Appendices

NOT FOR PUBLICATION

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. BENJAMIN D. MORROW, Defendant-Appellant.	No. 21-10242 D.C. Nos. 3:19-cr-00041-MMD-WGC-1 3:19-cr-00041-MMD-WGC MEMORANDUM*

Appeal from the United States District Court
for the District of Nevada
Miranda M. Du, Chief District Judge, Presiding

Argued and Submitted April 19, 2023
San Francisco, California

Before: SCHROEDER, CALLAHAN, and BUMATAY, Circuit Judges.

Benjamin D. Morrow appeals the district court's denial of his suppression motion and the restitution order following his conditional guilty plea to two counts of distribution of child pornography in violation of 18 U.S.C. §§ 2252A(a)(2) and (b)(1).

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

Morrow first challenges the validity of the search warrant on the ground that it was not supported by an oath or affirmation. It was executed under penalty of perjury, however, and was therefore supported by the requisite commitment to truth. *See United States v. Bueno-Vargas*, 383 F.3d 1104, 1109–12 (9th Cir. 2004).

Morrow next argues the warrant was not supported by probable cause. He contends that there was an insufficient basis to link Morrow to the incriminating communications. The district court found that the warrant affidavit sufficiently established that the three accounts used to communicate with law enforcement about child exploitation were operated by the same person, thus establishing a substantial basis for the probable cause determination.

Morrow further contends there was insufficient justification for a nighttime search. *See* Fed. R. Crim. P. 41. The evidence was inconsistent to the extent the affidavit said that Morrow "may be currently sexually assaulting the juvenile" and later included a message from Morrow that his niece was coming "this week sometime not sure what day yet." However, the district court held a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154, 171–72 (1978), and concluded there was no omission of material information. Even if we were to disagree with the district court on that question, there is no basis to disturb the district court's findings of good faith on the part of the government, *United States v. Mendonsa*,

989 F.2d 366, 369–70 (9th Cir. 1993), or Morrow's lack of prejudice. *See United States v. Stefanson*, 648 F.2d 1231, 1235–36 (9th Cir. 1981).

Finally, Morrow argues that the district court improperly ordered him to pay restitution to victims of conduct that he admitted in his plea agreement, but whose victimization was embodied in criminal charges the government dismissed. Morrow's plea agreement, however, explicitly stipulated that Morrow would pay $3,000 per victim identified through the Child Victim Identification Program or Child Recognition Identification System, and who requested restitution prior to sentencing.

AFFIRMED.

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. BENJAMIN D. MORROW, Defendant-Appellant.	No. 21-10242 D.C. Nos. 3:19-cr-00041-MMD-WGC-1 3:19-cr-00041-MMD-WGC District of Nevada, Reno ORDER

Before: SCHROEDER, CALLAHAN, and BUMATAY, Circuit Judges.

The Appellant's Pro Se Motion for Application for Indigency Status on Appeal, Docket. No. 53, is **DENIED AS MOOT.**

The panel has voted to deny Appellant's Petition for Panel Rehearing.

Appellant's Petition for Panel Rehearing, Docket. No. 54, is **DENIED.**

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

* * *

UNITED STATES OF AMERICA,

Plaintiff,

v.

BENJAMIN D. MORROW,

Defendant.

Case No. 3:19-cr-00041-MMD-WGC

ORDER

I. SUMMARY

Defendant Benjamin D. Morrow was indicted on two counts of distribution of child pornography, and four counts of possession of child pornography. (ECF No. 1.) Before the Court is Morrow's motion to suppress. (ECF No. 46 (the "Motion").)[1] In a prior hearing, the Court granted Defendant's request for a *Franks*[2] hearing contained within his Motion (ECF No. 80), and the Court held the *Franks* hearing on March 3, 2021 (ECF No. 90 (the "Hearing")).[3] Because Morrow fails to demonstrate by a preponderance of the evidence that the affiant intentionally omitted information or included misleading information in the search warrant ("Warrant"), and as further explained below, the Court denies the Motion and will not suppress any evidence.

///

[1]The government filed a response. (ECF No. 52.) Morrow filed a reply (ECF No. 64.)

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

[3]Following the initial hearing, the government filed a motion for leave to file a supplemental response to Morrow's Motion (ECF No. 83) with amended exhibits (ECF No. 84). Morrow subsequently filed a motion for leave to file reply with reply attached. (ECF No. 86.) The Court granted both motions at the Hearing. (ECF No. 90.)

II. FINDINGS OF FACT[4]

The Court relies on documents filed by the parties in support of the Motion and related briefs, along with testimony offered and exhibits admitted at the Hearing, to construct this factual background.

Complaining witness Roxanne Treesh ("Treesh") reported to law enforcement officials in Ohio that she had been contacted by an individual via text message from email account 'jayd@secmail.pro' who sent unsolicited photographs of child pornography and requested photographs of the sexual abuse of her minor daughter. (ECF No. 46 at 1.)

Federal agents in Ohio began an investigation. (*Id.*) On April 9, 2019, federal investigators interviewed Treesh who consented to a search of her phone. (ECF No. 52 at 3.) Investigators reviewed text messages from the individual ("UNSUB")[5] to Treesh, and discovered three images of a young female child being anally penetrated by a male. (*Id.*) Investigators then assumed the identity of Treesh, ("OCE-7478"),[6] and began texting with UNSUB. (*Id.*) On April 9, 2019, OCE-7478 asked UNSUB to chat on the messaging application Kik, and UNSUB provided his username, 'adventurej0hn.' (*Id.*) OCE-7478 briefly spoke with UNSUB on Kik on April 9, 2019 and April 10, 2019. (ECF NO. 52-4 at 14-15.)

UNSUB then asked to speak with OCE-7478 over the messaging application Telegram. (*Id.*) OCE-7478 provided a Telegram account. (ECF No. 53-2 at 15.) The affidavit ("Affidavit") fails to state how UNSUB and OCE-7478 connected on Telegram.[7]

---

[4]*See* Fed. R. Crim. P. 12(d) ("When factual issues are involved in deciding a motion, the court must state its essential findings on the record.").

[5]Both the Affidavit and government refer to the individual sending messages from 'jayd@secmail.pro,' who initially referred to himself as "John," as "UNSUB." (ECF No. 47-1 at 2.) The Court will refer to the individual as such.

[6]The government refers to the officers who assumed the identity of Treesh as OCE-7478. The Court will similarly refer to the agents as such.

On April 11, 2019, OCE-7478 and UNSUB began messaging on Telegram. On April 12, 2019, UNSUB sent eight images of child pornography to OCE-7478 over Telegram. (ECF No. 52 at 4.)

On approximately April 16, 2019, investigators subpoenaed Kik for subscriber and Internet Protocol ("IP") address information for account 'adventurej0hn.' (ECF Nos. 52 at 4, 46-6 at 3-4.) Kik provided subscriber information for 'adventurej0hn'—John C. and email address jayd@secmail.pro. (*Id.*) Kik provided two IP addresses: 172.221.35.154 and 149.56.182.0. (ECF No. 46-6 at 4.) Investigators conducted an Arin.net search for the first IP address which was connected to Charter Communications, with the second IP address connecting to CactusVPN. (ECF No. 52 at 4-5.) On April 16, 2019, investigators served an emergency disclosure request on Charter for three dates: 04/10/2019 at 03:16:36 UTC, 04/10/2019 at 03:50:12 UTC, and 04/10/2019 at 03:16:36 UTC. (ECF No. 46-4 at 2.) Charter provided investigators with the subscriber information for Benjamin Morrow at 313 Appaloosa Way, Fernley, NV 89408 over the telephone. (ECF No. 52 at 5.)

On April 20, 2019, UNSUB messaged OCE-7478 on Telegram: "I am going to see my fuck toy for spring break." These messages prompted Ohio Federal Bureau of Investigation ("FBI") agents to contact FBI Special Agent Cassie Redig ("Agent Redig") in Reno, Nevada. (*Id.*) On April 20, 2019, Agent Redig contacted Lyon County Sheriff Sergeant Ryan Powell ("affiant" or "Sergeant Powell"). (*Id.*) Investigators searched LSCO records which indicated that Morrow lived at 1361 Horse Creek Way and 313 Appaloosa Way. (*Id.*) Federal agents and local county deputies conducted surveillance outside the residence in Fernley, Nevada where Morrow was ultimately located. (*Id.*) Agents only noted an adult male in the home.

///

---

[7]The government acknowledges that the Affidavit fails to explain how UNSUB and OCE-7478 connected on Telegram. (ECF No. 52 at 4, n.2.)

On April 20, 2019, Sergeant Powell drafted the Warrant and Affidavit. (ECF No. 46 at 3.) Sergeant Powell emailed the Affidavit to Honorable Justice of the Peace Doug Kassebaum ("Judge Kassebaum") of the Walker River Justice Court in Lyon County, Nevada. (*Id.* at 2.) Sergeant Powell then called Judge Kassebaum at 9:32 pm on April 20, 2019 and recorded the call over dispatch. (ECF No. 46-3.) Judge Kassebaum began the conversation by saying "you're good to go." (*Id.*) Judge Kassebaum then swore in Sergeant Powell. (*Id.*) Judge Kassebaum confirmed receipt of the email application and Warrant and granted the request for a nighttime search. (*Id.* at 3-4.) Sergeant Powell inquired if he could sign the Warrant on behalf of Judge Kassebaum who then gave oral permission for Sergeant Powell to do so. (*Id.*) Sergeant Powell signed the Affidavit and Warrant on behalf of Judge Kassebaum at 9:35 pm. (ECF Nos. 47-1 at 15, 46-1 at 1.)

The Warrant authorized law enforcement to search the premises at 313 Appaloosa Way, Fernley, Nevada, 89408 and Benjamin Morrow. (ECF No. 46-1 at 2.) The Warrant also authorized a search of specific computer and technological property. Officers executed the Warrant at 10:35 pm. No child was found at the residence. (ECF No. 52 at 5.) Multiple devices were seized containing tens of thousands of images and videos of child pornography. (*Id.*)

III. DISCUSSION

Morrow argues that suppression is warranted for several reasons. At the initial hearing, the Court heard oral argument on each issue, and allowed three to proceed to the Hearing. The Court addresses the three remaining arguments below—first the two *Franks* arguments, next Morrow's argument regarding improper issuance of the Warrant, and finally, Morrow's argument regarding an improper nighttime search.

As explained below, the Court finds that none of these arguments are sufficiently meritorious to warrant suppression or exclusion of any evidence. Thus, the Court denies Morrow's Motion.

///

A. *Franks*

Morrow argues that Sergeant Powell made material misrepresentations and omissions in the Affidavit justifying suppression under *Franks.*

In *Franks*, the United States Supreme Court established a two-prong test for overturning a judicial officer's probable cause finding. Under this test, there is a "presumption of validity with respect to the affidavit supporting the search warrant." *Franks*, 438 U.S at 171. And here, as noted, the Court determined Morrow made a sufficient preliminary showing such that a *Franks* hearing was warranted as to two arguments presented (ECF No. 80; ECF No. 82 at 44-47) and held the Hearing. That brings the Court to the merits of Morrow's *Franks* challenge.

To prevail on a *Franks* challenge, the defendant must establish, by a preponderance of the evidence, that: "(1) that the affiant officer intentionally or recklessly made false or misleading statements or omissions in support of the warrant," and (2) "that the false or misleading statement or omission was material, *i.e.*, necessary to finding probable cause." *United States v. Perkins*, 850 F.3d 1109, 1116 (9th Cir. 2017) (internal quotation marks, punctuation, and citation omitted). "If both requirements are met, the search warrant must be voided and the fruits of the search excluded[.]" *Id.* (internal quotation marks and citation omitted). Under the first *Franks* step, a "negligent or innocent mistake does not warrant suppression." *Id.* Under the second step of *Franks*, the "key inquiry is 'whether probable cause remains once the evidence presented to the magistrate Judge is supplemented with the challenged omissions.'" *Id.* at 1119 (citation omitted). "Probable cause to search a location exists if, based on the totality of the circumstances, there is a 'fair probability' that evidence of a crime may be found there." *Id.* In this case, the Court ordered an evidentiary hearing in regards to two potential omissions and misstatements in the Affidavit. (ECF No. 82 at 44-47.)

///

///

i. Linkage of Accounts

Morrow first argues that the affiant included misleading conclusory statements in the Affidavit when referring to UNSUB as the person who sent all emails, texts, and communications; thus, there was insufficient information for Judge Kassebaum to draw a connection between the email, Kik, and Telegram accounts purportedly used by UNSUB. (ECF No. 46 at 23.) The government responds that there was sufficient linkage to establish probable cause. (ECF No. 52 at 26-27.)

To determine if Morrow can prevail, the Court begins with *Franks* step one. At step one, Morrow must demonstrate by a preponderance of the evidence "that the affiant officer intentionally or recklessly made false or misleading statements or omissions in support of the warrant." *Perkins*, 850 F.3d 1109 at 1116. Morrow has not established by a preponderance of the evidence that Sergeant Powell made misleading statements regarding a connection between the three accounts in in support of the Affidavit. Rather, the conclusion was supported by sufficient evidence.

First, the Affidavit notes that UNSUB used his jayd@secmail.pro account to message OCE-7478 his Kik username ('adventurej0hn'). (ECF Nos. 52 at 26; 47-1 at 3.) This tends to establish that the same person operated and used both accounts. Second, the content of the messages themselves, included in part in the Affidavit, "confirm that UNSUB was the user of all three." (ECF No. 52 at 26.) For example, in messages from all three accounts, UNSUB references "playing with" his niece or his "fuck toy." In conversations between UNSUB at the jayd@secmail.pro account and OCE-7478, UNSUB sends photographs of a juvenile and "state[s] that the girl in the pics is 7 years old and that he plays with his niece sometimes." (ECF No. 47-1 at 3.) Over Telegram messages, UNSUB references his "lil fuck toy" and over the recorded Telegram call with Treesh, UNSUB again references his niece. (*Id.* at 4.) Third, UNSUB refers to himself as "John" across all three accounts. On the jayd@secmail.pro account, one text reads, "Its John..." (ECF No. 47-1 at 2), UNSUB's Kik account name is 'adventurej0hn' (*Id.* at 3),

and UNSUB's Telegram account name is '@j0hncc' (*Id*). These similarities and connections across all three accounts are included in the Affidavit to indicate that the three accounts were controlled by the same person. Thus, there is no evidence that Sergeant Powell used conclusory statements to purposefully mislead Judge Kassebaum to conclude there was a link between the three accounts. Rather, the Affidavit included specific evidence of such a link.

Because Morrow has failed to establish by a preponderance of the evidence that Sergeant Powell made a misleading statement in support of the Affidavit, the Court will not move on to *Franks* step two. The Court will therefore decline to suppress any evidence as a result of Morrow's first *Franks* challenge.

ii. "With Child" Omissions

Next, Morrow argues that Sergeant Powell's statement in the Affidavit that UNSUB was "with child" was deliberately or recklessly false and he omitted material evidence regarding the presence of a child in the home in support of the Warrant. (ECF No. 46 at 10, 25.) Morrow specifically points to contradictory statements found in the Affidavit,[8] the deliberate omission of messages from Morrow,[9] and the deliberate omission of the results of an earlier investigation,[10] to argue that Sergeant Powell deliberately intended to

---

[8]The Affidavit claims that Morrow "may be currently sexually assaulting the juvenile" (ECF No. 47-1 at 1), and later includes a message from Morrow that his niece and her mom were coming "this week sometime not sure what day yet" (*Id*). Morrow argues that because these statements are impossible to reconcile "Sergeant Powell intended to influence the magistrate into believing that exigency required exercising the subject warrant at night, that night . . ." (ECF No. 46 at 10.)

[9]Morrow also proffers as evidence a message, sent after the "this week sometime not sure which day" message, which stated that the niece and her mom were coming "I think on Wednesday, not 100% tho." (ECF No. 52-4 at 27.)

[10]At the Hearing, Morrow examined Sergeant Powell about the circumstances of the home surveillance in an attempt to establish that Sergeant Powell purposefully omitted evidence that no child was seen in the home.

influence Judge Kassebaum to believe there were exigent circumstances justifying a Warrant. (*Id.* at 10-11, 64 at 6-8.) The government responds that Morrow failed to make a substantial showing of falsity because Sergeant Powell provided enough evidence for probable cause and was not required to have a certainty as to what "this week" meant. (ECF No. 52 at 15.)[11]

The Court begins with *Franks* step one. Again, Morrow has not established by a preponderance of the evidence that Sergeant Powell intentionally made false or misleading statements or intentionally omitted information in support of the Warrant.

As to the contradictory statements regarding whether a child was currently in danger, Morrow failed to demonstrate that these statements were included to intentionally mislead Judge Kassebaum. Rather, testimony at the Hearing indicated that Sergeant Powell included all the relevant information provided to him, which at times was inconsistent. If anything, the intentional inclusion of inconsistent information is evidence that Sergeant Powell was seeking to provide a more complete picture of the facts as he knew them. Thus, the Court does not find that the inclusion of inconsistent messages was used to intentionally mislead Judge Kassebaum.

As to the text message, "I think on Wednesday, not 100% tho" (ECF No. 52-4 at 27), Morrow has failed to proffer any evidence that Sergeant Powell intentionally omitted the message from the Affidavit. At the Hearing, Sergeant Powell testified that he was not aware of this particular text message. Agent Redig further testified that she did not recall receiving the text message, and even though there is evidence that she did, she did not

---

[11]In its supplemental response, the government provides additional evidence to clarify a statement made at the initial hearing—that Sergeant Powell did not know about the text message that Morrow believed his niece was arriving Wednesday. The government produces a text message from Agent Hunt to Agent Redig that reads "says he thinks niece will be there Wednesday" (ECF No. 83-4) to clarify that "while Agent Redig was not the affiant for the search warrant, nor do these messages identify what the affiant Sgt. Powell specifically knew at the time" there was communication between two agents regarding the Wednesday arrival (ECF No. 83-1 at 8).

recall relaying the contents of this specific message to Sergeant Powell nor would she have purposefully excluded the existence of the text message. Therefore, Morrow failed to prove that Sergeant Powell knew about the message in question, let alone prove that he purposefully omitted it from the Affidavit.

Finally, although the Affidavit contains no information about the results of the surveillance, including information that agents did not observe a child in the home, there is no evidence that Sergeant Powell intentionally omitted this to support the Warrant. At the Hearing, Sergeant Powell explained that while he himself did not surveille the residence, the agents who did relayed information to him, including information that an adult man was in the home. At no point did Sergeant Powell specifically inquire if agents had observed a child in the home, rather he inferred that no child was seen in the home because he would have been informed if so. While Morrow argues that failing to include information about a child not being seen in the home is a material omission, the Court is not persuaded. For one, Sergeant Powell testified that seeing an adult male in the house did not alleviate his concerns that a child might be in danger because agents were only able to see a small portion of the house, and thus he could not rule out the possibility of a child in the home given all the other information he had. Further, as noted above, Sergeant Powell included other inconsistent information regarding the presence of a child in the home which again indicates that he was not intentionally omitting specific information so as to mislead Judge Kassebaum, but rather including any evidence that he found relevant. The Court therefore finds that Morrow failed to demonstrate by a preponderance of the evidence that Sergeant Powell intentionally omitted information about the results of the home surveillance.

Morrow has not established by a preponderance of the evidence that Sergeant Powell included misleading statements or intentionally omitted material information, thus Morrow again fails at step one. Even if the Court found for Morrow at step one, Morrow would still fail to demonstrate step two, that "the affidavit, once corrected and

supplemented, establishes probable cause." *Id.* at 1119 (citation and internal quotation marks omitted). While adding the omitted evidence and correcting the misleading statements might paint a *slightly* different picture of the urgency of the search—there is still enough probable cause to justify a search based on evidence of child pornography. Sergeant Powell included enough information in the Affidavit, untainted by these argued omissions and misleading statements, for the magistrate to find probable cause to issue the Warrant. Accordingly, the Court will not suppress any evidence based on Morrow's second *Frank's* challenge.

B. Issuance of Warrant

Morrow next argues[12] that the Warrant should be quashed because Sergeant Powell failed to obtain a signed and sworn affidavit in violation of the Fourth Amendment requirement that a warrant be "supported by oath or affirmation." (ECF No. 64 at 1-6 (citing *United States v. Vargas-Amaya,* 389 F.3d 901, 904 (9th Cir. 2004)).)[13] Specifically, Morrow proffers the transcript of the telephonic conference between Sergeant Powell and Judge Kassebaum as evidence that Sergeant Powell lacked permission to sign the Affidavit.[14] (*Id.* at 3-4.) Further, Morrow argues that the swearing in of Sergeant Powell is not enough to satisfy the oath or affirmation requirement because Judge Kassebaum never asked if the information contained in the Affidavit was true and correct nor was

---

[12]Morrow also initially argues that the Affidavit violated Nevada law (ECF No. 46 at 26-27) but abandons this argument in subsequent briefing and at the Hearing. Thus, the Court will not address it here.

[13]In *United States v. Vargas-Amaya,* the Ninth Circuit Court of Appeals held that "where a warrant is issued unsupported by oath or affirmation, it is invalid under the Fourth Amendment." 389 F.3d at 904. More specifically, the Ninth Circuit has held that "probable cause, supported by Oath or affirmation" requires "the government to establish by sworn evidence presented to a magistrate that probable cause exists . . ." *United States v. Rabe,* 848 F.2d 994, 997 (9th Cir. 1988).

[14]On the call, Sergeant Powell inquired: ". . . I will print off the search warrant applic- or I'm sorry *just the search warrant itself* and then . . . do I have your permission to sign your name to it?" (ECF No. 46-3 at 4 (emphasis included).)

there a substantive discussion regarding the facts supporting probable cause. (ECF No. 82 at 12.)

The government responds that the constitutional requirements for a warrant were met here: (1) the Warrant was issued by neutral and detached magistrate; (2) there was a showing of probable cause; and (3) a particularized description of places to be searched and things to be seized. (ECF No. 52 at 7-12.) Specifically, the government argues that Judge Kassebaum and the affiant were not required to have a substantive discussion about probable cause over the phone because an affidavit outlining probable cause, which Judge Kassebaum stated he had read, had been emailed, the affiant was sworn in over the phone, and it was "evident from the recording that Judge Kassebaum authorized his required signatures on the warrant as a whole, which expressly incorporates the affidavit." (*Id.* at 11.) Rather, the government classifies Morrow's argument as a "technical noncompliance with procedural rules" which does not require suppression of otherwise legally obtained evidence unless there is a showing of "prejudice" or "intentional and deliberate disregard of a provision." (*Id.* at 8 (citing *United States v. Stefenson,* 648 F.2d 1231, 1235 (9th Cir. 1981); *United States v. Ritter,* 752 F.2d 435, 441 (9th Cir. 1985); *Frisby v. United States,* 79 F.3d 29, 32 (6th Cir. 1996)).)

The Warrant was supported by oath or affirmation as required by the Fourth Amendment. First, the facts in the Ninth Circuit case cited by Morrow are distinguishable from those here. In *Vargas,* the Court found that a term of supervised release can be extended based on a warrant issued during the term of supervision only if the warrant was based on sworn facts. 389 F.3d at 904. Here, the Warrant and Affidavit were issued based on facts sworn under oath. Although Sergeant Powell only explicitly requested Judge Kassebaum's signature on the Warrant and not the Affidavit, the Court finds that Judge Kassebaum made clear that Sergeant Powell had authority to sign both the application (which includes the Affidavit) and Warrant on his behalf. For example, during the phone conversation, it was clear that Judge Kassebaum had received, reviewed, and

approved of, both the Affidavit and Warrant. (ECF No. 46-3 at 3.) At the telephonic hearing, Sergeant Powell asks Judge Kassebaum if he received the email application and Warrant to which Judge Kassebaum replies: "That is correct. I believe there were approximately fourteen pages of affidavit and five pages of search warrant. Is that correct?" (*Id.*) Judge Kassebaum later states: ". . . I did – I did read that and that warrant is granted. That warrant will be granted based on that affidavit and search warrant." (*Id.* at 3-4.)

Furthermore, and more importantly, Judge Kassebaum placed Sergeant Powell under oath at the beginning of the telephonic conference. (*Id.*) Finally, because Judge Kassebaum had reviewed the emailed Warrant and Affidavit and found sufficient probable cause, as evidenced by their conversation, there was no need for a substantive discussion about probable cause.

The Court therefore finds that the oath and affirmation requirement under the Fourth Amendment is satisfied. Thus, the government is correct that Morrow's argument is hyper-technical and without a showing of actual prejudice or intentional and deliberate disregard of a rule, Morrow has failed to demonstrate a constitutional violation.

C. Nighttime Search

Finally, Morrow argues that suppression is necessary because Sergeant Powell omitted material evidence in order to justify a nighttime search, thereby intentionally and deliberately disregarding the timing requirements of Federal Rule of Criminal Procedure 41.[15] Specifically, Sergeant Powell omitted material evidence—as discussed above in

[15]Morrow initially argued that suppression was necessary under Nevada law (Nev. Rev. Stat § 179.045(6)) (ECF No. 46 at 26-29), but he abandoned the Nevada law argument at both the preliminary hearing and Hearing, and instead argued that suppression is appropriate when there is "an intentional and deliberate disregard for a provision of the Rule in Rule 41." (ECF No. 82 at 20.) The Court addresses the latter argument only.

regards to the "with child" omissions—in order to create a false exigency, thereby amounting to an "intentional and deliberate disregard" of Rule 41.

The government responds that Morrow failed to raise a timely Rule 41 argument, and even so, Rule 41 only applies to federal and not state warrants. (ECF No. 83-1 at 2-3 (citing *United States v. Crawford,* 657 F.2d 1041, 1046 (9th Cir. 1981)).)[16] Rather, the only applicable standard is whether the search was reasonable under the Fourth Amendment, which it was, because nothing in the Fourth Amendment "declares a search unconstitutional simply because it occurs at night." (*Id.*)[17] Finally, the government argues that even if there was a violation related to the nighttime search, suppression is not an appropriate remedy because there was still probable cause for issuance of the Warrant. (*Id.* (citing *United States v. Pagan,* Case No. 2:16-cr-246-GMN-NJK, 2017 WL 6606851 (D. Nev. 2017; *United States v. Pruitt,* Case No. 2:16-cr-285-APG-NJK, 2017 WL 5505571 (D. Nev. 2017); *United States v. Cisneros,* 154 Fed. Appx. 591, 593 (9th Cir. 2005)).)

Contrary to the government's first argument, Rule 41 applies here. In *Crawford*, the Ninth Circuit case cited by the government, the court held that "the mere fact that evidence obtained by state officers, under a state warrant, based upon violations of state law, is used in a federal prosecution does not invoke the requirements of Rule 41." 657 F.2d at 1046. But, the decision goes on to say that if the search "is federal in character then the legality of the search should be analyzed in light of federal constitutional

---

[16]While the government responded to Morrow's modified argument at the preliminary hearing, it submitted a supplemental response following the preliminary hearing to more fully respond. (ECF No. 83.) As the Court noted at the Hearing and above, because Morrow did not raise his Rule 41 arguments until the preliminary hearing, the government's supplemental response is granted and considered here.

[17]The government argues in its response and at the Hearing that the search was reasonable because: it was initiated at a reasonable hour (10:35 pm) (ECF No. 83-2), and based on the body camera footage, Morrow was afforded freedom, offered a warm car to sit in, and additional clothing (ECF No. 83-3). The government further established reasonableness through the testimony of Sergeant Powell at the Hearing.

requirements and those provisions of Rule 41 . . ." *Id.* (citing *Lustig v. United States*, 338 U.S. 74, 78-79 (1949) (a search is a search by a federal officer "if he had a hand in it"); *United States v. Sellers*, 483 F.2d at 42 n.4 (federal search when one federal informant and federal officer participated in certain phases of the search); *United States v. Harrington*, 504 F.2d 130, 133 (7th Cir. 1974) (federal search when two federal officials were present during a state search.) As Morrow notes (ECF No. 86-1 at 2), even though the Warrant was presented to a state court justice of the peace, it was "clearly federal in character" because federal officers were involved in providing information to support the Warrant and were involved in the search. Thus, because it was a federal and not state warrant, Rule 41 applies.

Federal Rule of Criminal Procedure 41(e)(2)(A)(ii) states that a search warrant must command the officers to "execute the warrant during the daytime, unless the Judge for good cause expressly authorizes execution at another time." Fed. R. Crim. P. 41(a)(2)(B). "Daytime" is defined as "the hours between 6:00 a.m. and 10:00 p.m. according to local time." *Id.* As mentioned above, in *United States v. Stefenson,* the Ninth Circuit held:

> noncompliance with Rule 41 requires suppression of evidence only where, (1) there was 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if the rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule.

648 F.2d at 1235 (citations omitted).

Under *Stefanson,* Morrow's argument fails. A mere violation of Rule 41 is not enough when probable cause for issuance of the Warrant has been proven, as here. As discussed above, Sergeant Powell did not omit any material evidence regarding the presence or absence of a child in the home so as to create a false exigency. Therefore, Morrow failed to demonstrate an intentional or deliberate disregard of a provision of Rule

41. Furthermore, Morrow completely failed to address, let alone demonstrate any prejudice such that "the search might not have occurred or would not have been so abrasive if the rule had been followed." *Stefanson,* 648 F.2d at 1235 (citations omitted). Suppression is therefore unwarranted on Rule 41 grounds.

Moreover, the search did not violate the Fourth Amendment's reasonableness requirements. Under a Fourth Amendment analysis, courts apply the traditional reasonableness test based on the totality of the circumstances. First, the search was initiated around 10:35 pm, a reasonable hour, and Morrow was not handcuffed. (ECF No. 83-1 at 3.) Furthermore, Morrow was offered a jacket to keep warm and agreed, but was not forced, to sit in the back of a heated patrol car to stay warm while the search was conducted. (*Id.*) Finally, Sergeant Powell testified at the Hearing that the search lasted about 2.5 hours, the standard length for this type of search. In short, the search was reasonable and does not amount to a constitutional violation.

In sum, the Court will deny Morrow's motion to suppress on all grounds.

IV. CONCLUSION

The Court notes that the parties made several arguments and cited to several cases not discussed above. The Court has reviewed these arguments and cases and determines that they do not warrant discussion as they do not affect the outcome of the issues before the Court.

It is therefore ordered that Defendant's motion to suppress (ECF No. 46) is denied.

DATED this 25th Day of March 2021.

MIRANDA M. DU
CHIEF UNITED STATES DISTRICT JUDGE

Transcription of: Telephonic Search Warrant

Re: Benjamin Morrow

Transcribed by: Crystal

Date of Recording: April 20, 2019

S: Sergeant Ryan Powell

J: Judge Doug Kassebaum

J: Judge Kassebaum here. How you doing?

S: Hey. Good. How you doing Judge?

J: Good...good...good. Hey, I got to read that. You're good to go.

S: Ok. So what do we need to do for, hum, uh, the purposes of swearing me in and doing all that stuff?

J: Ok, what we're gonna have to do is record it and I don't know if we should go through your dispatch or not. That's probably the best way to do it.

S: I, I can actually record the call so if you're good now I can just record it.

J: Ok. Yeah, that's fine. Yeah-

S: -ok

J: -I'll need to get a copy too if you would, hum...

S: ok

J: and let's see uh, yeah, what I'll do I'll who I am and, uh, that you're requesting a telephonic search warrant. We'll give todays date, time. I'll have you identify yourself. Hum, how long you've been an officer. I'll swear you in and then we'll talk about the search warrant, ok?

S: Ok. Ok. So go ahead and begin whenever your ready.

J: Oh, is it recording now?

S: Yep. Yeah.

J: Ok. This is, uh, Judge Douglas R. Kassebaum of the Walker River Justice Court. And this is a request for a telephonic serach warrant for the jurisdi- jurisdiction of the Walker River Justice Court. Todays date is April 20th 2019 and it is approxamaltey 9:32 p.m. Uh, I'm on the phone right now, currently, with Sergeant Powell who's requesting the warrant. Uh, Sergeant could you please state your full name for the record, spell your last please.

S: Yes, sir. Sergeant, uh, Ryan Powell P-O-W-E-L-L

J: Ok. Thank you and how long have you been employed with Lyon County?

S: Uh, sixteen years.

J: Ok, thank you. Ok, can I get you to raise your right hand please and I'll swear you in.

S: Yes sir.

J: Ok. Do you swear to tell the truth, the whole truth, nothing but the truth so help you God?

S: That is correct, yes.

J: Ok thank you. Ok go ahead please.

S: So, uh, did you receive the, uh, email application and search warrant?

J: That is correct. I believe there were approxamley forteen pages of affidavit and five pages of search warrant. Is that correct?

S: Yes, yeah, nineteen total. Yes.

J: Ok. Yes, I did.

S: Ok. And, hum, I just want to make sure that we're good - I, I don't have to read that to you over the phone due to the, uh, I mean it's uh, 7,200 words so, hum, if, if you're good with that then I'm good with that.

J: You bet. I did - I did read that and that warrant is granted. That warrant will be granted based on that affidavit and search warrant
S: Ok. Very good. So what I'll do is the - I've requested that it's, uh, to be sealed, hum, so how do you want me to, uh, to note on the search warrant that its sealed?
J: Ok what you can do is just use my name and just put that the search warrant is to be sealed and then if you can get that into the Court Monday morning for us as soon as you can-
S: yeah
J: -we'll make sure that we complete the rest of that
S: Ok. Ok. Very good. I'll take care of that then. And then just for the purposes of the phone call-
J: - and (inaudible- two seconds)
S: I'll just uh, confirm that night- night search is approved? Is that correct?
J: that - that's correct.
S: Ok and that we did not ask for a no-knock warrant so I just checked those boxes or that box "no".
J: That's correct. I understand.
S: Ok and then, uh, so what I'll do is I will print off the search warrant applic- or I'm sorry just the search warrant itself and then, uh, do I have your permission to sign your name to it?
J: Yes, you do. Now, did you need the correct spelling of my name?
S: Oh, is it wrong in there?
J: Uh, no I believe you had it right.
S: Ok.
J: Uh, it's K-A-S-S-E-B-A-U-M.
S: So two S's right?

J: Yes, that was correct.
S: Ok. Good. Ok. Yep. I got it so I will, I will put that in there that I, uh, signed it with your permission and, hum, I think that's, that's it. I just want to make sure that you got all nineteen pages, hum, and, uh, it sounds like you did so.
J: That's correct. And can you also do me a favor too Sergeant Powell, can you make sure we get a copy of this recorded, uh, information here just as soon as you can at least within seven days ok.
S: Absolutely, yep, I will- I'll take care of that and then you-
J: -ok, that's a lot
S: -wanted me to see April on Monday right and get the and get a number assigned to it and everything?
J: That is correct, yeah.
S: Ok.
J: She'll have to get you a number and get you the information for sealing the rest of the documents and uh-
S: Ok
J: -as soon as you can Monday that would be great.
S: Yeah, very good. I will take care of that.
J: Ok, thank you Sergeant-
S: Alright thank you for your time.
J: -you have a good evening.
S: You too.
J: Ok good.
S: Alright, bye.
END OF RECORDING

Court Case # 19SW13

FILED

2019 APR 22 PM 2:50

WALKER RIVER JUSTICE COURT

IN THE WALKER RIVER TOWNSHIP JUSTICE COURT OF THE STATE OF NEVADA

IN AND FOR THE COUNTY OF LYON

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

State of Nevada, }

} ss:

County of Lyon }

I, Sergeant Ryan Powell, being first duly sworn, and under penalty of perjury, on oath say and depose the following on this 20th day of April, 2019:

1. I am a peace officer employed by the Lyon County Sheriff's Office and have been so employed for over 15 years. I am currently assigned to the Detectives Division within the Lyon County Sheriff's Office. I have been continuously employed as a Law Enforcement Officer in the State of Nevada for over 15 years. During my career, I have investigated roughly 500+ felony cases, and have received approximately 2,000+ hours of training in Nevada criminal law and criminal investigations.

2. I am currently conducting an investigation regarding Sexual Assault of a Child Under the age of 14, a felony as defined by NRS 200.366 and Possession of Child Pornography, a felony as defined by NRS 200.700.

3. That during the course of my investigation, I have learned the following information, based upon my personal knowledge, or where indicated, based upon information given me which I believe to be reliable and truthful. I offer the following relevant statements which statements are incorporated herein by reference;

- On April 20, 2019, your affiant was contacted by FBI Special Agent Cassie Redig, who stated that she was assisting with a child pornography investigation initially started with the Toledo, Ohio FBI Resident Agency Office. During the course of the investigation it was determined by FBI Agents the crimes are occurring in Fernley, NV. Agent Redig advised that she received information that the suspect in her case is with a child, described as a female juvenile between the ages of four (4) and seven (7) years old, and the suspect may be currently sexually assaulting the juvenile. Agent Redig requested the assistance of the Lyon County Sheriff's Office.

- Agent Redig provided me with the following details about her case, which are detailed as follows: On April 5, 2019, a Toledo, Ohio adult escort Roxanne Treesh (hereinafter TREESH) received a text message from 'jayd@secmail.pro' (hereinafter UNSUB), "Hi love how are u?" and "Its John...was just kinda feeling like sharing something special with u". Shortly after, UNSUB

sent her three (3) images of child pornography. TREESH told UNSUB that he was disgusting and to never message her again. One of the images depicted a prepubescent female lying on her back wearing only a blue and gray striped shirt. An adult male was anally penetrating the child with his penis. The juvenile appears to be approximately 4 to 5 years old. The adult male is wearing blue camouflaged patterned underwear. The juvenile is holding what appears to be a white in color electronic controller with a white chord. One of the images depicted a prepubescent female lying on her back wearing only a blue and gray striped shirt that was pulled up. An adult male was anally penetrating the child with his penis. The juvenile appears to be approximately 4 to 5 years old. The adult male is wearing blue camouflaged patterned underwear and tan khakis.

- One of the images depicted a prepubescent female lying on her back wearing only a white shirt with cupcakes printed on it. An adult male was anally penetrating the child with his penis while lifting the child's vagina up with his thumb. The juvenile appears to be approximately 3 to 5 years old. In the majority of the photographs, the child is being abused on top of a comforter and sheet (likely on top of a bed). The comforter is striped in different shades of gray and the bed and the bed sheet is white with tan and navy dotted squares.

- On April 9, 2019, Federal investigators interviewed TREESH. TREESH had no idea who UNSUB was. TREESH gave investigators consent to search her phone and to assume her identity utilizing her phone. On April 9, 2019, OCE -7478 began chatting with UNSUB utilizing TREESH's cell phone. UNSUB was concerned about the way TREESH initially responded to the child pornography he sent her and said, "After what u said about turning me in...we have a lot of trust to build". OCE-7478 apologized and continued chatting with UNSUB. UNSUB asked if OCE-7478 liked the pictures he sent. He asked how old OCE-7478's kids were. OCE-7478 advised that OCE-7478 had a nine-year-old daughter. UNSUB asked if OCE-7478 was active with her. UNSUB stated that the girl in the pics is 7 years old and that he plays with his niece sometimes. UNSUB stated that his favorite was under 10 years old.

- UNSUB expressed an interest in OCE-7478's daughter. OCE-7478 asked UNSUB to chat on Kik. UNSUB text messaged OCE-7478 that he got a Kik account 'adventureJ0hn'. OCE-7478 and UNSUB briefly chatted via Kik on April 9, 2019, and April 10, 2019. On April 10, 2019, OCE-7478 text messaged UNSUB if he got OCE-7478's Kik message. UNSUB responded, "Idk yet. I leave that phone at home during the day s". (This information leads investigators to believe that the UNSUB may have multiple cell phones.)

- UNSUB wanted to communicate with OCE-7478 via application 'Telegram' because it was safe and encrypted. Specifically, UNSUB wanted to speak on the phone with OCE-7478 via 'Telegram'. UNSUB explained, "I told u... we need to talk. After what u said first, I still have questions. I have a lil fuck toy so I don't need to take too many risks..."

- On April 11, 2019, OCE-7478 messaged UNSUB on UNSUB's Telegram account '@J0hncc'. On April 12, 2019, TREESH (along with investigators) placed a recorded Telegram phone call to

UNSUB. During the recorded phone call, UNSUB states that he is glad TREESH liked the pictures he sent and asked TREESH about her 9 year old daughter. UNSUB asked if her daughter had ever had sex before and if TREESH had ever played with her daughter. UNSUB stated with his niece when she was 5 years old and that he doesn't see her often. UNSUB thought that his niece's ass was better because if you started playing with their ass first, its less noticeable.

- UNSUB requested to see sexual pictures of TREESH's 9 year old daughter. UNSUB asked TREESH if she got wet and excited when she got the pictures he sent her. He further asked if she got a toy and rubbed one out. After the recorded phone call concluded, UNSUB messaged OCE-7478 via Telegram that he had to get back to work.

- On April 12, 2019, UNSUB Telegram messaged OCE-7478 eight (8) images of child pornography. The images are described below: The first image is of a prepubescent female, approximately 4-6 years old, lying on her back. She appears to be wearing a red long sleeved shirt. Her legs are up and her vagina and anus are the focal point of the picture. The second image is of a prepubescent female, approximately 4-6 years old, lying on her back. She is being anally penetrated by an adult male's penis. The image is a close-up and it does not appear that the child is wearing any clothing. The third image is of a prepubescent female, approximately 4-6 years old, lying on her stomach on top of a comforter. The child is only wearing a green shirt that is pulled up. She is being anally penetrated by an adult male's penis. The male is wearing a gray shirt and what appears to be red and black checkered fleece pants. The fourth picture is of a prepubescent female, approximately 4-6 years old, lying on her back. She is being anally penetrated by an adult male's penis. The image is a close-up and it does not appear that the child is wearing any clothing. The fifth picture is of a prepubescent female, approximately 4-6 years old, lying on her stomach. She is only wearing a green shirt. The focal point is of the child's vagina and buttocks. The sixth picture is of a prepubescent female, approximately 4-6 years old, lying on her back. The picture is close-up and the child does not appear to be wearing any clothing. The focal point of the picture is the child's vagina and anus. In front of the child's anus and vagina is an adult male's erect penis. The seventh picture is of a prepubescent female, approximately 4-6 years old, lying on her back. She is only wearing a blue and gray long sleeved shirt that is pulled up. The focal point is of an adult male's penis ejaculating into the child's anus. The eighth picture is of a prepubescent female, approximately 4-6 years old, lying on her back. She is only wearing a blue and gray striped long sleeve shirt that is pulled up. The child is holding an adult male's erect penis in her hands between her legs. In the majority of the photographs, the child is being abused on top of a comforter and sheet (likely on top of a bed). The comforter is striped in different shades of gray and the bed sheet is white with tan and navy dotted squares.

- On approximately April 14, 2019, a subpoena was served to Kik for subscriber and IP information for account 'adventureJ0hn'. On April 16, 2019, Kik responded with the following information: First Name: John Last Name: C Email: jayd@secmail.pro Username: adventureJ0hn 2019/04/10 and 2019/4/11, "ip":"172.221.35.154" and 2019-04-11 "ip":"149.56.182.0". An Arin.net search was conducted for "ip":"172.221.35.154" which returned to Charter Communications. An

Arin.net search was conducted for "Ip":"149.56.182.0" which returned to CactusVPN Inc. On Approximately April 16, 2019, an exigent subpoena was served to Charter Communications for subscriber information associated with 2019/04/10. and 2019/4/11, "Ip":"172.221.35.154". Because the subpoena request was exigent, Charter Communications telephonically informed investigators that the subscriber was Benjamin Morrow of 313 Appaloosa Way, Fernley, Nevada 89408. (Note: Morrow's DMV lists him at 1361 Horse Creek Way, Fernley, NV. Law Enforcement Search database – 'CLEAR' lists both addresses as recent as 12/31/2018. FBI Intelligence Analyst Rob Smith did a GMAN search for Morrow and found a Telegram account (402866408) associated with Morrow and also a Whatapp account (unknown account name) – for both accounts; telephone number 816-308-6031 is listed).

- On April 16, 2019, UNSUB stated that he lives in LA (Los Angeles, CA.) and travels all over for work. UNSUB states, "I was just imagining u teaching ur daughter how to suck my dick". On April 20, 2019, UNSUB messages OCE-7478 on Telegram, "I'm going to see my fuck toy for spring break", "Just for a day. Her and her mom are coming to see me", "My dick is about to explode", "This week sometime not sure what day yet". He further messages, "Does your little one like sucking dick?...", I'm trying to get my niece to give better head lol", "She needs a good teacher". OCE-7478 asks, "R u worry about ur niece telling". UNSUB responds, "Sometimes yeah but we have been active for a couple years", "So if I made it past that I think I'm good to go".

- After speaking with Agent Redig, I contacted other Lyon County Sheriff's Office Detectives to assist in this investigation. Detectives were briefed on the details of the case. LCSO records were searched and Benjamin Morrow was found in local records, indicating that he resides at both 1361 Horse Creek Way, Fernley, NV. AND 313 Appaloosa Way, Fernley, Nevada 89408.

That for the purposes of this affidavit, your Affiant further states and informs the Court:

DEFINITIONS

As used in NRS 200.700 to 200.760, inclusive, unless the context otherwise requires:

1. "Performance" means any play, film, photograph, computer-generated image, electronic representation, dance or other visual presentation.
2. "Promote" means to produce, direct, procure, manufacture, sell, give, lend, publish, distribute, exhibit, advertise or possess for the purpose of distribution.
3. "Sexual conduct" means sexual intercourse, lewd exhibition of the genitals, fellatio, cunnilingus, bestiality, anal intercourse, excretion, sado-masochistic abuse, masturbation, or the penetration of any part of a person's body or of any object manipulated or inserted by a person into the genital or anal opening of the body of another.
4. "Sexual portrayal" means the depiction of a person in a manner which appeals to the prurient interest in sex and which does not have serious literary, artistic, political or scientific value.

1. The following non-exhaustive list of definitions applies to this Affidavit:

a. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.)

b. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves, obscene or illegal. In contrast to "child pornography," this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries. *See* Kenneth V. Lanning, *Child Molesters: A Behavioral Analysis* (2001) at 65. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child pornography cases. *See United States v. Vosburgh*, 602 F.3d 519 (3d Cir. 2010) (possession of child erotica is admissible because images suggest that defendant harbors sexual interest in children and to disprove lack of knowledge or mistake); *United States v. Cross*, 928 F.2d 1030, 1050 (11th Cir. 1991) (testimony about persons deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant).

c. "Visual depictions" include developed or undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

d. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

e. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

f. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

g. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic,

magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. "Computer software," as used herein, is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. "Internet." As used herein, is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. "Internet Service Providers," or "ISPs," are commercial organizations that provide individuals and businesses access to the Internet. ISPs can offer various means by which to access the Internet including telephone-based dial-up, broadband-based access via a digital subscriber line (DSL) or cable television, or satellite-based subscription. Many ISPs assign each subscriber an account name. By using a computer connected with an Internet capable modem, the subscriber can establish a connection to the Internet through the ISP service.

l. "Internet Protocol address," or "IP address," The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

m. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard drives, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device.

n. "Digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central processing units; desktop computers; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes, and memory chips; and security devices.

o. "Storage medium or medium": A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

p. "Imaging" or "copying" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.

"Hash value" refers to a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data. A hash value can be described as a digital fingerprint for a computer data file. Any alteration of a computer data file would change that file's hash value.

BACKGROUND ON COMPUTERS AND EVIDENCE ASSESSMENT PROCESS

1. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One

form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

2. I submit that if a computer or storage medium is found on the Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Individuals can transfer images and videos from one electronic device to others through direct connection, scanning, wireless transfer, and other electronic means.

b. Computers and other digital storage devices are capable of storing large amounts of electronic data, which can include images and videos. This data can be electronically stored virtually anywhere within the file structure on the device. Storage device sizes have continued to increase and the chances of recovering previously deleted content from these devices also has increased as a result of the content being less likely to be overwritten with the increase in storage size.

c. As is the case with most digital technology, computer communications can be saved or stored on hardware and computer storage media used for these purposes. Storing of information can occur through intentional acts of saving or downloading files, or by other methods; which automatically occur through normal computer use. This automatic storing of information can be considered "footprints" of use in which the device stores temporary files, links, cached files, opened and accessed files, and history. This information, like any other data can be stored for extensive periods of time until overwritten or intentionally wiped or destroyed. A thorough search of the data contained on these devices could often uncover evidence the crimes listed in this affidavit.

d. Data that exists on a computer is particularly resilient to deletion. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive or other storage medium, deleted, or viewed via the Internet. Even when such files have been deleted, they can often be recovered later using readily available forensic tools. When a person "deletes" a file on a home computer, the file is sent to the recycle bin, where it can be easily accessed by the user. Even when a person deletes a file from the recycle bin, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

e. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

f. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

g. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

h. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

3. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premise for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a

computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to examine storage media thoroughly to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools and software.

4. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

5. Because it may be determined other computer users could share the Premises as a residence, it is possible that the Premises will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well. Efforts would normally be taken during the search to minimize seizing of unrelated evidence through onsite computer forensic previewing when possible.

a. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

BACKGROUND ON CHILD EXPLOITATION WITH THE USE OF TECHNOLOGY AND OFFENDER CHARACTERISTICS INVOLVING SUCH ACTS

1. Based upon my knowledge, training, and experience in online child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers and computer technology have revolutionized the way in which child pornography is produced, distributed, stored and communicated as a commodity and a further tool of online child exploitation.

2. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals involved in the advertisement, transportation, distribution receipt and possession of child pornography. Those who advertise, transport, distribute, receive and/or possess child pornography. These individuals:

a. May receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. May collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Often possess and maintain "hard copies" of child pornographic material, which is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years. These individuals may be referred to as "collectors."

d. Often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and may be kept close by, usually at the individual's residence, to

enable the collector to view the collection, which is valued highly. The collections are often backed up on external devices or other digital media. These "collectors" claim to be unable to delete or be without the material for any extended period of time. These "collectors" may also choose to store their material online using "cloud" based file storage provided by Internet Service Providers (ISP). This "cloud" based storage allows an offender to store the material on servers maintained by ISPs and access the material anywhere in the world through an internet connection.

e. May correspond with and/or meet others to share information and materials; often maintain correspondence from other child pornography distributors/collectors; may conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. May engage in a pattern of continual activity involving the download and sharing of child pornography for sexual gratification, regardless of their actions of storing, collecting, or deleting the material.

g. May take steps to avoid detection by intentionally downloading, viewing, and maintaining dominion and control of child pornography related material to achieve sexual gratification, then purposely deleting the material until choosing to download again. Individuals previously showing traits as a "collector" may have transitioned into a deleting behavior pattern due to the ease and accessibility of child pornography through the internet.

h. May collect non-sexually explicit images and/or videos of children relating to their preference concerning age, sex, hair color, body type, and other physical characteristics and maintain those images in similar manner as the child pornography described above.

i. May organize, catalog, and separate their collections based on physical characteristics of the children, series, or scene types and settings.

j. Often download large quantities of child pornography during online sessions and later filter through the material to locate the desirable content to save based upon the offender's preferences at the time or to determine of the file is already in their possession.

k. Sometimes enjoy and maintain both adult and child pornography ranging in broad types of scene content or portrayal from voyeuristic nudity to brutal rape scenes. Offender's preferences of the scene settings often change from time to time in addition to showing a progression towards more sexually explicit material.

4. Your affiant has positively identified Benjamin Morrow through local and N.C.I.C. records. He is a white male adult; date of birth of [Social Security Number of [Benjamin Morrow is listed as 5'07" in height and weighs 180 pounds. He has brown hair and blue eyes, according to Nevada DMV records.

5. It is my opinion, based on the above-asserted facts, that Benjamin Morrow is engaged in possession of Child Pornography, and is in fact in possession of child pornography, located at 313 Appaloosa Way, Fernley, Nevada 89408.

6. It is my opinion that images and videos of child pornography will be found at 313 Appaloosa Way, Fernley, Nevada 89408 and Benjamin Morrow will continue to possess child pornogrphy at the time this warrant is served.

7. Based on the foregoing information, your affiant believes there is probable cause to search the premises located at 313 Appaloosa Way, Fernley, Nevada 89408 described as:

A Tan in color single story "stick built" residence with white trim. The front door faces east and there is a white picket fence around the front yard. The numbers '313' are affixed to the right side of the garage.

8. Based upon the information in this affidavit, your affiant asks for a search warrant that includes the following described person:

1.Benjamin Morrow / DOB: SSN:

9. You affiant is requesting that this search warrant affidavit to be sealed as the details and information listed in the affidavit are so specific that if released to the suspect the investigation would be compromised. Additionally there is a juvenile(s) involved in this investigation and their protection is paramount to assure their safety and general health and welfare.

10. WHEREFORE, I request that a search warrant be issued, directing that a peace officer of the County or the State of Nevada, to include Federally Sworn Law Enforcement Officers (to include but not limited to, Federal Bureau of Investigation Special Agents and Department of Homeland Security Special Agents) make a search of the residence and/or person described above. That such search is to be made during any time of day or night, for the purpose of seizing the above described property.

Given under my hand and dated: 4/20/2019 2019

Affiant

Subscribed and sworn before me on: 4/20/19, 2019 at 2135 a.m./(p.m.)

Doug Kassebaum by Det. Sgt. Powell

Judge

TELEPHONIC SW

*Case #*_____

IN THE WALKER RIVER TOWNSHIP JUSTICE COURT OF THE STATE OF NEVADA

IN AND FOR THE COUNTY OF LYON

***

SEARCH WARRANT

***

State of Nevada, }

} ss:

County of Lyon }

AFFIDAVIT SEALED PER REQUEST

The State of Nevada, to any Sheriff or Peace Officer in Lyon County, State of Nevada to include Federally Sworn Law Enforcement Officers (to include but not limited to, Federal Bureau of Investigation Special Agents and Department of Homeland Security Special Agents): Proof of Affidavit having been made before me this day by Detective Sergeant Ryan Powell. The Affidavit is incorporated by this reference. That there is probable cause to believe that the property described herein may be found at the location set forth herein and that it is lawfully seizable as indicated below:

YOU ARE THEREFORE COMMANDED TO SEARCH: The premises located at 313 Appaloosa Way, Fernley, Nevada 89408, Nevada described as:

A Tan in color single story "stick built" residence with white trim. The front door faces east and there is a white picket fence around the front yard. The numbers '313' are affixed to the right side of the garage.

PERSONS:

1. Benjamin Morrow /

FOR THE FOLLOWING PROPERTY:

Any computers, associated storage devices and/or other devices located therein that can be used to store information and/or connect to the Internet, for records and materials evidencing a violation of NRS 200. which make it a crime to possess, by computer, child pornography; as more specifically identified below:

1. Any and all computers, computer system and related peripherals, cellular telephones, gaming consoles, personal digital assistants, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, tape systems and hard drive, terminals (keyboards and display screens) and other computer related operation equipment, in addition to computer photographs, digital graphic file formats and/or photographs, slides or other visual depictions of such digital graphic file format equipment that may be, or are used to visually depict child pornography, information pertaining to the sexual interest in child pornography, sexual activity with children or the distribution, possession, or receipt of child pornography, or information pertaining to an interest in child pornography.

2. Any and all material depicting child pornography, any sexual conduct regardless of whether it is between adult(s) and children, or between children, child erotica; any images, visual recording, digital imagery, sketches, drawings, or other media depicting or portraying lewd or lascivious exhibition of children's genitalia; sexually suggestive poses involving children; or any type of sexually explicit conduct involving children, as defined in Title 18, United States Code, Section 2256(8). Any and all audio recordings involving children engaging in sexual acts, whether alone, with another child or children, or with an adult or adults.

3. Any and all computer software, including programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

4. Any computer-related documentation, which consists of written, recorded, printed or electronically stored material that explains or illustrates how to configure or use computer hardware, software or other related items.

5. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs and electronic messages), pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as

defined in Title 18, United States Code, Section 2256.

6. In any format and media, all originals, copies and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

7. Any and all cameras, camera equipment, photography equipment or any other digital device capable of recording or storing sexually explicit images of minors in negative, digital or other format.

8. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs and electronic messages) identifying persons transmitting through interstate or foreign commerce, including via computer, any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

9. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs, electronic messages, other digital data files and web cache information), bearing on the receipt, shipment or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

10. Records of communication (as might be found, for example, in digital data files) between individuals concerning the topic of child pornography, the existence of sites on the Internet that contain child pornography or who cater to those with an interest in child pornography, as well as evidence of membership, subscription or free membership, in online clubs, groups, services, or other Internet sites that provide or make accessible child pornography to its members and constituents.

11. Evidence of any online storage, e-mail or other remote computer storage subscription to include unique software of such subscription, user logs or archived data that show connection to such service, and user login and passwords for such service.

12. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

13. Records, in any format or media, evidencing ownership or use of computer equipment and paraphernalia found in the residence to be searched, including, but not limited to, sales receipts, registration records, records of payment for Internet access, records of payment for access to newsgroups or other online subscription services, handwritten notes and handwritten notes in computer manuals.

14. Any and all buddy lists, correspondence, or text messages in whatever media and format pertaining to Group E-Mails which relate to child exploitation or child pornography.

15. Images and videos of children in non-sexually explicit poses or scenes, located in

electronic, digital, or printed formats, which are necessary for comparison purposes of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

16. Any and all records, in any format, relating to or showing use of peer-to-peer filing sharing programs and software.

17. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the lack of such malicious software;

d. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. Evidence of the times the COMPUTER was used;

g. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER.

AND TO SEIZE IT IF FOUND and bring it forthwith before me, or this court, at the courthouse of this court. The Affidavit in support of this Search Warrant is attached to this Search Warrant and was sworn to and subscribed before me this ~~THIRTY~~ 20 day of APRIL, **2019** at 2135 A.M./P.M. Wherefore, I find probable cause for the issuance of this Search Warrant and do issue it.

NIGHT SEARCH APPROVED: YES (XXX) NO ( )

KNOCK AND ANNOUNCE WITHOUT

WAITING FOR A RESPONSE: YES ( ) NO (XXX)

Doug Kassebaum by DEI SGT. Powell of SCSO

Judge Douglas Kassebaum

Walker River Township Justice Court

Yerington, NV. 89447

No. _____

IN THE

SUPREME COURT OF THE UNITED STATES

Benjamin D. Morrow — PETITIONER
(Your Name)

VS.

United States of America — RESPONDENT(S)

PROOF OF SERVICE

I, Benjamin D. Morrow, do swear or declare that on this date, September 21, 2023, as required by Supreme Court Rule 29 I have served the enclosed MOTION FOR LEAVE TO PROCEED *IN FORMA PAUPERIS* and PETITION FOR A WRIT OF CERTIORARI on each party to the above proceeding or that party's counsel, and on every other person required to be served, by depositing an envelope containing the above documents in the United States mail properly addressed to each of them and with first-class postage prepaid, or by delivery to a third-party commercial carrier for delivery within 3 calendar days.

The names and addresses of those served are as follows:

U.S. Solicitor General
950 Pennsylvania Ave., NW, Room 5614
Washington, DC 20530

I declare under penalty of perjury that the foregoing is true and correct.

Executed on September 21, 2023

(Signature)