Therefore, the District Court's ruling incorrectly left in the fact that "Cheryl told Detective Southwick that she gets her internet in the home and that Michael Huntoon uses . . . from the 5th wheel RV into

---

[49]CR 100; MH 6/20/17, 25-26, 33-35.

[50]CR 100; MH 6/20/17, 41.

[51]CR 100; MH 6/20/17, 39.

[52]CR 100; MH 6/20/17, 41.

her home and into the router."[53] The Ninth Circuit, in upholding the District Court's decision claimed the PPD detective "had a good faith belief that there was a 'hard wire' . . .connection" between Cheryl's residence and Huntoon's fifth wheel. Both courts made assumptions about the PPD detective's knowledge, without such testimony being presented. Also, the courts made assumptions about the language and its meaning when Southwick's recording of his conversation with Cheryl was not presented to the judge who issued the search warrant. Lastly, this information was presumably not told to the Detective for use in drafting his Affidavit because Southwick did not recall speaking to the Detective.

The District Court also left in the statement that Huntoon "stated . . . he accesses the internet from the RV to the house."[54] Southwick's report did not discuss if Huntoon had internet or not.[55] Southwick followed a checklist of questions and internet access was not on the checklist.[56] Southwick's report indicated that Huntoon had a hotmail account because that was a question on his checklist. Southwick did not know if he even asked Huntoon if he had computer access.[57]

After setting aside the false statements, the lower should have determined

---

[53]CR 142, 9.

[54]CR 142, 9.

[55]CR 100; MH 6/20/17, 31-32.

[56]CR 100; MH 6/20/17, 27-30.

[57]CR 100; MH 6/20/17, 28.

the facts in SW Affidavit would say the following:

> Detective Southwick went to . . . S. Smythe Drive and verified that Cheryl . . . along with two minor children under CPS care reside at . . . S. Smythe Drive. Cheryl . . . told Detective Southwick that her mailing address is . . . S. Cedar Drive but she and the two children reside in . . . S. Smythe Dr. She further told Detective Southwick that Michael Huntoon and his wife Courtney reside in the 5th wheel RV parked on the property at . . . S. Smythe Drive. Detective Southwick also met with Michael Huntoon. He and his wife Courtney are not allowed into the home at . . . S. Smythe if the children are there without Cheryl. All the residents access the mobile RV also parked on the property at the north end of the lot.

This does not establish probable cause to search Huntoon's fifth wheel.

Therefore, in denying Huntoon's Motion, the lower court erred when they inserted the fact that Huntoon had internet access into the Affidavit which is contrary to established case law. The Court cannot consider information not presented to the issuing judge in evaluating whether there was probable cause. See, United States v. Luong, 470 F.3d 898, 904-05 (9th Cir., 2006)(reviewing court may not consider information beyond the four corners of the Affidavit). Therefore, when the false information is removed from the SW Affidavit, there is no probable cause to search Huntoon's residence to which he has an expectation of privacy. Therefore, the search was invalid and the lower courts erred in failing to suppress the evidence as fruit of the poisonous tree. See, Wong Sun v. United States, 371 U.S. 471, 484-88 (1963).

B. The Lower Court Incorrectly Denied a Frank's Hearing since the Detective Misrepresented Material Facts in the Affidavit in Support of a Search Warrant in an Effort to Mislead the Issuing Court Regarding the Existence of Probable Cause.

In Franks v. Delaware, the Supreme Court held that affidavits containing reckless

or intentional false statements are subject to challenge by motion. If it is determined that the affidavit, without the challenged statements, does not establish probable cause, the remedy is suppression of the derivative evidence. Franks, 438 U.S. at 171-72. Even if probable cause existed and could have been shown in a truthful affidavit, the Franks error will not be cured. Baldwin v. Placer County, 418 F.3d 966, 971 (9th Cir., 2005). Misstatements or omissions in an affidavit are grounds for a Franks hearing even if the official at fault is not the affiant. United States v. DeLeon, 979 F.2d 761, 763-64 (9th Cir., 1992).

The defendant bears the burden of establishing that an affidavit fails to include information that would negate probable cause, including intentionally false statements or statements made with a reckless disregard for their truth. Franks, 438 U.S. at 171. A defendant must only produce a substantial showing of the falsity of the statements. United States v. Stanert, 762 F.2d 775, 781 (9th Cir., 1985). This showing can be made by affidavit, agents' reports, or other writings. Id., at 780. If these submissions contradict the allegations of the affiant, a hearing is required where the challenged information is material to the finding of probable cause. United States v. DiCesare, 765 F.2d 890, 895 (9th Cir., 1985). Statements contradicting the affiant are sufficient to obtain an evidentiary hearing. Id. There is an inference of recklessness when the false statements relate to critical information for probable cause. Rivera v. United States, 928 F.2d 592, 604 (2nd Cir., 1991); DeLoach v. Bevers, 922 F.2d 618, 622 (10th Cir., 1990); Hale v. Fish, 899 F.2d 390, 400 (5th Cir., 1990); United States v. Reivich, 793 F.2d 957, 961 (8th Cir., 1986).

According to the District Court, "[b]ut for the arguably glaring inconsistency between the affidavit statement and the conversation, the Defendant makes no offer of proof to accompany his allegation of deliberate falsehood or reckless disregard for the truth."[58] Appellant disagrees. Appellant showed from the sworn testimony of Southwick on June 20, 2017 and the transcript of Southwick's conversation with Cheryl, that Southwick did not know if he spoke to Angel or another Detective about the conversation, that Southwick did not specifically ask Cheryl about the internet but instead asked about her Media account, and that Southwick did not recall asking Huntoon about his internet access. When asked specifically if Southwick told Angel that Huntoon used an ethernet cable to run internet into his fifth wheel, Southwick said, "I don't know if I used the word Ethernet. I mean, I can't say positively I recall saying those exact statements . . ."[59]

Therefore, the defense made a substantial showing of the falsity of the statements or in reckless disregard for the truth which were material to the finding of necessity, thereby entitling Huntoon to a Franks evidentiary hearing.

CONCLUSION

For the forgoing reasons, the petition for writ of certiorari should be granted.

RESPECTFULLY SUBMITTED this 5th day of February, 2020.

Law Office of Stephanie K. Bond. P.C.

s/Stephanie K. Bond
STEPHANIE K. BOND
Attorney for Petitioner

---

[58]CR 142, 8.

[59]CR 100; MH 6/20/17, 36.

APPENDIX

NOT FOR PUBLICATION

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. MICHAEL HUNTOON, Defendant-Appellant.	No. 18-10277 D.C. No. 4:16-cr-00046-DCB-DTF-1 MEMORANDUM*

Appeal from the United States District Court
for the District of Arizona
David C. Bury, District Judge, Presiding

Argued and Submitted December 10, 2019
Pasadena, California

Before: N.R. SMITH and WATFORD, Circuit Judges, and HELLERSTEIN,** District Judge.

Michael Huntoon appeals his convictions for one count of distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2) and one count of

---

* This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

** The Honorable Alvin K. Hellerstein, United States District Judge for the Southern District of New York, sitting by designation.

knowing access of child pornography in violation of 18 U.S.C § 2252A(a)(5)(B). We have jurisdiction under 28 U.S.C. § 1291, and we affirm.

1. Huntoon argues that the district court erred in denying his motion to suppress, because the state search warrant was not supported by probable cause due to alleged misrepresentations in the affidavit. We review a district court's denial of a motion to suppress de novo, but its underlying factual findings for clear error. *United States v. Mayer*, 560 F.3d 948, 956 (9th Cir. 2009). "We review questions of probable cause de novo, but with 'due weight to inferences drawn from the facts by resident judges and local law enforcement officers.'" *United States v. Chavez-Miranda*, 306 F.3d 973, 978 (9th Cir. 2002) (alteration adopted) (quoting *Ornelas v. United States*, 517 U.S. 690, 699 (1996)). The district court found "no evidence of deliberate falsehood or reckless disregard for the truth," because Detective Angel had a "good faith belief that there was a 'hard wire' . . . connection between [the mother-in-law's] house and [Huntoon's] 5th wheel RV." The court further found that, even without the allegedly false statements, "there remains sufficient content in the warrant affidavit to support a finding of probable cause." Based upon these findings, the district court did not err in upholding the magistrate's determination of probable cause.

Huntoon additionally argues that the district court erred by denying his request for a *Franks* hearing. "We review the denial of a *Franks* hearing de novo, but review supporting factual determinations for clear error." *Id.* at 979. To be entitled to a *Franks* hearing, a defendant must make "a substantial preliminary showing that '(1) the affidavit contains intentionally or recklessly false statements, and (2) the affidavit purged of its falsities would not be sufficient to support a finding of probable cause.'" *United States v. Stanert*, 762 F.2d 775, 780 (9th Cir. 1985) (quoting *United States v. Lefkowitz*, 618 F.2d 1313, 1317 (9th Cir. 1980)). As determined above, the court's factual finding (that there were no intentional or reckless false statements) was not clearly erroneous. Thus, Huntoon failed to show he was entitled to a *Franks* hearing.

2. Huntoon argues that the district court erred by denying his motion to suppress, because the federal government relied on the state search warrant to search the laptop. First, the district court's finding that the federal search did not exceed the bounds of the state search warrant was not clearly erroneous. Further, it is well settled that "once an item in an individual's possession has been lawfully seized and searched, subsequent searches of that item, so long as it remains in the legitimate uninterrupted possession of the police, may be conducted without a warrant." *United States v. Johnson*, 820 F.2d 1065, 1072 (9th Cir. 1987) (quoting

United States v. Burnette, 698 F.2d 1038, 1049 (9th Cir. 1983)). State police served a valid search warrant on Huntoon's trailer at the Apache Valley property and seized his laptop. That laptop remained in the "legitimate uninterrupted possession of the police" and a mirror image of the laptop was given to Agent Nuckles for use in the federal investigation. Therefore, a new search warrant was unnecessary.

3. Huntoon argues that the court abused its discretion in admitting other-acts evidence: (a) a prior conviction from 1999 for child molestation, and (b) evidence stemming from his charges in Pinal County for possession of child pornography.

Federal Rule of Evidence 414(a) provides: "[i]n a criminal case in which a defendant is accused of child molestation, the court may admit evidence that the defendant committed any other child molestation. The evidence may be considered on any matter to which it is relevant." The district court did not abuse its discretion in determining that both sets of evidence were relevant. Because our circuit has held that prior child molestation convictions can be relevant to child pornography charges, the 1999 conviction was relevant. *See United States v. Thornhill*, 940 F.3d 1114, 1118 (9th Cir. 2019) (holding that a the defendant's "prior conviction was relevant because it tended to prove [the defendant's] sexual interest in children"). Similarly, because the Pinal County charges were nearly identical to the federal charges, the court was within its discretion to find they were relevant.

Relevant evidence is still subject to the balancing test under Federal Rule of Evidence 403. In evaluating whether to admit evidence of a defendant's prior acts of sexual misconduct, a court must consider the following factors: "(1) 'the similarity of the prior acts to the acts charged,' (2) the 'closeness in time of the prior acts to the acts charged,' (3) 'the frequency of the prior acts,' (4) the 'presence or lack of intervening circumstances,' and (5) 'the necessity of the evidence beyond the testimonies already offered at trial.'" *United States v. LeMay*, 260 F.3d 1018, 1027-28 (9th Cir. 2001) (quoting *Doe ex rel. Rudy-Glanzer v. Glanzer*, 232 F.3d 1258, 1268 (9th Cir. 2000)). The district court properly analyzed the *LeMay* factors to determine whether both sets of evidence should be admitted and did not abuse its discretion in finding the factors weighed in favor of admission.

4. Huntoon argues the district court abused its discretion by denying his discovery request. "We review the district court's Rule 16 discovery rulings for abuse of discretion." *United States v. Budziak*, 697 F.3d 1105, 1111 (9th Cir. 2012). "A defendant must make a 'threshold showing of materiality' in order to compel discovery pursuant to Rule 16(a)(1)(E)." *Id.* (quoting *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)). The district court did not abuse its discretion by finding that the evidence sought was not material, because Huntoon

had access to the laptop and his expert testified she had seen the software previously and was familiar with its use.

5. Huntoon argues the district court abused its discretion by denying his motion for a mistrial. "A mistrial is appropriate only where a cautionary instruction is unlikely to cure the prejudicial impact of the error." *United States v. Gann*, 732 F.2d 714, 725 (9th Cir. 1984). Because the court struck the previously admitted testimony and instructed the jurors to disregard any stricken testimony, the district court did not abuse its discretion by denying Huntoon's motion for a mistrial. We presume that the jury followed its instructions. *United States v. Olano*, 507 U.S. 725, 740 (1993).

6. There was not cumulative error.

AFFIRMED

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

United States of America, Plaintiff, v. MICHAEL HUNTOON, Defendant.	No. CR-16-00046-TUC-DCB (DTF) **REPORT AND RECOMMENDATION**

Before the Court is Defendant Michael Huntoon's (Huntoon) motions to suppress evidence (Docs. 66, 89, and 97) on referral by order of the Honorable David C. Bury, United States District Judge, pursuant to LRCrim 5.1 (Doc. 96). The government responded to Huntoon's motions (Docs. 79, 100, and 102). These matters came before Magistrate Judge Ferraro for hearing on March 15 and 20, 2018. (Docs. 108 and 114.) Neither the government nor Huntoon offered live testimony. Instead, both parties submitted exhibits for the Court to consider. As explained below, the Magistrate Judge recommends that the District Court, after its independent review, deny the motions (Docs. 66, 89, and 97).

I.

FACTUAL BACKGROUND

The relevant facts are not in dispute. This case involves child pornography distribution using peer to peer file sharing (P2P) software over the Internet. P2P file sharing is a method of communication available to Internet users through publically

available software. Computers linked together through the Internet using this software form a network. The P2P network enables its users to share designated files from their computer with anyone using compatible P2P software on the Internet worldwide.

Here, Huntoon was investigated by three different law enforcement agencies for sharing child pornography over the Internet via a P2P network; two municipal police departments within the State of Arizona and the Department of Homeland Security. All three investigations began after law enforcement officers, who at different times, discovered that child pornography was being shared on a P2P network believed to originate from Huntoon's computer. While State officers quickly discovered each other's investigation, the federal agents were unaware of the State investigations until a federal search warrant was executed at Huntoon's last known address. During the execution of this warrant, Huntoon's father told the federal agents his son was in State custody on State child pornography charges. The federal agents then discovered that Huntoon had been arrested after police found child pornography on his laptop that was seized pursuant to a State search warrant.

The federal search resulted in the seizure of numerous items including a USB flash drive and a Lenovo computer tower.[1] Huntoon is charged in a two count indictment with distribution of child pornography and knowingly accessing child pornography. (Doc. 1.) The indictment is based on the child pornography found on the USB flash drive (Count Two) and the child pornography that federal agents discovered was being shared by Huntoon over the Internet (Count One).

Nearly two years after the execution of the State search warrant and on the eve of the federal trial, State officers provided a mirror image of Huntoon's laptop to federal

---

[1] In the motions referred to the Magistrate Judge, Huntoon does not seek to suppress any evidenced seized in this search. However, at the hearing on March 15, 2018, the government announced its intention to offer evidence found on the Lenovo tower computer. Thus, on March 18, 2018, Huntoon moved to suppress the evidence found on the Lenovo tower computer (Doc. 104). This motion has not been referred to a magistrate judge due to the government's late notice of its intention to offer evidence found on the Lenovo tower computer which resulted in the late filing of Huntoon's motion to suppress this evidence. (*See* Doc. 115 at p. 53.)

agents. Without first obtaining a search warrant, federal agents examined the laptop for the purpose of providing trial testimony concerning the child pornography charged in the federal indictment. The warrantless search indeed revealed that many of the images found during the examination appeared to be the images shared by Huntoon on the P2P network alleged in Count One.

II.

DISCUSSION

Huntoon moves to suppress all evidence found on the laptop seized in the State search. Huntoon asserts this search warrant lacked probable cause and was supported by knowingly false information. Huntoon also argues the recent examination of the mirror image of his laptop by federal agents is presumptively unreasonable because they did not get a search warrant.

In the affidavit supporting the State search warrant, the affiant, Detective Frank Angel (Angel), Phoenix Police Department, describes P2P networks, file sharing and other technical aspects of his investigation. He then describes how he began his investigation using a law enforcement version of P2P software to obtain images of child pornography being publicly shared by the defendant over a P2P network. The affidavit describes the names and titles of the images he viewed and provided a description, which clearly showed the images and videos depicted the sexual exploitation of minors.

During Det. Angel's preliminary investigation of IP address associated with the child pornography, he discovered Detective William McDonald, Chandler Police Department, was also investigating the same IP address. According to the affidavit, Det. McDonald had obtained many of the same images Det. Angel had. Det. Angel took over the investigation because he was a member of the AZICAC[2] Task Force, which included the Pinal County Sheriff's Office, where the IP address was believed to be located.

According to the affidavit, Det. Angel learned that Huntoon, a registered sex offender, was living in a 5th wheel recreational vehicle next to a home at 1404 S. Smythe

[2] Arizona Internet Crimes Against Children

Drive, Apache Junction, Arizona. He also learned Huntoon had access to the Internet from that address. On October 27, 2015, Det. Angel obtained a state search warrant for the premises at 1404 S. Smythe Drive and the 5th wheel recreational vehicle parked on the property. The search warrant was executed on October 29, 2015, and items of evidentiary value were seized, including the laptop computer that is the subject of Defendant's motion to suppress.

Huntoon moves for an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), arguing Det. Angel, the affiant, made a knowingly false statement concerning how Huntoon acquired Internet access. Here, the affidavit describes how Det. Angel learned that Huntoon had access to the IP address located at 1404 S. Smythe Drive, as follows:

> Detective Southwick went to 1404 S. Smythe Drive and verified that Cheryl Friederich along with two minor children under CPS care reside at 1404 S. Smythe Drive. Cheryl Friederich told Detective Southwick that her mailing address is 1404 S. Cedar Drive but she and the two children reside in 1404 S. Smythe Dr. She further told Detective Southwick that Michael Huntoon and his wife Courtney reside in the 5th wheel RV parked on the property at 1404 S. Smythe Drive. Cheryl told Detective Southwick that she gets her internet in the home and that Michael Huntoon uses an Ethernet cable and runs it from the 5th wheel RV into her home and into the router. This cable connects Michael's laptop to the internet. Detective Southwick also met with Michael Huntoon and Michael stated that he and his wife reside in the 5th wheel at 1404 S. Smythe and he accesses the internet from the Ethernet cable from the RV to the house. He and his wife Courtney are not allowed into the home at 1404 S. Smythe if the children are there without Cheryl. All the residents access the mobile RV also parked on the property at the north end of the lot.

(Doc. 100-5 at p. 14.) According to Hunton, the conversation between Det. Southwick and Cheryl Friederich was recorded. A transcript of the conversation was attached to Huntoon's motion. The relevant portion of the transcript is as follows:

> Detective Southwick: So do you have a router and a modem and all that?
> Cheryl [Friederich]: I don't honestly know.
> [Detective]Southwick: He doesn't have his own connection out there as far as the hardware for a media account?

> Cheryl [Friederich]: No he's got it connected on mine.
> [Detective] Southwick: He's got it connected to yours, alright.

(Doc. 89 at Ex. 3.) The gravamen of Huntoon's falsity claim is that Det. Angel represented that Huntoon connected to the Internet via an Either net cable attached to Cheryl Freiderich's modem. (Cheryl Freidrech is Huntoon's mother.) What Cheryl Freiderich actually told detectives was that her son (Huntoon) received his Internet service from her but she did not know how he was connected.

The device Huntoon used to connect to his mother's Internet service is not material. The material fact is that Huntoon was connected to his mother's Internet service where the child pornography was received and shared. This was not in dispute at the motions hearing. When, as here, the offending material does not affect probable cause there is no need for a *Franks* hearing. *United States v. Reeves*, 210 F.3d 1041, 1044 (9th Cir. 2000). Accordingly, the Court denied the request for a *Franks* hearing.

This Court also assesses whether there is substantial evidence in the record supporting the judge's decision to issue the State search warrant. *See Massachusetts v. Upton*, 466 U.S. 727, 728 (1984) ("[T]he task of 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.") Here, the affidavit details the affiant's extensive training and experience investigating child pornography, describes Internet software often used to obtain and distribute child pornography on the Internet. The affiant then details the results of two State investigations, which included discovering specific videos depicting sexual exploitation of minors that were available for sharing on a specific IP address. The officers were advised by the Internet provider that this IP address was for Ms. Friederich's Internet connection. Ms. Friederich told investigators her son was connected to her Internet service. The Court finds that based on the affidavit there is substantial evidence in the record to support a fair probability that State investigators would find child pornography at the location to be searched and on Huntoon's laptop.

This Court also rejects Huntoon's contention the State warrant is invalid because there was no recording of Det. Angel being sworn in before the warrant was issued. In support of his argument, Huntoon merely alleges "upon information and belief" that there was an irregularity (Doc. 89-3 at p. 6). However, the State Justice of the Peace Magistrate signed the search warrant avowing that it was "SUBSCRIBED AND SWORN to before me this 27th day of October, 2015." (Doc. 100-5 at p. 5.) Huntoon has offered no evidence to the contrary. Accordingly, the Court will recommend that Huntoon's motion to suppress the results of the State search be denied without a *Franks* hearing.

Turning now to the federal agent's examination of the laptop seized pursuant to the State search, the Court assess whether a separate warrant was necessary. As mentioned above, about two years after State law enforcement officers searched Huntoon's laptop and found child pornography, federal agents received a mirror image of the laptop. Thereafter, the federal agents conducted their own examination of Huntoon's laptop without first obtaining a warrant. Huntoon argues this warrantless search violated his rights under Fourth Amendment.

Whether there was a Fourth Amendment violation turns on whether there was a search. A search occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. For example, in *Illinois v. Andreas*, 463 U.S. 765, 771 (1983), the Supreme Court held,

> The Fourth Amendment protects legitimate expectations of privacy rather than simply places. If inspection by police does not intrude upon a legitimate expectation of privacy, there is no "search" subject to the Warrant Clause. [Citation omitted] The threshold question, then, is whether an individual has a legitimate expectation of privacy in the contents of a previously lawfully searched container. It is obvious that the privacy interest in the contents of a container diminishes with respect to a container that law enforcement authorities have already lawfully opened and found to contain illicit drugs. No protected privacy interest remains in contraband in a container once government officers lawfully have opened that container and identified its contents as illegal.

Later, in *United States v. Jacobsen*, 466 U.S. 109, 114-15 (1984), employees of a private freight company opened a damaged package and found a white powdery

substance. They summoned federal agents who opened the package again and tested the powder. The test revealed that the package contained cocaine. The Supreme Court analyzed the effect a private search had on the reasonableness of the package owner's expectation of privacy. The Court determined:

> that agents of a private carrier independently opened the package and made an examination that might have been impermissible for a government agent cannot render otherwise reasonable official conduct unreasonable. The reasonableness of an official invasion of the citizen's privacy must be appraised on the basis of the facts as they existed at the time that invasion occurred.

Jacobsen, 466 U.S. at 115. The Court ultimately held that the federal agents did not "infringe any constitutionally protected privacy interest that had not already been frustrated as a result of the private conduct." *Id.* at 126.

This Court has determined that the State police detectives lawfully searched the laptop and found child pornography. As in *Jacobsen*, Huntoon's privacy interest had been lawfully frustrated. The distinction between a private citizen disrupting that expectation of privacy and the police lawfully doing so is of no legal significance. Once police lawfully discovered contraband on the laptop Huntoon lost his expectation of privacy, at least to the extent the laptop had already been searched by the police. Obviously, the police will not be required to seek another search warrant to examine the laptop in preparation for a State trial. Huntoon no longer had a reasonable expectation of privacy remaining in the contraband while the laptop was possessed by the police and he did not regain an expectation of privacy after a mirror image of the laptop was given to federal agents.

All that remains is to determine whether the federal agents' examination exceeded the lawful parameters of the State search warrant. Put differently, did the federal agents look into a part of the container not searched by the State detectives? The State search warrant permitted a search for:

- Any and all computer records, documents, and materials, including but not limited to computer towers (desktop), notebook computers (laptops) […]

- Any image or movie file containing or displaying minors engaging in any sexual activity or sexual exploitation contained within any media storage device. To include any computer media storage device, video tape, DVD and/or other media. […]
- Any documentation, written or electronic, showing the use of, possession of, or affiliation with any online peer to peer network […]

(Doc. 100-5 at p.3.) The affidavit limited the search to "not reading any electronic mail or chat conversations." *Id*. at p. 16.

In sum, the State search warrant authorized a robust search for any child pornography. The federal agents' examination may not exceed this authorization. Venturing into other areas would clearly implicate Huntoon's expectation of privacy in those unexplored places. Provided that the federal agents examined Huntoon's laptop only for child pornography there was "no search subject to the Warrant Clause." *Illinois v. Andreas*, 463 U.S. at 771. Thus, this Court will recommend that Huntoon's motion to suppress evidence found by federal agents on Huntoon's laptop be denied as to any child pornography recovered from the laptop.

Lastly, the Court disagrees with Huntoon's argument that in turning over the mirror image of his laptop to federal agents the terms of the search warrant were violated and that such an act "was also unreasonable under the Fourth Amendment." (Doc. 98 at p. 18.) The State search warrant provides:

> After completion of the evidence copies, the duplicate originals, or "forensic images" will be sealed and retained in evidence storage for later discovery and trial purposes. None of the contents of the duplicate original, other than those which may be required for prosecution will be displayed to any person other than the analyst and case agents, or otherwise disclosed, used or copied.

(Doc. 100-5 at p. 16.) The express terms of the State warrant do not prohibit State agents from turning over Huntoon's laptop to federal agents. The warrant permits use of Huntoon's laptop for prosecution. Nor was this language in the search warrant intended to restore any reasonable expectation of privacy that Huntoon previously had in the

laptop. The purpose of the restriction on the disclosure of Huntoon's laptop is to protect the identity of the victims of child pornography.

III.

RECOMMENDATION

Accordingly, it is recommended that, after an independent review of the record, the District Court **deny** Defendant's motions to suppress (Docs. 66, 89, and 97).

Pursuant to Federal Rule of Criminal Procedure 59(b)(2), any party may serve and file written objections within fourteen days of being served with a copy of this Report and Recommendation. A party may respond to the other party's objections within fourteen days. No reply brief shall be filed on objections unless leave is granted by the district court. If objections are not timely filed, they may be deemed waived.

Dated this 23rd day of March, 2018.

Honorable D. Thomas Ferraro
United States Magistrate Judge

WO

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

United States of America,

Plaintiff,

v.

Michael Huntoon ,

Defendant.

No. CR-16-00046-001-TUC-DCB (DTF)

ORDER

Procedural Background

On March 12, 2018, the Court denied the Defendant's Motion to Preclude evidence from and related to the Defendant's laptop computer, which was seized and searched in another case in Pinal County. The Court continued the trial date to Tuesday, April 17, 2018, to allow the Defendant time to have his expert examine the laptop and to afford him sufficient time to supplement his Motion to Suppress with any relevant evidence. The Court afforded the parties an opportunity to present evidence by referring the motion to Magistrate Judge Ferraro, along with a re-urged and related Motion for Disclosure.

The Magistrate Judge held two hearings. At the first, March 15, 2018, hearing, the parties informed the Court that the Defendant's expert was at that very time examining the laptop and the examination would continue the next day too. Defendant's counsel advised the Court that she would then have to consult with her expert to determine whether she could withdraw the Motion for Disclosure of the Government's

law enforcement software used to search the laptop or if her motion would stand. (TR (Doc. 106) 3/15/2018 at 14-15.) She would also know whether to supplement her Motion to Suppress with any evidence from the laptop, if any was discovered by her expert. Noting it would rely on the Defendant's expert testimony presented at the original hearing on January 4, 2018, on the Motion for Disclosure (TR (Doc. 74) 1/4/2018), the Magistrate Judge set an evidentiary hearing for March 20, 2018, to afford the parties an opportunity to supplement the record on both the discovery and suppression issues. *See United States v. Caymen*, 404 F.3d 1196, 1199 (9th Cir. 2007) (burden on proponent of motion to suppress to demonstrate that he has a reasonable expectation of privacy), *see also Coolidge v. New Hampshire*, 403 U.S. 443, 455 (1971) (where a search is conducted without a warrant, the government must demonstrate by a preponderance of the evidence that an exception applies).

Both parties supplemented their briefs related to the Motion to Suppress. (D's Supp. (Doc. 97); Gov't Resp. to Supp. (Doc. 100); Gov't Supp. (Doc. 102). On March 20, 2018, the Government filed a Motion to Continue, or Vacate as Moot, the hearing because Defendant had not disclosed the identity of the Defendant's expert nor the information he intended to elicit at the hearing. (Motion (Doc. 110)). Magistrate Judge Ferraro denied the motion. (Order (Doc. 111)). At the March 20, 2018, hearing neither party presented any evidence; argument by an attorney is not evidence. *Adams v. United States*, 152 F.2d 743, 744 (9th Cir. 1946), *see also Germinaro v. Fidelity National Title Insurance Company*, 2016 WL 5942236 *2 (Penn. October 13, 2016) (citations omitted) (explaining argument is not evidence, but is simply a characterization of the evidence).

The Court has reviewed the record presented to the Magistrate Judge, which primarily consisted of the state record including the warrant and affidavit executed in the Pinal County case. *See* (Transcript of Record (TR) Motion to Suppress hearing 3/15/2018 (Doc. 106); (TR hearing con't 3/20/2018 (Doc. 115); (Gov't Response (Doc. 100) at Ex. E: Maricopa County Search Warrant and Affidavit, Ex. F: TR 6/20/2017 hearing in Maricopa County Superior Court, Motion to Suppress, Ex. G: TR hearing

con't 9/1/2017). On March 23, 2018, the Magistrate Judge issued the Report and Recommendation (R&R). (R&R (Doc. 122)). He recommends that the Court deny the motion. For the reasons explained below, the Court adopts the recommendation and denies the Motion to Suppress the laptop computer evidence.

On March 13, 2018, during the pendency of this referral to the Magistrate Judge, the Government filed a Notice of Intent under Rule 414 and 404(b) to present evidence from a Lenovo computer tower which was seized and searched in this case. (Notice (Doc. 98)). The Defendant filed a Motion to Suppress the Lenovo computer. Because of the Government's late Notice, *see* (Order (Doc. 61) (setting motions in limine deadline for March 5, 2018)), the Defendant's expert had not yet examined it nor had the Government filed a Response to the Motion to Suppress it. The Magistrate Judge could not address the Motion to Suppress the Lenovo computer in his R&R. The motion is now fully briefed. The Court grants the Motion to Suppress the Lenovo computer, without reaching the merits. For reasons explained below, the Court finds the Defendant's disclosure of the Lenovo computer evidence, made on the eve of trial, is late, and it would be prejudicial to the Defendant to allow its introduction at trial on April 17, 2018.

The Report and Recommendation

The duties of the district court in connection with a R&R are set forth in Rule 59 of the Federal Rules of Criminal Procedure and 28 U.S.C. § 636(b)(1). The district court may "accept, reject, or modify, in whole or in part, the findings or recommendations made by the magistrate judge." Fed. R. Crim. P. 59(b)(3); 28 U.S.C. § 636(b)(1). Where the parties object to a R&R, "'[a] judge of the [district] court shall make a *de novo* determination of those portions of the [R&R] to which objection is made.'" *Thomas v. Arn*, 474 U.S. 140, 149-50 (1985) (quoting 28 U.S.C. § 636(b)(1)). When no objection is filed, the district court need not review the R&R *de novo*. *Wang v. Masaitis*, 416 F.3d 992, 1000 n. 13 (9th Cir. 2005); *United States v. Reyna-Tapia*, 328 F.3d 1114, 1121-22 (9th Cir. 2003) (en banc). Therefore, to the extent that no objection has been made, arguments to the contrary have been waived. *McCall v. Andrus*, 628 F.2d 1185, 1187

(9th Cir. 1980) (failure to object to Magistrate's report waives right to do so on appeal); *see also*, Advisory Committee Notes to Fed. R. Civ. P. 72 (citing *Campbell v. United States Dist. Court*, 501 F.2d 196, 206 (9th Cir. 1974) (when no timely objection is filed, the court need only satisfy itself that there is no clear error on the face of the record in order to accept the recommendation).

The parties were sent copies of the R&R and afforded an opportunity to object. Given the fast approaching trial date and the extensive briefing already existing related to the Motion to Suppress the laptop, the Court called for expedited briefing of Objections. (Order (Doc. 128) at 3) (allowing 7 days, with 2 for a Reply)). The Motion to Suppress the laptop computer evidence is now fully briefed. The parties have likewise completed briefing the Motion to Suppress the Lenovo computer.

The Fourth Amendment

A Fourth Amendment search occurs if the government, to obtain information, trespasses on a person's property to obtain that information. A Fourth Amendment search also occurs if the government violates a person's subjective expectation of privacy when such expectation is one that society is prepared to consider reasonable if infringed. *Florida v. Jardines,* 569 U.S. 1, 10 (2013) (describing reasonable-expectation test as "added to, not substituted for," the traditional property-based understanding of the Fourth Amendment) *see also* (R&R (Doc. 122) at 6 (citing *Illinois v. Andreas,* 463 U.S. 765, 771 (1983)).

"The touchstone of the Fourth Amendment is reasonableness . . .." *United States v. Knights*, 534 U.S. 112, 118 (2001)). "[S]earches pursuant to a warrant will rarely require any deep inquiry into reasonableness." *Illinois v. Gates*, 462 U.S. 213, 267 (1983) (White, J., concurring in judgment)). Nevertheless, both the scope of a seizure permitted by a warrant, and the reasonableness of government conduct in executing a valid warrant, can present Fourth Amendment issues. *United States v. Ganias,* 824 F.3d 199, 209-210 and n. 21-22 (2nd Cir. 2016) (en banc) (describing scope of the seizure as limited by the

prohibition on "general warrants," and the manner of execution of a warrant as being subject to later judicial review for reasonableness).

In *Ganias*, the court considered whether to suppress evidence found by the government pursuant to a 2006 search warrant issued to search mirrored images of hard drives seized and searched pursuant to a 2003 search warrant issued in an investigation into different conduct by a different individual. The court denied suppression based on the government's good faith execution of the second search warrant, but noted an awkward fit of container cases such as *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982) in the context of computer searches. *Ganias.* 824 F.3d at 208-221, *see also* (D's Objection (Doc. 131) at 6-11). The court in *Ganias* suggested that courts grappling with applying the Fourth Amendment to digital data soon recognize the distinctions, and should as best they can remain mindful of the privacy interests that necessarily inform the analysis. *Id.* at 218.

To do this, the *Ganias* court underscored the importance of a fully developed record regarding the technological specifics of the case in answering Fourth Amendment questions. *Id.* at 217. And, while resolving the *Ganias* case on the issue of good faith, it concluded "moreover, that [it] should not decide [the Fourth Amendment] question on the present record before it because the record did not permit a full assessment of the complex and rapidly evolving technological issues and the significant privacy concerns relevant to the inquiry. *Id.* at 220-221.

The Court is confident that an adequately developed record exists here to decide the Defendant's Fourth Amendment challenge to the search of the laptop computer, but finds that the record is not sufficiently developed to decide the merits of the Motion to Suppress the Lenovo computer.

The Magistrate Judge's R&R lays out the facts relevant to the Motion to Suppress the laptop evidence, (R&R (Doc. 122) at 1-3), and the Court does not repeat them. Suffice it to say that the Defendant's motion hinges on two assertions: 1) the state search warrant lacked probable cause because the affidavit contained knowingly false

information, and 2) the federal search of the mirror image of the laptop is presumptively unreasonable because the Government did not get a search warrant. *Id.* at 3. In his Objection, the Defendant adds a new argument not presented to the Magistrate Judge challenging the state search warrant as over-broad and lacking particularity. (D's Objection (Doc. 131) at 13-17.)

1. Motion to Suppress Laptop Computer and request for *Franks*[1] Hearing

The Court is aware that in respect to the first question it was previously urged and rejected in the state court case. But, "[i]n determining whether there has been an unreasonable search and seizure by state officers, a federal court must make an independent inquiry, whether or not there has been such an inquiry by a state court, and irrespective of how any such inquiry may have turned out. The test is one of federal law, neither enlarged by what one state court may have countenanced, nor diminished by what another may have colorably suppressed." *Elkins v. United States*, 364 U.S. 206, 223-224 (1960).

The duty of a court reviewing whether or not a warrant is supported by probable cause "is simply to ensure that the magistrate had a 'substantial basis for... conclud[ing]' that probable cause existed." *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983); *see also United States v. Kelley*, 482 F.3d 1047, 1050 (9th Cir. 2007) ("Normally, we do not 'flyspeck' the affidavit supporting a search warrant through *de novo* review; rather, the magistrate judge's determination should be paid great deference." (internal quotation marks omitted)). "Probable cause exists when 'there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Grubbs*, 547 U.S. 90, 95 (2006) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). "Whether there is a fair probability depends upon the totality of the circumstances, including reasonable inferences, and is a commonsense, practical question. Neither certainty nor a preponderance of the evidence is required." *United States v. Kelley*, 482 F.3d 1047, 1050

[1] *Franks v. Delaware*, 438 U.S. 154 (1978).

(9th Cir. 2007) (internal quotes omitted)). In the Ninth Circuit, a magistrate judge's determination that probable cause exists is accorded "great deference." *Id.*

In the Defendant's Objection, he complains that the Magistrate Judge erred by not conducting a *de novo* review. (Objection (Doc. 131) at 4 (citing *United States v. Elliott*, 893 F.2d 220, 222 (9th Cir. 1990)). The court in *Elliott* distinguished between a magistrate's determination that sufficient probable cause exists to issue a search warrant, which will not be overturned unless it is clearly erroneous, and a district court's review of the motion to suppress allegations of false statements and their effect on probable cause, which is an independent determination of the consequences of a fraud on the issuing magistrate-- which the magistrate was not in a position to evaluate. The latter is subject to *de novo* review while the former is not. The Magistrate Judge limited his *de novo* review to his assessment of "whether there is substantial evidence in the record supporting the judge's decision to issue the State search warrant." (R&R (Doc. 122) at 5.)

In his Objection, the Defendant reasserts that a glaring conflict exists between a statement in the warrant affidavit and a transcript of the conversation upon which the affidavit statement is allegedly based, and therefore the affidavit contains a false material statement. According to the Defendant the agent added false information about a fictitious Ethernet cable. (D's Objection (Doc. 131) at 2-6.) The warrant affidavit says that Cheryl Friederich, Defendant's mother-in-law, told police that the Defendant uses an Ethernet cable to run her internet service from her house to his 5th wheel recreational vehicle, parked on her property, where he lives with her daughter, the Defendant's wife. The transcript of the conversation between Friederich and the police officer, Detective Southwick, reflects that she said she didn't know whether she had a router or a modem but that the Defendant had his computer connected to her internet service. A subsequent conversation between Friederich and Detective Angel, the officer who prepared the warrant, made it abundantly clear that she "had no understanding of her internet service, the technology involved, including the modem, the router, and how the internet service was transmitted." (D's Supp. Motion to Dismiss (Doc. 97) at 5.)

The Defendant charges: "Detective Angel obviously added the false information to create probable cause for the judge to grant entry into Huntoon's separate residence. Detective Angel created a fictitious connection of the computer in Huntoon's residence to the modem and router in Friederich's residence via a fictitious Ethernet cable. This was the connection Detective Angel needed to get probable cause to enter Huntoon's separate residence." (D's Objection131) at 5.) But for the arguably glaring inconsistency between the affidavit statement and the conversation, the Defendant makes no offer of proof to accompany his allegation of deliberate falsehood or reckless disregard for the truth. (Reply (Doc. 134) at 7-8.) The evidence is, however, as follows: Detective Angel, who provided the affidavit, testified in the Maricopa County Superior Court that he based his affidavit on what he was told by Detective Southwick,[2] who was the police officer who interviewed Friederich. As described by the Superior Court, after watching the taped interview, "Detective Southwick asks the question, "He doesn't have his own connection out there as far as a hard wire" – his words "hard wire" . . . It's all under yours"? Ms. Friederich says, "No. He's got it connected to mine." (Gov't Response (Doc. 100) at Ex. G: Maricopa County Superior Court Motion to Suppress TR 9/1/2017 hearing (Doc. 100-7) at 25); *see also* (Gov't Response (Doc. 100) at Ex. C: TR Audio Recording (Doc. 100-3) at 2).[3] The Court finds no evidence of deliberate falsehood or reckless disregard for the truth. Based on his question, her failure to correct him regarding the notion of a hard wire connection, and her response that Defendant was connected to her internet service, Detective Southwick and Detective Angel, who relied on Southwick's representations, had a good faith belief that there was a "hard wire," i.e. Ethernet, connection between Friederich's house and the Defendant's 5th wheel RV.

In his Objection, the Defendant asserts the Magistrate Judge erred because he did not set aside the false statement to determine probable cause but instead inserted the fact

[2] Detective Southwick testified that he could not remember whether he spoke with Detective Angel or to another agent, but it is undisputed that he was the originating source for these details. (Gov't Response (Doc. 100) at Ex. F: Maricopa County Superior Court Motion to Suppress TR 6/20/2017 hearing (Doc. 100-6) at 18.)

[3] *But see* (R&R (Doc. 122) at 4) (relying misstated transcript of record as provided by Defendant in Supplement (Doc. 97) at 4.)

that Huntoon had internet access from Friederich's IP Address. "The Court cannot consider information not presented to the issuing judge in evaluating whether there was probable cause." (D's Objection (Doc. 131) at 5 (citing *United States v. Luong*, 470 F.3d 898, 904-05 (9th Cir. 2006) (explaining the reviewing court may not consider information beyond the four corners of the affidavit)). The Defendant argues that the *Franks* error cannot be cured even if probable cause existed and could have been shown in a truthful affidavit. *Id.* (citing *Baldwin v. Placer County*, 418 F.3d 966, 971 (9th Cir. 2005)).

The Court has reviewed the affidavit and finds that the Magistrate Judge did not add to it, he simply did not set aside the entirety of the information related to the Defendant's access to the internet service associated with Cheryl Friederich's IP address. The affidavit as redacted by the Defendant is highlighted, in comparison to the Court's set-aside of information reflected by the strikeouts, both are as follows:

> . . . **Cheryl told Detective Southwick that she gets her internet in the home and that Michael Huntoon uses ~~an Ethernet cable and runs~~ it from the 5th wheel RV into her home and into the router. ~~This cable connects Michel's laptop to the internet.~~** Detective Southwick also met with Michael Huntoon and **Michel stated that he and his wife reside in the 5th wheel at 1404 S. Smythe and he accesses the internet from ~~the Ethernet cable from~~ the RV to the house.**

The Court agrees with the Magistrate Judge. It is undisputed that the Defendant's laptop computer was connected to Friederich's internet service having the IP address corresponding to the search warrant. (TR (Doc. 115) 3/20/2018 hearing); (TR (Doc. 106) 3/15/2018). It is not material whether Defendant received his internet service through an Ethernet cable or Wifi modem; "[t]he material fact is that Huntoon was connected to his mother[in-law]'s Internet service where the child pornography was received and shared." (R&R (Doc. 122) at 5.) This fact remains after the allegedly false Ethernet information is set aside.

The Court agrees that with or without the Ethernet detail there is substantial evidence in the record supporting the state judge's issuance of the warrant. The affidavit reflected details of two state investigations, which had discovered specific videos depicting sexual exploitation of minors that were available for sharing on a specific IP

address associated with the property, 1404 S. Smythe Drive, Apache Junction, where Defendant, who was living on the property in a 5th wheel RV. Officers were told by the owner of the IP address that the Defendant was connected to her internet service. The Court agrees that the affidavit provided substantial evidence to support a fair probability that state investigators would find child pornography at the location to be searched. (R&R (Doc. 122) at 5.) The location included all the dwelling structures on the property, including the 5th wheel RV, and sheds and all computer equipment, including Huntoon's laptop.

The Court agrees with the Magistrate Judge that a *Franks* hearing is not required because even when the allegedly intentional and reckless false "Ethernet" statements are set aside, there remains sufficient content in the warrant affidavit to support a finding of probable cause. *Franks v. Delaware*, 438 U.S. 154, 171-172 (1978).

2. Government's Search of the Mirror Image of the Defendant's Laptop Computer

"[T]wo years after State law enforcement officers searched Huntoon's laptop and found child pornography, federal agents received a mirror image of the laptop. Thereafter, the federal agents conducted their own examination of Huntoon's laptop without first obtaining a warrant. Huntoon argues this warrantless search violated his rights under [the] Fourth Amendment." (R&R (Doc. 122) at 6.)

Having adopted Magistrate Judge Ferraro's recommendation to find that state police detectives lawfully searched the Defendant's laptop computer, the Court likewise adopts his conclusion that subsequently the Defendant no longer had any expectation of privacy in the contraband child pornography files. (R&R (Doc. 122) at 6 (citing *United States v. Jacobsen*, 466 U.S. 109, 114-115 (1984)).

As explained in the R&R, whether there is a reasonable expectation of privacy is determined by whether society is prepared to recognize a subjective privacy expectation as objectively reasonable. (R&R (Doc. 122) at 6), *see also United States v. Ruiz*, 664 F.3d 833, 838 (10th Cir. 2012). The Supreme Court has cautioned: "The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very

nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities." *Jacobsen*, 466 U.S. at 122. As explained by the Court in *Jacobsen*, there are multiple factors to consider when determining whether the government's intrusion infringes on a legitimate interest, and no single factor is determinative—but ultimately whether society recognizes a privacy interest as reasonable is determined based on our societal understanding regarding what deserves protection from government invasion. *United States v. Alabi*, 943 F. Supp.2d 1201, 1247 (NM 2013) (relying on *Katz v. United States*, 389 U.S. 347, 353 (1967)); *Ruiz*, 664 F.3d at 838; *Jacobsen*, 466 U.S. at 122; *California v. Ciraolo*, 467 U.S. 207, 212 (1986); *Oliver v. United States*, 466 U.S. 170, 181-83 (1984). "The Supreme Court has held that '[o]fficial conduct that does not 'compromise any legitimate interest in privacy is not a search subject to the Fourth Amendment.'" *Alabi*, 943 F. Supp.2d at 1247-48 (quoting *Illinois v. Caballes*, 543 U.S. 405, 409 (2005) (quoting *Jacobsen*, 466 U.S. at 123), *see also* (R&R (Doc. 122) at 6).

The Supreme Court has held that there is "'[n]o protected privacy interest [] in contraband in a container once government officers lawfully have opened that container and identified its contents as illegal.'" (R&R (Doc. 122) at 6) (quoting *Jocobsen*, 466 U.S. at 114-115)).

In his Objection, the Defendant argues that *Jacobsen* and other container cases should no longer be applied in the context of computer searches He asserts that privacy interests in a person's computer storage devices are especially strong because they store vast amounts of personal information, (D's Objection (Doc. 131) at 7) (citing *Riley v. California*, 134 S. Ct 2473, 2458 (2014)), of a type which "implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers,'" *id.* (quoting *United States v. Cotterman*, 709 F3d 952, 964 (9th Cir. 2013) (quoting U.S. Constitution Amendment IV)).

The Court agrees. Likewise, the Court agrees: "'[t]he contours of [the Fourth Amendment's] protections in the context of computer searches pose difficult questions.'"

(D's Objection (Doc. 131) at 7) (quoting *United States v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006)). "Computers are simultaneously file cabinets (with millions of files) and locked desk drawers; they can be repositories of innocent and deeply personal information but also of evidence of crimes. . . . As society grows ever more reliant on computers . . . courts will be called upon to analyze novel legal issues and develop new rules within our well established Fourth Amendment jurisprudence." *Id.* The Court does not, however, agree that: "Huntoon's case appears to be one with such novel legal issues that was not contemplated in the 1980's by the Supreme Court." *Id.* The HSI search of Huntoon's laptop, pursuant to the state search warrant, was limited to searching and finding contraband, specifically child pornography. When the state officers turned over the mirror image of the laptop to HSI, it had already been searched and found to contain such contraband and HSI searched for only these contraband materials.

There is strong precedential support for the Magistrate Judge's finding that there is no constitutionally protected privacy interest in contraband. The Court has gone so far as to create a class all its own, *sui generis,* for cases involving unique investigative procedures which are limited to searching only contraband, such as canine sniffs which seek and find only contraband or drug tests which establish a substance is or is not illicit. The point being that these types of searches are limited in both manner and content to disclose only the presence or absence of a contraband item and, therefore, do not constitute a "search" within the meaning of the Fourth Amendment. *Alabi*, 943 F.Supp.2d at 1248-1250 (citing *United States v. Place*, 462 U.S. 696, 707 (1983) (drug dogs); *Jacobsen*, 466 U.S. at 122-24 (drug testing for illicit chemical substances).

This Court does not suggest that this is a *sui generis* case, but the search here was limited in both manner and content to contraband. Only contraband, child pornography, was subject to the HSI search and the search was designed to only find contraband child pornography. The Court rejects the Defendant's argument that the search had to be limited to "searching" the exact contraband files found by the state officers, s*ee* (D's Objection (Doc. 131) at 8-9 (complaining that HSI found child pornography files not on

the State's evidence list)). It was only necessary for HSI to limit the search to finding evidence of child-pornography.[4]

This Court agrees with the Magistrate Judge's conclusion that the Government's examination of only the contraband child pornography files contained in the Defendant's laptop was not a search within the meaning of the Fourth Amendment.

The Court rejects the various arguments made in Defendant's Objection that the State either violated statutory warrant provisions[5] or the plain language of the search warrant protocols. The Defendant makes these arguments to challenge HSI's lawful right to search the laptop computer without obtaining a second search warrant. This Court finds instead that the Defendant had no protected privacy interest in the contraband child pornography files on his laptop computer.

There is ample case law to support the Government's position that a second warrant to search a properly seized computer is not necessary as long as the subsequent search does not exceed the probable cause articulated in the original warrant. *United States v. Gregoire*, 638 F.3d 962, 967–68 (8th Cir.2011) (allowing second search after one-year delay), *see also United States v. Grimmett*, 439 F.3d 1263, 1268–69 (10th Cir. 2006) (finding no second warrant necessary because federal agent's search was within confines of search authorized by state search warrant and was not an impermissible general search), *compare United States v. Carey*, 172 F.3d 1268, 1271, 1273-74 (10th Cir.

[4] Because the Court finds that the Government is not limited to re-searching the same contraband files found by the State, it also finds that it is reasonable that HSI may have inadvertently "searched" files which ultimately turned out to not be part of the contraband child pornography on the Defendant's laptop. Under the Fourth Amendment some perusal, generally fairly brief, of documents is allowed to enable police to perceive the relevance of the documents to the crime. *United States v. Mannino*, 635 F.2d 110, 115 (2d Cir.1980); *accord Andresen v. Maryland*, 427 U.S. 463, 482 n. 11 (1976) (explaining some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized for seizure). In the event the Government intends to offer any evidence that is not contraband, the Court will preclude it.

[5] To the extent the warrant affidavit and A.R.S. § 13-3920 precluded state law enforcement from turning over the mirror image of the laptop hard drive or the evidence they discovered in the state investigation, without a court order, this Court would have issued such an Order and thus the evidence which is the subject of the Motion to Suppress would have been inevitably discovered. The Court does not find this to be a constitutional argument; there is no evidence that A.R.S. 13-3920 disclosure provisions are based on the Fourth Amendment.

1999) (finding the original warrant authorized a search of a computer for evidence related to illegal drug sales, when officers found evidence of another crime—possession of child pornography—another warrant was needed). "[E]ven evidence not described in a search warrant may be seized if it is reasonably related to the offense which formed the basis for the search warrant." *United States v. Wright*, 343 F.3d 849, 863 (6th Cir. 2003).

In the Ninth Circuit, subsequent searches conducted years apart have been allowed pursuant to one warrant. *United States v. Johnston*, 789 F.3d 934, 941 (9th Cir. 2015).[6] In the Ninth Circuit, "once an item in an individual's possession has been lawfully seized and searched, subsequent searches of that item, so long as it remains in the legitimate uninterrupted possession of the police, may be conducted without a warrant." *United States v. Turner*, 28 F.3d 981, 983 (9th Cir. 1994) (quoting *United States v. Burnette*, 698 F.2d 1038, 1049 (1983) (finding no reasonable expectations in privacy once an item has been lawfully seized and searched). And, so the Court's analysis comes full circle. The Court finds that once the State lawfully searched the laptop and found contraband, the Defendant no longer had a protected privacy interest in the contraband contents of the laptop.

Finally, the Defendant makes one last argument. He asserts that the state search warrant was over-broad and lacked particularity in describing the places to be searched and the items to be seized. He argues that the warrant failed to provide sufficient guidance to officers conducting the search because it failed to specify "the crime to be investigated, the specific places to be searched, and the types of evidence to be seized.

[6] The Court rejects the Defendant's interpretation of Fed. R. Crim. P. 41(e)(2)(B), which provides that a warrant may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information, and unless specified otherwise, the warrant authorizes **a later review** of the media or information. The Defendant submits "a" means one and only one search. (Objection (Doc. 131) at 12.) The Court cannot agree. The Ninth Circuit has allowed staged or phased searches. *See e.g.*, *Johnston*, 789 F.3d at 942 (finding reasonable to phase searches with initial scan performed on site to determine if computer contained child pornography; another done later after defendant declined to accept a plea offer, and later still the third, most exhaustive, search was conducted in anticipation of trial). So while it is "constitutionally unreasonable" for the Government to "seize and indefinitely retain every file on [defendant's] computer for use in future criminal investigations," *Ganias*, 755 F.3d at 137. This is not that case. The mirror image of the Defendant's laptop was being retained by the State for use in an ongoing criminal investigation in Pinal County.

(D's Objection (Doc. 131) at 16-17.) The Court has reviewed the briefs submitted to the Magistrate Judge and the transcripts from the two hearings he held. The Defendant raises this issue for the first time in the Objection. This Court need not consider an issue which is raised for the first time in an Objection to the Report and Recommendation and may consider it waived for Defendant's failure to raise it before the Magistrate Judge. *See Greenhow v. Sec'y of Health & Human Servs.*, 863 F.2d 633, 638–39 (9th Cir.1988) (district court properly ruled that issues raised for the first time in objections to magistrate's report had been waived), overruled on other grounds, *United States v. Hardesty*, 977 F.2d 1347, 1348 (9th Cir.1992), *see also, Zamani v. Carnes*, 491 F.3d 990, 997 (9th Cir. 2007) ("The district court need not consider arguments raised for the first time in a reply brief.") The Court finds the issue waived.[7]

3. Motion to Suppress Illegal Search of Lenovo Tower[8]

Subsequent to the Government's Supplemental Notice of Intent to Introduce 414 Evidence, which was filed as noted above on March 13, 2018, the Defendant filed the Motion to Suppress the Lenovo computer evidence under the Fourth Amendment. The Magistrate Judge could not address the Motion to Suppress the Lenovo computer in his R&R because it was not fully briefed. The Government has now filed a Response. The

[7] The warrant specified the premises as including the manufactured home, the 5th wheel RV, another RV, and unattached sheds, from where there was being possessed or concealed certain property or things, which were described with particularity as computer related things, images or movies, generally or as specified in the warrant, containing or displaying minors engaging in any sexual activity or sexual exploitation, evidence related to ownership, control, or use of the residences, computer systems, etc., *see* (Reply to D's Objection (Doc. 134) at 13) (summarizing warrant), all of which property or things were being used as a means for committing the public offense of Sexual Exploitation of a Minor, a class 2 felony. It is absolutely inaccurate to describe the warrant as failing to place limitations on the specific evidence sought or to describe it as allowing officers to search all of Huntoon's computer records without any limitations on what files could be seized or how those files related to specific criminal activity. The Court agrees with the Magistrate Judge's description of the parameters of the state search warrant as being robust but limited to those things used as a means for committing sexual exploitation of a minor, i.e., possessing and/or distributing child pornography. (R&R (Doc. 122) at 7-8.)

[8] The Government also filed a Superseding Indictment on March 21, 2018, adding new charges based on child pornography found on the Lenovo computer: Count Three. The Court severed Count Three for trial because, without a waiver, under 18 U.S.C. § 3161(c)(2), a trial on Count Three "shall not commence less than thirty days from the date on which the defendant first appears." Given the firm April 17, 2018, trial date set in this case, severing Count Three allows the case to proceed to trial on Counts One and Two.

Government intends to introduce under Fed. R. Evid. 414 and 404(b) "evidence of child pornography located on the Lenovo desktop computer seized during the execution of the search warrant by HSI." (Notice (Doc. 98) at 1.) The Government asserts "a subsequent examination of the Lenovo desktop computer seized by [Homeland Security Investigation] HSI from the Polly Drive address in Hereford contained approximately 110 files depicting child pornography in the downloads folder of the computer." *Id.* at 3.

Defendant challenges the "subsequent" examination of the Lenovo desktop computer under the Fourth Amendment. Defendant explains that the HSI search warrant was executed on November 16, 2015, at the Hereford address and agents seized 28 items from a detached garage for later analysis, including a Lenovo computer tower and USB flash drives. A forensic examination was conducted around December 3, 2015. SA Nuckles authored a forensic report as follows: "Of all of the items submitted for analysis, only one item was found to contain child pornography. That item was a 4GB Sony brand USB flash drive (thumb drive)." (Motion to Suppress (Doc. 104): Forensic Report (Doc. 104-3) at 1.) This forensic report was disclosed to the Defendant.

Subsequently,[9] on February 14, 2018, the Government had Magnet Forensics conduct another search of the Lenovo computer. They found the child pornography files and generated a forensic report on February 22, 2018, which was thereafter disclosed to the Defendant.

The Court notes that the merits of the Defendant's Fourth Amendment challenge related to the February 2018 search of the Lenovo computer differs from the analysis

[9] In its Response, the Government paints the December 3, 2015, search as not a complete forensic examination because the Defendant was in state custody, (Response (Doc. 130), and explains that "once the defendant rejected the government's plea offer and indicated that he would be proceeding to trial, Agent Nuckles completed a "more thorough forensic examination," which is the subject to the Motion to Suppress, *id.* at 3. The Court is confused because the Defendant's Motion to Suppress includes a copy of a forensic report for the "subsequent" search which reflects it was conducted by Magnet Forensics, requested by the Government on February 14, 2018, and reported on the 24th. The record reflects the last extension of the Plea Deadline occurred on November 3, 2017, when it was extended to January 5, 2018, and a pretrial conference was set before Magistrate Judge Ferraro. At the time the Government requested the "subsequent" more thorough forensic examination there was a "firm" trial date set for March 19, 2018. *See also* (Reply (Doc. 133) (reporting there was no formal plea offer in this case and any informal plea offer would have been sometime before May, 2017).

applied to the Government's search of the laptop. First, and foremost, the February search was conducted after an initial search of the Lenovo computer found no child pornography on it. Accordingly, the contraband analysis above does not apply here. There is a question of whether probable cause even existed for the search subsequent to the laptop being found to not contain any contraband. Additionally, the Court notes the rational for allowing later review of electronically stored information does not apply to the delay that occurred here. Rule 41(e)(2) allows for later review because it can take "a substantial amount of time" for "forensic imaging and review of information . . . due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs." Advisory Committee Notes, 2009 Amendments. There is no support in the existing record that the two-year delay in conducting the February 2018 search of the Lenovo computer was reasonable under the Rule 41 rational for later review.

Likewise, the Government's arguments in opposition differ here as well. The Government asserts that the Defendant cannot establish a legitimate privacy interest in the Lenovo computer because he has "both repeatedly denied ownership and abandoned the property at his father's house." (Response (Doc. 130) at 5.) The Government argues it was reasonable to retain the Lenovo computer to phase in the searches as the investigation progressed. And, even if the February 2018 search was not reasonable, the Government submits "there is no evidence in the record to suggest that agents were acting in any manner other than an objectively reasonable one," (Response (Doc. 130) at 13), by relying on the lawfully issued and executed November 2015 warrant. Therefore, the good faith exception applies. The Court notes the burden is on the Government to prove this warrant exception applies. *Coolidge*, 403 U.S. at 455.

Here, there are no facts in evidence for this Court to make a reasonableness determination, especially since the "subsequent" search wasn't phased in until the eve of trial—a fact undermining the credibility of this rationale. There is no evidence in the record upon which this Court may rely to make a finding of good faith.

On the limited record that exists at this time, the Court is unable to decide the merits of the Defendant's Fourth Amendment claim. This inability is caused by the Government's delay in conducting the "subsequent" search until the eve of trial.[10] The Court notes that the search was initiated by the Government on February 14 and completed February 22, when the trial was set for March 19, per the parties' request for a firm trial date. The Court does not know when the Magnet Forensics' forensic report was disclosed to the Defendant, but the Notice of Intent to use this evidence under Rules 414 and 404(b) was filed March 18, six days after the Court continued the trial date to April 17, 2018, a continuance necessitated by the Government's delay in securing the laptop evidence. As noted in the previous section of this Order, the Government knew the laptop existed from the inception of the case, and offers no explanation for why it delayed securing it until after the discovery and pretrial motions deadlines had expired in the case. While the Court remedied this late disclosure in respect to the laptop by continuing the trial date, it will not further delay the trial. *See* (Order (Doc. 127) (severing Count III (Lenovo computer) for trial)).

The Court precludes the evidence[11] found on the Lenovo computer because it was disclosed by the Government after the disclosure deadline, November 17, 2017, after the pretrial motions deadline, January 3, 2018, and with at most only about 30[12] days left before trial. This late disclosure prejudiced the Defendant's ability to prepare for trial because it is only now that he sees the full extent of evidence the Government seeks to bring against him. Neither his attorney nor his computer expert has had time to examine

[10] *See* n. 2.

[11] At the pretrial conference, the Government asked the Court to except evidence other than child pornography images found on the Lenovo computer from the suppression order. The Court suggested it might allow the Government to present evidence linking the Defendant's laptop computer to the Lenovo computer and vice versa. The Defendant objected without argument. The Court will hear from Defendant regarding his argument supporting his objection before deciding whether to admit non-image evidence found on the Lenovo computer.

[12] The Court is aware that Rule 414(b) provides for the Government to disclose its intent to use 414 evidence "at least 15 days before trial' but that assumes there has been timely disclosure and opportunity to challenge by pretrial motion the evidence which is the subject of the notice of intent. Here, no such timely disclosure was made. To the contrary, the Government disclosed there was no incriminating evidence on the Lenovo computer.

the Lenovo computer evidence to prepare a defense. *Cf.* (Motion to Preclude (Doc. 83) (complaining about late disclosures related to laptop computer, requiring continuance of March 19 trial date to April 17, 2018)). Finally, this Court does not have time to conduct a hearing and develop the evidentiary record which would enable it to rule on the merits of the pretrial motion challenging the search under the Fourth Amendment. This Court agrees with the court in *Ganias* that a fully developed record regarding the technological specifics of the search is important in answering Fourth Amendment questions, i*d.* at 217, especially here where the first search failed to find the child pornography found in the second search. The Court grants the Motion to Suppress for purposes of the trial on Counts One and Two set on April 17, 2018, and refers the Motion to Suppress the Lenovo Computer to Magistrate Judge Ferraro for an evidentiary hearing and R&R in time for the trial on Count III.

Conclusion

After *de novo* review of the issues raised by the Defendant in his objections, this Court agrees with the findings of fact and conclusions of law made by the Magistrate Judge in the R&R for determining the pending Motion to Suppress the laptop computer evidence. The Court adopts it. The Court denies Defendant's Motion to Suppress Evidence from the laptop computer. The Court grants the Motion to Suppress the Lenovo computer for purposes of the April 17, 2018, trial and refers the motion to Magistrate Judge Ferraro for an evidentiary hearing and R&R to be held in time for a trial on Count III.

Accordingly,

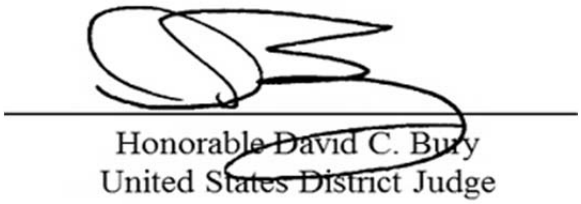
IT IS ORDERED that after a full and independent review of the record, in respect to the Defendant's objections, the Magistrate Judge's Report and Recommendation (Doc. 122) is accepted and adopted as the findings of fact and conclusions of law of this Court.

IT IS FURTHER ORDERED that Defendant's Motion to Suppress Illegal Search of Laptop Computer (Doc. 66) is DENIED.

IT IS FURTHER ORDERED that the Defendant's Motion to Suppress Illegal Search of Lenovo Computer (Doc. 104) is GRANTED.

IT IS FURTHER ORDERED that this matter remains referred to Magistrate Judge Ferraro for an evidentiary hearing and R&R on Defendant's Motion to Suppress Illegal Search of Lenovo Computer.

Dated this 11th day of April, 2018.



Honorable David C. Bury
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

United States of America

v.

Michael Huntoon

JUDGMENT IN A CRIMINAL CASE
(For Offenses Committed On or After November 1, 1987)

No. CR-16-00046-001-TUC-DCB (DTF)

Stephanie Kathryn Bond (CJA)
Attorney for Defendant

USM#: 73418-408

THERE WAS A VERDICT OF guilty on 4/19/2018 as to Counts 1 and 2 of the Superseding Indictment.

ACCORDINGLY, THE COURT HAS ADJUDICATED THAT THE DEFENDANT IS GUILTY OF THE FOLLOWING OFFENSE(S): violating Title 18, U.S.C. §2252(a)(2) and (b)(1), Distribution of Child Pornography, a Class B Felony offense, as charged in Count 1 of the Superseding Indictment; Title 18, U.S.C. §2252A(a)(5)(B) and (b)(2), Knowing Access of Child Pornography, a Class C Felony offense, as charged in Count 2 of the Superseding Indictment.

IT IS THE JUDGMENT OF THIS COURT THAT the defendant is committed to the custody of the Bureau of Prisons for a term of **TWO HUNDRED FORTY (240) MONTHS**, on Count 1 and **TWO** and on Count 2, said counts to run concurrently, with credit for time served. Upon release from imprisonment, the defendant shall be placed on supervised release for a term of **LIFE**, on Count 1 and on Count 2, said counts to run concurrently. Sentence imposed to run concurrent to the sentence to be imposed in Pinal County Superior Court, docket number CR201503282.

CRIMINAL MONETARY PENALTIES

The defendant shall pay to the Clerk the following total criminal monetary penalties:

SPECIAL ASSESSMENT: $200.00 **FINE:** WAIVED **RESTITUTION:** N/A

The defendant shall pay a special assessment of $200.00 which shall be due immediately.

The Court finds the defendant does not have the ability to pay a fine and orders the fine waived.

If incarcerated, payment of criminal monetary penalties are due during imprisonment at a rate of not less than $25 per quarter and payment shall be made through the Bureau of Prisons' Inmate Financial Responsibility Program. Criminal monetary payments shall be made to the Clerk of U.S. District Court, Attention: Finance, Suite 130, 401 West Washington Street, SPC 1, Phoenix, Arizona 85003-2118. Payments should be credited to the various monetary penalties imposed by the Court in the priority established under 18 U.S.C. § 3612(c). The total special assessment of $200.00 shall be paid pursuant to Title 18, United States Code, Section 3013 for Count 1 and 2 of the Superseding Indictment.

Any unpaid balance shall become a condition of supervision and shall be paid within 90 days prior to the expiration of supervision. Until all restitutions, fines, special assessments and costs are fully paid, the defendant shall immediately notify the Clerk, U.S. District Court, of any change in name and address. The Court hereby waives the imposition of interest and penalties on any unpaid balances.

SUPERVISED RELEASE

It is ordered that while on supervised release, the defendant must comply with the mandatory and standard conditions of supervision as adopted by this court, in General Order 17-18, which incorporates the requirements of USSG §§ 5B1.3 and 5D1.2. Of particular importance, the defendant must not commit another federal, state, or local crime during the term of supervision. Within 72 hours of sentencing or release from the custody of the Bureau of Prisons the defendant must report in person to the Probation Office in the district to which the defendant is released. The defendant must comply with the following conditions:

MANDATORY CONDITIONS

1) You must not commit another federal, state or local crime.
2) You must not unlawfully possess a controlled substance. The use or possession of marijuana, even with a physician's certification, is not permitted.
3) You must refrain from any unlawful use of a controlled substance. The use or possession of marijuana, even with a physician's certification, is not permitted. Unless suspended by the Court, you must submit to one drug test within 15 days of release of imprisonment and at least two periodic drug tests thereafter, as determined by the court.

STANDARD CONDITIONS

1) You must report to the probation office in the federal judicial district where you are authorized to reside within 72 hours of sentencing or your release from imprisonment, unless the probation officer instructs you to report to a different probation office or within a different time frame.
2) After initially reporting to the probation office, you will receive instructions from the court or the probation officer about how and when you must report to the probation officer, and you must report to the probation officer as instructed.
3) You must not knowingly leave the federal judicial district where you are authorized to reside without first getting permission from the court or the probation officer.
4) You must answer truthfully the questions asked by your probation officer.
5) You must live at a place approved by the probation officer. If you plan to change where you live or anything about your living arrangements (such as the people you live with), you must notify the probation officer at least 10 days before the change. If notifying the probation officer in advance is not possible due to unanticipated circumstances, you must notify the probation

officer within 72 hours of becoming aware of a change or expected change.

6) You must allow the probation officer to visit you at any time at your home or elsewhere, and you must permit the probation officer to take any items prohibited by the conditions of your supervision that he or she observes in plain view.

7) You must work full time (at least 30 hours per week) at a lawful type of employment, unless the probation officer excuses you from doing so. If you do not have full-time employment you must try to find full-time employment, unless the probation officer excuses you from doing so. If you plan to change where you work or anything about your work (such as your position or your job responsibilities), you must notify the probation officer at least 10 days before the change. If notifying the probation officer at least 10 days in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.

8) You must not communicate or interact with someone you know is engaged in criminal activity. If you know someone has been convicted of a felony, you must not knowingly communicate or interact with that person without first getting the permission of the probation officer.

9) If you are arrested or questioned by a law enforcement officer, you must notify the probation officer within 72 hours.

10) You must not own, possess, or have access to a firearm, ammunition, destructive device, or dangerous weapon (i.e., anything that was designed, or was modified for, the specific purpose of causing bodily injury or death to another person such as nunchakus or tasers).

11) You must not act or make any agreement with a law enforcement agency to act as a confidential human source or informant without first getting the permission of the court.

12) If the probation officer determines that you pose a risk to another person (including an organization), the probation officer may require you to notify the person about the risk and you must comply with that instruction. The probation officer may contact the person and confirm that you have notified the person about the risk.

13) You must follow the instructions of the probation officer related to the conditions of supervision.

SPECIAL CONDITIONS

The following special conditions are in addition to the conditions of supervised release or supersede any related standard condition:

1) You must participate as instructed by the probation officer in a program of substance abuse treatment (outpatient and/or inpatient) which may include testing for substance abuse. You must contribute to the cost of treatment in an amount to be determined by the probation officer.

2) You must submit your person, and any property, house, residence, vehicle, papers, computer, other electronic communications or data storage devices or media, and effects to search at any

time, with or without a warrant, by any law enforcement or probation officer with reasonable suspicion concerning a violation of a condition of supervised release or unlawful conduct, and by any probation officer in the lawful discharge of the officer's supervision functions. You must consent to and cooperate with the seizure and removal of any hardware and/or data storage media for further analysis by law enforcement or the probation officer with reasonable suspicion concerning a violation of a condition of supervision or unlawful conduct. Failure to submit to a search may be grounds for revocation of release. You must warn any other occupants that the premises may be subject to searches pursuant to this condition.

3) You must not use or possess alcohol or alcoholic beverages.

4) You must cooperate in the collection of DNA as directed by the probation officer.

5) You must attend and participate in a sex offender treatment program and sex offense specific evaluations as approved by the probation officer. You must abide by the policies and procedures of all the treatment and evaluation providers. You must contribute to the cost of such treatment and assessment not to exceed an amount determined to be reasonable by the probation officer based on ability to pay.

6) You must attend and participate in periodic polygraph examinations as a means to determine compliance with conditions of supervision and the requirements of your therapeutic program, as directed by the probation officer. No violation proceeding will arise solely on the result of the polygraph test. A valid Fifth Amendment refusal to answer a question during a polygraph examination will not be used as a basis for a violation proceeding. You must contribute to the cost of such polygraph not to exceed an amount determined to be reasonable by the probation officer based on ability to pay.

7) You must reside in a residence approved, in advance, by the probation officer. Any changes in the residence must be pre-approved by the probation officer.

8) You must not knowingly possess, view, or otherwise use material depicting sexually explicit conduct as defined in 18 U.S.C. § 2256 (2). You will submit any records requested by the probation officer to verify your compliance with this condition. You must not enter any location where the primary function is to provide these prohibited materials.

9) You must register as a sex offender in compliance with all federal, state, tribal or other local laws or as ordered by the Court. Failure to comply with registration laws may result in new criminal charges.

10) You must not be in the company of or have contact with children who you know are under the age of 18, with the exception of your own children. Contact includes, but is not limited to, letters, communication devices, audio or visual devices, visits, or communication through a third party.

11) You are restricted from engaging in any occupation, business, volunteer activity or profession where you have the potential to be alone with children under the age of 18 without prior written

permission. Acceptable employment shall include a stable, verifiable work location and the probation officer must be granted access to your work site.

12) You must not possess any device capable of capturing and/or storing an image, or video recording device without the prior written permission of the probation officer.

13) You must consent, at the direction of the probation officer, to having installed on your computer(s) (as defined at 18 U.S.C. § 1030(e)(1), including internet capable devices), at your own expense, any hardware or software systems to monitor your computer use.

14) You must not go to, or remain at, any place where you know children under the age of 18 are likely to be, including parks, schools, playgrounds, and childcare facilities. You must not go to, or remain at, a place for the primary purpose of observing or contacting children under the age of 18.

THE DEFENDANT IS ADVISED OF DEFENDANT'S RIGHT TO APPEAL BY FILING A NOTICE OF APPEAL IN WRITING WITHIN 14 DAYS OF ENTRY OF JUDGMENT.

The Court may change the conditions of probation or supervised release or extend the term of supervision, if less than the authorized maximum, at any time during the period of probation or supervised release. The Court may issue a warrant and revoke the original or any subsequent sentence for a violation occurring during the period of probation or supervised release.

The Court orders commitment to the custody of the Bureau of Prisons.

Date of Imposition of Sentence: **Tuesday, July 24, 2018**

Dated this 24th day of July, 2018.

Honorable David C. Bury
United States District Judge

RETURN

I have executed this Judgment as follows: _____

defendant delivered on _____ to _____ at _____, the institution designated by the Bureau of Prisons with a certified copy of this judgment in a Criminal case.

_____ By: _____
United States Marshal Deputy Marshal