

**IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF ARKANSAS
FAYETTEVILLE DIVISION**

UNITED STATES OF AMERICA

v.

Criminal No. 5:21CR50014-001

JOSHUA JAMES DUGGAR

**UNITED STATES' RESPONSE TO DEFENDANT'S
MOTION TO COMPEL**

Comes now the United States of America, by and through Dustin Roberts and Carly Marshall, Assistant United States Attorneys for the Western District of Arkansas, William G. Clayman, Trial Attorney for the United States Department of Justice, and for its Response to the Defendant's Motion to Compel Discovery (Doc. 31), states:

I. SUMMARY OF ARGUMENT

As with many cases based on undercover investigations of individuals sharing child sexual abuse material ("CSAM") over peer-to-peer networks, this case is straight-forward. In May 2019, Detective Amber Kalmer in Little Rock, Arkansas, used a law enforcement tool to download files depicting the sexual abuse of children directly from the user of a single Internet Protocol ("IP") address over the BitTorrent peer-to-peer network. The detective sent a lead related to her undercover downloads to Special Agent Gerald Faulkner with Homeland Security Investigations ("HSI"), who determined that the IP address was assigned to the defendant's small used car dealership in this District at the time of the downloads and applied for a warrant to search the premises. During the execution of the warrant, law enforcement seized the dealership's computer and multiple electronic devices belonging to the defendant. Based on forensic artifacts found on these devices, among other evidence, a federal grand jury returned a two-count indictment

charging the defendant with receipt and possession of child pornography.

Faced with these charges, the defendant has moved to compel the production of non-existent material related to Detective Kalmer's undercover downloads and, separately, material related to other downloads conducted by other law enforcement officers not involved with this case and not in the Government's possession. The problem with the defendant's motion, however, is that it appears to be based on a misapprehension of this investigation and the basis for the charges against him. The United States has already provided him with comprehensive discovery, including all relevant log files associated with Detective Kalmer's undercover downloads, which are described above, in the search warrant affidavit, and in the testimony of Special Agent Faulkner during the detention hearing on May 5, 2021. While it might strain the defendant's credulity, the Government, as it has advised numerous times, has provided all the discovery covering Detective Kalmer's involvement in this case.¹

The other officers who downloaded CSAM from the user of the defendant's IP address, as the United States has also already advised, played no part in the investigation of this case and did not provide the prosecution team with any materials related to their activity. The officers' downloads therefore in no way informed the magistrate judge's determination that there was probable cause to search his car lot, nor did they provide the basis for any of the charges in this case. In short, the information the defendant now seeks, to the extent it even exists, is immaterial to all aspects of this case. The Government has complied with and will continue to comply with all pertinent discovery obligations. The defendant's conclusory assertions to the contrary fall well

¹ Importantly, even if Detective Kalmer did author certain reports, which she did not, the existence of said reports would not automatically trigger a discovery obligation. As argued below, if the detective's activities are documented in the HSI reports that have been provided in discovery, the defendant's motion equates to asking this court for early disclosure of Jencks material.

short of establishing the requested information's materiality under Rule 16, *Brady*, *Giglio*, or any other relevant legal precedent, and his motion represents nothing more than a request to embark on an impermissible fishing expedition for evidence that is either nonexistent, immaterial to his defense, or already produced. Accordingly, the defendant's motion should be denied.

1. The United States' Investigation

As set forth in the extensive materials already provided to the defendant, the present case came to law enforcement's attention in May 2019, when Detective Kalmer of the Little Rock Police Department was conducting an undercover online investigation on the BitTorrent peer-to-peer file-sharing network. (Detention Hearing Transcript "Tr" p. 13). During her investigation, she observed that a user connected to the network from IP address 167.224.196.113 ("the target IP") was sharing CSAM over the network. Using a BitTorrent software designed for law enforcement, Detective Kalmer downloaded CSAM directly from this user. (Tr. pp. 14-15). The downloaded files include:

- A video file downloaded at approximately 5:42 PM on May 14, 2019, depicting two fully nude prepubescent females, one of whom is vaginally penetrated by an adult male; and
- A zip file downloaded at approximately 6:45 PM on May 15, 2019, containing approximately 65 image files of a prepubescent female, many of which are child pornography, including an image depicting the girl lying on her back and using her hands to expose her vagina and anus.

(Tr. pp. 14-15).

After downloading these files, Detective Kalmer determined that the target IP geolocated to Northwest Arkansas. She then contacted HSI Special Agent Faulkner, who investigates federal child pornography offenses in Northwest Arkansas, to inquire if he would further investigate the user of the target IP. (Tr. p. 16). After Special Agent Faulkner advised that he would, Detective Kalmer notified the Internet Crimes Against Children ("ICAC") administrator with the Arkansas

State Police (“ASP”) of the downloads, which were logged in the ICAC Data System (“IDS”), and told the administrator that Special Agent Faulkner had indicated he was willing to investigate her lead further. The ASP administrator then forwarded the lead information to Special Agent Faulkner. (Tr. p. 16).

According to law enforcement databases, two other law enforcement officers in Arkansas appear to have likewise downloaded CSAM from the user of the target IP over the BitTorrent peer-to-peer network on May 14, 2021. These officers did not advise Special Agent Faulkner that they had downloaded CSAM from the user of the target IP, nor did they send him any information related to these downloads.

After receiving the lead from Detective Kalmer, HSI Special Agents Faulkner and Howard Aycock determined that the target IP was issued by an internet service provider known as Ozarks Go and requested subscriber information associated with the user’s account. (Tr. p. 16). On or about October 7, 2019, in response to a federal summons, Ozarks Go identified the subscriber associated with the target IP at the time of Detective Kalmer’s undercover investigation as the defendant, with an address that ultimately returned to the defendant’s used car dealership—Wholesale Motorcars—in the Western District of Arkansas. (Tr. p. 16-17). Relying on Detective Kalmer’s undercover downloads, the information provided by Ozarks Go, and additional background information related to the defendant and online child pornography and BitTorrent investigations, among other information, Special Agent Faulkner applied for a federal warrant to search the Wholesale Motorcars lot for child-pornography-related evidence. (See Government’s exhibit A). Special Agent Faulkner’s affidavit in support of his application for a search warrant only referenced Detective Kalmer’s undercover downloads and did not discuss whether any other officers had downloaded CSAM from the target IP in May 2019, as he had not received any

information from any officers or other law enforcement agencies regarding any additional downloads. On November 4, 2019, then-Chief Magistrate Judge Erin L. Wiedemann issued a warrant to search the defendant's car lot based on Special Agent's Faulkner's application. *Id.*

At approximately 3:00 p.m. on November 8, 2019, law enforcement executed the warrant. Agents encountered the defendant and two other men standing outside on the car lot. (Tr. p. 18-20). Inside the small building on the lot, which operated as the business's main office, law enforcement located an HP Desktop Computer with an image of the defendant and his family on its screen. (Tr. 23-24). A subsequent forensic examination of that device and other devices seized from the defendant and the car lot pursuant to the warrant uncovered evidence demonstrating that the defendant used the HP Desktop to download from the internet and, subsequently, possess multiple files depicting minors engaged in sexually explicit conduct. (Tr. 34).

2. Procedural Background and Relevant Case History

A grand jury sitting in the Western District of Arkansas later returned a two-count indictment charging the defendant with receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2), and possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). (Doc. 1). This case was originally set for trial on July 6, 2021. (Doc. 15). However, on motion of the defendant, the Court continued the trial until November 30, 2021. (Doc. 28).

On June 2, 2021, the United States provided the defendant with a screenshot reflecting that two other law enforcement officers in Arkansas also downloaded CSAM from the target IP over the BitTorrent network on May 14, 2019. (Doc. 31-1). On July 9, 2021, the defense requested all discovery related to the screenshot, all reports from the two other officers, all reports from Detective Kalmer, and all log files related to law enforcement's use of Torrential Downpour to download CSAM from the target IP, among other things. (Doc. 31-3). In response, the United

States provided all the relevant log files related to Detective Kalmer’s undercover downloads from the target IP on May 14 and May 15, 2019, and explained that material related to the screenshot and the activity of the two other officers is extraneous to the instant case and therefore not discoverable. (Doc. 31-4). The United States reiterated and expanded on this on July 21, 2021, explaining to the defense that the material they sought was not discoverable because the two other officers played no part in the investigation or the prosecution of the defendant’s federal case and that the United States provided the screenshot to simply make the defense aware that other officers not involved with this prosecution had downloaded CSAM from the target IP. (Doc. 31-6).

On July 26, 2021, the defendant filed the instant motion pursuant to Federal Rule of Criminal Procedure 16 (“Rule 16”) and the Supreme Court’s decisions in *Brady v. Maryland*, *Giglio v. United States*, and *Kyles v. Whitley*, requesting that “this Court enter an Order compelling the Government to produce (1) all discovery related to, and underlying, an undated screen shot disclosed by the Government ... and (2) all law enforcement reports and related discovery prepared by the Little Rock, Arkansas law enforcement entity and 2 other unidentified law enforcement entities which participated in the investigation of this case.” (Doc. 31 at 1–3).

II. ARGUMENT

Criminal defendants do not have a constitutional right to discovery absent a specific “statute, rule of criminal procedure, or other entitlement.” *United States v. Johnson*, 228 F.3d 920, 924 (8th Cir. 2000). The United States has complied with its Rule 16, *Brady*, and other discovery obligations and will continue to comply with both the letter and spirit of those obligations. In his motion, however, the defendant seeks to compel the United States to turn over either nonexistent or immaterial information to which he is not entitled. Specifically, with respect to Detective Kalmer’s undercover downloads, the defendant seeks material that does not exist. And with respect

to the screenshot and the other officers' downloads, he incorrectly asserts that the United States has already conceded that the information he now seeks is discoverable based on a strained reading of prior communications while simultaneously asserting that the requested information is material based on his own *ipse dixit* that it is and his mistaken assumption that the other officers are members of the prosecution team. He also asserts with little explanation that the requested information will allow him to impeach Special Agent Faulkner based on a misunderstanding of the evidence and the agent's prior testimony. In short, the defendant fails to demonstrate that the various categories of information he seeks are discoverable under any of the relevant rules, standards, or legal precedent, and his motion should therefore be denied.

1. The United States Has Produced All Relevant Discovery Related to Detective Kalmer's Investigation

In his instant motion, the defendant seeks, among other things, "all law enforcement reports and related discovery prepared by the Little Rock, Arkansas law enforcement entity," presumably referring to Detective Kalmer's undercover investigation in which she downloaded files of CSAM from the defendant's IP address. (Doc. 31 at 1). Without any elaboration or evidence, the defendant asserts that "[i]t strains credulity" to believe the United States has produced all relevant discovery related to Detective Kalmer's investigation because of the few months that passed between her undercover downloads and HSI's investigative activity.² (Doc. 31 at 8). The defendant offers no explanation as to why this strains credulity, of course, because his claim is nothing more than

² As Special Agent Faulkner testified, HSI received Detective Kalmer's lead shortly after her May 2019 undercover downloads and Ozarks Go responded to HSI's federal summons in October 2019. (Tr. at pp. 16, 60). A thorough review of the discovery provided—which includes the federal summons HSI issued to Ozarks Go well before October 2019—confirms the faulty premise of the defendant's argument. More importantly, the defendant has not identified any actual or potential inconsistencies in Special Agent Faulkner's sworn statements, either at the detention hearing or in the affidavit in support of the search warrant, rendering his claim that the information he seeks might provide him with material to use to impeach Special Agent Faulkner meritless.

impermissible, rank speculation. *United States v. Hoeffener*, 950 F.3d 1037, 1043 (8th Cir. 2020) (noting that discovery requests require more than “mere speculation or conjecture”).

In any event, the defendant is mistaken. The United States has produced the relevant log files documenting Detective Kalmer’s undercover downloads and has confirmed that Detective Kalmer did not produce any reports related to this activity. As the United States has repeatedly made clear, after she downloaded the CSAM from the target IP, Detective Kalmer contacted Special Agent Faulkner to see if he would further investigate the user of that IP address, at which point he took the investigative lead. The information the defendant seeks is nonexistent, and this portion of his motion to compel should therefore be denied.

2. The Remaining Information the Defendant Seeks Is Not Material to his Defense under Rule 16

Under Rule 16, a defendant has a right to inspect documents, data, or tangibles objects “if the item is within the government's possession, custody, or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant.” Fed. R. Crim. P. 16(a)(1)(E). Information is material under Rule 16 if it is “helpful to the defense.” *United States v. Jean*, 891 F.3d 712, 715 (8th Cir. 2018) (citation omitted). “But a showing of materiality is not satisfied by a mere conclusory allegation that the requested information is material to the preparation of the defense.” *Id.* (citation and quotation marks omitted). Nor is it satisfied by “speculation or conjecture.” *Hoeffener*, 950 F.3d at 1043. Rather, a defendant must present some evidence to show that the government is in possession of information that would be helpful to the defense. *United States v. Krauth*, 769 F.2d 473, 476 (8th Cir. 1985); *see also United States v. Jean*, Case No. 5:15-CR-50087-001, 2016 WL 6886871, at *4 (W.D. Ark. Nov. 22, 2016) (“[T]he defendant must demonstrate that the requested evidence bears some abstract logical relationship to the issues in

the case.” (citation and quotation marks omitted)); *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990) (noting that “[n]either a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense”).

Here, the defendant seeks “all discovery related to, and underlying, an undated screen shot” reflecting that two other officers in Arkansas also downloaded CSAM from the user of the defendant’s IP address on May 14, 2019, and “all law enforcement reports and related discovery prepared by . . . [the] 2 other unidentified law enforcement entities which participated in the investigation of this case.” (Doc. 31 at 1). His primary claims to the materiality of this information are: (1) his counsel’s assertion, without any supporting authority, that the two other officers’ log files might reveal the type of device from which they downloaded CSAM from the target IP; and (2) his view that the Government has conceded that the material he seeks is discoverable and should therefore be “estopped” from opposing his motion. (Doc. 31 at 6–8). As explained below, neither of these theories has any merit, and his motion to compel pursuant to Rule 16 should be denied.

As an initial matter, the defendant’s claim that the two other officers “participated in the investigation of this case” is speculative and, ultimately, incorrect. (Doc. 31 at 1). He concedes as much, noting that he has no information about what “involvement either had in investigating this matter.” *Id.* And despite the voluminous discovery produced thus far, he has not pointed to a single document describing or even referencing the other officers’ involvement. That is because, as the United States has repeatedly advised him, they had no involvement with the investigation or prosecution of this case. *See* (Doc. 31-4; Doc. 31-6). And importantly, none of their materials is in the possession of the prosecution team.

Indeed, the defendant's motion brushes past its most fundamental defect: the activity of the two other law enforcement officers is immaterial to this entire case. In fact, the defendant appears to misapprehend the charges here, drawing an inapt comparison between this case and a "gun case" in which the government produces "a picture of the gun allegedly at issue" but not the gun itself. (Doc. 31 at 7–8). To frame it in those terms, this is a receipt of child pornography case; the details of a picture documenting his distribution of child pornography to officers not involved with the case is not at issue. The officers' undercover downloads do not serve as the basis for either of the charges against him, nor did they lend any support to the probable cause set out in the search warrant affidavit. The defendant is of course free to challenge the magistrate judge's probable cause determination, but any such challenge is limited to the information contained within the four corners of the affidavit. See *United States v. Etheridge*, 165 F.3d 655, 656 (8th Cir. 1999). In that regard, the United States has provided the defendant with all the relevant information regarding Detective Kalmer's undercover downloads, which are detailed in the affidavit. The information he now seeks related to the screenshot and the other officers, however, has no relationship to any of the issues in this case, and his motion should be denied.

Seeking to avoid this result, the defendant speculates that the information he requests might "reveal the type of *hardware* a file was allegedly downloaded from," and that the other officers' log files might differ from Detective Kalmer's log files in this respect. (Doc. 6–7). The defense provides no support for this claim beyond its own conclusory assertion, nor does it attempt to explain if Detective Kalmer's log files contained such information. The United States, on the other hand, reviewed her log files and found no such information, confirming that the defendant's current request is based on nothing more than wishful speculation. And even assuming *arguendo* that such information exists in the other officers' log files—which, to be clear, the United States

doubts based on Detective Kalmer’s log files but ultimately does not know, as the other officers played no role in this investigation and did not provide any material to the United States—it would not be helpful to the defense because it would not provide any logical basis for the defendant to challenge the search warrant or the indictment. Put simply, the activity of these other officers is immaterial to his defense.³

The defendant also argues that the United States has conceded that the information he seeks is discoverable and that the Court should find that the United States is “estopped” from opposing his motion. (Doc. 31 at 7). The defendant is again mistaken. The United States made clear in its initial communication that it was producing a document that merely reflected the fact that two other officers in Arkansas downloaded CSAM from the defendant’s IP address on May 14, 2019. (Doc. 31-1). To the extent any subsequent communication left the defense confused, the United States twice confirmed in writing—and is confirming again now—that the document was produced to make the defense generally aware of the two other officers’ downloads, but its production in no way should be construed to suggest that the United States believes the additional information the

³ To the extent the defendant’s motion is requesting access to any law enforcement database related to the software used to download CSAM from the user of his IP address or the software itself, the United States notes separately that such information is protected from disclosure by law enforcement privilege. As other courts have explained in similar cases, “the government has a legitimate interest in preserving its ability to investigate and prosecute the distribution of child pornography” and the databases maintained by various law enforcement entities in connection with online peer-to-peer investigations “contain[] highly sensitive information about thousands of ongoing investigations into child pornography worldwide, including hash values for torrents of interest and the IP addresses of both suspects and investigating officers.” *United States v. Gonzales*, No. CR-17-01311, 2020 WL 5210821, at *11 (D. Ariz. Sept. 1, 2020); *see also United States v. Chiaradio*, 684 F.3d 265, 278 (1st Cir. 2012) (noting that “the government reasonably fears that traders of child pornography (a notoriously computer-literate group) . . . would be able to use the source code [of law enforcement peer-to-peer software] to develop ways either to evade apprehension or to mislead authorities”). Thus, even if the defendant had articulated some logical and material connection between the information he seeks and this case—which he has not—his broad discovery request should still be denied.

defendant seeks is discoverable. (Doc. 31-4; Doc. 31-6). In this context, the defendant's judicial estoppel argument is entirely misplaced. *New Hampshire v. Maine*, 532 U.S. 742, 749 (2001) (noting that the rule is designed to prevent a party from prevailing in one phase of litigation and then relying on a contradictory argument in another phase).

3. The Defendant Is Not Entitled to the Remaining Information He Seeks Under *Brady* or its Progeny

While the defendant's motion is primarily a discovery request, he also frames as it as a request for *Brady* materials. "*Brady* is not a discovery rule, but a rule of fairness and minimum prosecutorial obligation." *Krauth*, 769 F.2d at 476 (citation and quotation marks omitted). "Under *Brady* and its progeny, prosecutors have a duty to disclose to the defense all material evidence favorable to the accused, including impeachment and exculpatory evidence." *United States v. Robinson*, 809 F.3d 991, 996 (8th Cir. 2016) (citations omitted). The Government has no duty under *Brady*, however, "to disclose evidence that is neutral, speculative, or inculpatory, or evidence that is available to the defense from other sources." *United States v. Pendleton*, 832 F.3d 934, 940 (8th Cir. 2016) (citation omitted). The defendant bears the burden of making a "preliminary showing that the requested information is exculpatory." *United States v. Roach*, 28 F.3d 729 (citing *Krauth*, 769 F.2d at 476).

Evidence is material for purposes of *Brady* "only if there is a reasonable probability that, had it been disclosed to the defense, the result of the proceeding would have been different"—that is, "a probability sufficient to undermine confidence in the outcome." *United States v. Conroy*, 424 F.3d 833, 837 (8th Cir. 2005). And while *Brady* and its progeny place an obligation upon a prosecutor "to disclose evidence known by police officers, even if not known by the prosecutor," *United States v. Tyndall*, 521 F.3d 877, 882 (8th Cir. 2008), that obligation only applies to officers "acting on the government's behalf *in the case*," *Kyles v. Whitley*, 514 U.S. 419, 437 (1995)

(emphasis added); *see also United States v. Merlino*, 349 F.3d 144, 154 (3rd Cir. 2003) (“Kyles cannot ‘be read as imposing a duty on the prosecutor’s office to learn of information possessed by other government agencies that have no involvement in the investigation or prosecution at issue.’” (quoting *United States v. Morris*, 80 F.3d 1151, 1169 (7th Cir. 1996)); *United States v. Locascio*, 6 F.3d 924, 949–50 (2d Cir. 1993) (same).

Applying these principles here, the defendant’s request for “all discovery related to, and underlying, an undated screen shot” reflecting that two other officers in Arkansas downloaded CSAM from the user of the defendant’s IP address and “all law enforcement reports and related discovery prepared by” those officers’ agencies should be denied. (Doc. 31 at 1). His request for this alleged *Brady* material is premised on a two-pronged argument, both parts of which fail. First, he asserts in conclusory fashion that the information he requests is exculpatory because he will find in it some unspecified material that he can use to impeach Special Agent Faulkner, pointing to Special Agent Faulkner’s testimony at the detention hearing regarding the timeline of HSI’s investigation and the fact that he did not mention the other officers.⁴ (Doc. 31 at 8). As explained above, however, *see supra* p. 7 n.2, Special Agent Faulkner’s testimony regarding HSI’s initiation of this investigation is entirely consistent with his other sworn statements and the events of this case. Further, Special Agent Faulkner did not “materially omit[]” the activities of the other officers from his testimony, as the defendant unfairly suggests. (Doc. 31 at 5). Indeed, the defendant

⁴ The defendant also claims that the information must be exculpatory because “there is no good reason” the United States would otherwise not produce it. (Doc. 31 at 8–9). This sort of circular reasoning turns the criminal discovery process on its head and could be used to justify unlimited discovery demands. It also falls well short of satisfying the defendant’s requirement under *Brady* to make a preliminary showing, based on some evidence, that the information he seeks is exculpatory and in the Government’s possession. And to be clear, as the United States has advised repeatedly, the material is not discoverable because it relates to investigators who are not involved with any part of this federal prosecution and who are not members of the prosecution team.

acknowledges that he does not even know what role these officers played in this investigation, *see Id.* at 1, and that is because they played none. Their activity is, by definition, not material to this case. For this reason alone, the defendant's motion should be denied.

The second part of the defendant's argument in support of his request for this alleged *Brady* material is that the United States must produce the requested information—which he incorrectly labels exculpatory—because the two other officers were acting on the United States' behalf in this case. (Doc. 31 at 9). This too is incorrect. Despite the defendant's repeated incantation, the two officers were not involved with the United States' federal investigation of the defendant and they did not provide the prosecution team with any materials. They certainly were not acting on behalf of the United States with respect to this case, as explained in more detail above, and the defendant's request for this alleged *Brady* material should therefore be denied.

III. CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court deny the defendant's Motion to Compel Discovery (Doc. 31).

Respectfully submitted,

By: */s/ Dustin Roberts*
Dustin Roberts
Assistant United States Attorney
Arkansas Bar No. 2005185
414 Parker Avenue
Fort Smith, AR 72901
Office: 479-249-9034

/s/ Carly Marshall
Carly Marshall
Assistant United States Attorney
Arkansas Bar No. 2012173
414 Parker Avenue
Fort Smith, AR 72901
Office: 479-249-9034

AND

/s/ William G. Clayman
William G. Clayman
D.C. Bar No. 1552464
Trial Attorney
Child Exploitation and Obscenity Section
U.S. Department of Justice
1301 New York Avenue NW
Washington, D.C. 20005
Telephone: 202-514-5780
Email: william.clayman@usdoj.gov

CERTIFICATE OF SERVICE

I, Dustin Roberts, Assistant United States Attorney for the Western District of Arkansas, hereby certify that on August 9, 2021, a true and correct copy of the foregoing pleading was electronically filed with the Clerk of Court using the CM/ECF System which will send notification of such filing to the following:

Justin Gelfand, Travis Story, Gregory Payne, Attorneys for the Defendant

/s/ Dustin Roberts _____
Assistant United States Attorney

ATTACHMENT C

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS

STATE OF ARKANSAS

:
:
:
:

ss. A F F I D A V I T

COUNTY OF WASHINGTON

Affidavit in Support of Application for Search Warrant

I, Gerald Faulkner, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI), currently assigned to the Assistant Special Agent in Charge Office in Fayetteville, Arkansas. I have been so employed with HSI since April 2009. As part of my daily duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, online enticement, transportation, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2251A, 2422(b), 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants and arrest warrants, a number of which involved child exploitation and/or child pornography offenses. This Affidavit is being submitted based on information from my own investigative efforts as well as information obtained from others who have investigated this matter and/or have personal knowledge of the facts herein.

GOVERNMENT
EXHIBIT

A

2. This Affidavit is being submitted in support of an application for a search warrant for the premises **Wholesale Motorcars located at 14969 Wildcat Creek Road, Springdale, Arkansas 72762** the "SUBJECT PREMISES". As such, it does not include all of the information known to me as part of this investigation, but only information sufficient to establish probable cause for the requested search warrant.

Statutory Authority

3. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors, which has been defined in Title 18 U.S.C. 2256, as an individual under 18 years of age.

a. Under 18 U.S.C. Section 2252(a)(1) (transportation), 2252(a)(2) (receipt and distribution), and 2252(a)(4)(B) and 2252A(a)(5)(B) (possession), it is a federal crime for any person to transport, distribute, receive, and possess child pornography, as that term is defined by federal law. Further under 18 U.S.C. Section 2253(a)(3), a person who is convicted of an offense under 18 U.S.C. Section 2252 or 2252A, shall forfeit to the United States such person's interest in any property, real or personal, used or intended to be used to commit or to promote the commission of such offense.

Computers and Child Pornography

4. Based upon my knowledge and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant

amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership-base/subscription-based websites to conduct business, allowing them to remain relatively anonymous.

5. In addition, based upon my own knowledge and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that the development of computers has also revolutionized the way in which those who seek out child pornography are able to obtain this material. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by those who seek to obtain access to child pornography in these ways.

6. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In

addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

7. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial Internet Service Providers (ISPs) which allow subscribers to dial a local number and connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

8. The Internet allows users, while still maintaining anonymity, to easily locate other individuals with similar interests in child pornography; and websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by business, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the recipient.

9. The computer's capability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as a "hard drive") used in home computers has grown tremendously with the last several years. Hard drives with the capacity of 160 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

10. It should be noted that Internet Protocol (IP) numbers are unique identifiers leased to Internet customers by their ISP's. Although IP numbers are capable of changing over time, only one (1) unique IP number can be assigned to a given customer's computer at any given time. Logs of these leased IP's (and their assigned customer accounts) are stored by ISP's routinely.

11. Your Affiant knows from his own experience and the training and experience of other law enforcement officers that Internet computers identify each other by an Internet Protocol or IP address. These IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead the law enforcement officer to a particular Internet service company and that company can typically identify the account that uses the address to access the Internet.

12. Law enforcement uses specialized "peer to peer" (P2P) software to locate computers offering to participate in the distribution of child pornography images and files over P2P sharing networks in Arkansas. Millions of computer users throughout the world use P2P file

sharing networks to share files containing music, graphics, movies and text. These networks have also become a popular way to download and distribute child pornography. Any computer user who can connect to the Internet can download P2P application software, which is typically free, and use it to share files through a P2P network.

13. The BitTorrent network is a very popular and publically available P2P file sharing network. Most computers that are part of this network are referred to as “peers” or “clients”. A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients.

14. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, uTorrent client program, and Vuze client program, among others. These client programs are publically available and typically free P2P client software programs that can be downloaded from the Internet.

15. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading.

16. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as “seeding”.

17. Files or sets of files are shared on the BitTorrent network via the use of “Torrents”. A “Torrent” is typically a small file that describes the file(s) to be shared. It is

important to note that “Torrent” files do not contain the actual file(s) to be shared, but information about the file(s) to be shared needed to accomplish a download.

18. The strength of a Peer to Peer Network is that it bases all of its file shares on the Secure Hash Algorithm (SHA1). This mathematical algorithm allows for the fingerprinting of files. Once you check a file with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that will be a fixed-length unique identifier for that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA1 is called secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.

19. This information includes things such as the name(s) of the file(s) being referenced in the “Torrent” and the “info hash” of the “Torrent”. The “info hash” is a SHA-1 hash value of the set of data describing the file(s) referenced in the “Torrent”. This set of data includes the SHA-1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The “info hash” of each “Torrent” uniquely identifies the “Torrent” file on the BitTorrent network. The “Torrent” file may also contain information on how to locate file(s) referenced in the “Torrent” by identifying “Trackers”.

20. “Trackers” are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the “Torrent” file. A “Tracker” is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the “Torrent”. “Trackers” do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of “Tracker(s)” on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a

particular "Torrent" file. There are many publically available servers on the Internet that provide BitTorrent tracker services.

21. In order to locate "Torrent" files of interest and download the files that they describe, a typical user will use keyword searches on Torrent indexing websites, examples of which include isohhunt.com and the piratebay.org. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate "Torrent" files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by "Torrent" files, only the "Torrent" files themselves.

22. Once a "Torrent" file is located on the website that meets a user's keyword search criteria, the user will download the "Torrent" file to their computer. The BitTorrent network client program on the user's computer will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file. It is again important to note that the actual file(s) referenced in the "Torrent" are actually obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent", to include the remote peers/clients Internet Protocol (IP) addresses.

23. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing website.

24. Based on the results of the keyword search, the user would then select a "Torrent" of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the "Torrent" file.

25. Utilizing "trackers" and other BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files.

26. Typically, once the BitTorrent network client has downloaded part of a file or files, it may immediately begin sharing the part of the file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 hash value of that piece which is described in the "Torrent" file.

27. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file or files, including the torrent file, will remain in that location until moved or deleted by the user.

28. Law Enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. To search the network for these known torrents can quickly identify targets in their jurisdiction.

29. Law Enforcement receives this information from "Trackers" about peers/clients on the BitTorrent network recently reporting that they are involved in sharing digital files of known or suspected child pornography, based on "info hash" SHA-1 hash values of torrents. These

torrents being searched for are those that have been previously identified by law enforcement as being associated with such files. There are BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

30. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes 1) the suspect client's IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the suspect client program; and 3) the BitTorrent network client program and version being utilized by the suspect computer. The law enforcement has the ability to log this information.

31. It should be noted, during the downloading and installation of the publically available uTorrent client program, the license agreement for the software states the following: "Automatic Uploading. uTorrent accelerates downloads by enabling your computer to grab pieces of files from other uTorrent or BitTorrent users simultaneously. Your use of the uTorrent software to download files will, in turn, enable other users to download pieces of those files from you, thereby maximizing download speeds for all users. In uTorrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users'

use of your network connection to download portions of such files from you. At any time, you may uninstall uTorrent through the Add/Remove Programs control panel utility.

32. In addition, you can control uTorrent in multiple ways through its user interface without affecting any files you have already downloaded thereby maximizing download speeds for all users. In uTorrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall uTorrent through the Add/Remove Programs control panel utility. In addition, you can control uTorrent in multiple ways through its user interface without affecting any files you have already downloaded.

33. Additionally, your Affiant knows that P2P software may display the Globally Unique Identifier (GUID) identification number of computers offering to share files on the network. A Globally Unique Identifier or GUID is a pseudo-random number used in software applications. This GUID number is produced when some P2P software applications are installed on a computer. While each generated GUID is not guaranteed to be unique, the total number of unique keys is so large that the probability of the same number being generated twice is very small. When comparing these GUIDs, your Affiant can quickly determine with a high degree of certainty that two different IP addresses that are associated with the same GUID are associated with the same computer.

Summary of Investigation to Date

34. In May 2019, a HSI Internet Crimes Against Children (ICAC) Task Force affiliate was conducting an online investigation on the BitTorrent Peer-to-Peer (P2P) file sharing network for offenders sharing child pornography. During the course of the online investigation, a connection was made between the HSI ICAC Task Force affiliate's investigative computer and a

computer/device running BitTorrent software from an IP Address of 167.224.196.113. In May 2019, two separate downloaded files were successfully obtained from IP Address 167.224.196.113. One of the downloaded files was a ".zip" folder containing approximately sixty-five (65) images and the other downloaded file was a single video. The HSI ICAC Task Force affiliate then viewed portions of the downloaded files which were determined to be consistent with child pornography. The device at IP Address 167.224.196.113 was the only IP Address which shared the contents for the files downloaded, and as such, the files were downloaded directly from this IP Address. The HSI Task Force affiliate then determined the IP Address was geo-located to Northwest Arkansas, at which time the lead information and downloads were forwarded to the HSI Assistant Special Agent in Charge Office in Fayetteville, Arkansas for further investigation.

35. In October 2019, your Affiant reviewed the two files successfully downloaded by the HSI ICAC affiliate computer from IP Address 167.224.196.113. Your Affiant more specifically described the files as follows:

(a) File Name: marissa.zip

This ".zip" folder contains approximately sixty-five (65) image files of a prepubescent female, many of which were consistent with child pornography. One file within the folder entitled 2203.jpg, is an image depicting a prepubescent female approximately seven (7) to nine (9) years of age lying on her back and using her hands to expose her vagina and anus.

(b) File Name: mov_0216.mp4

This video is approximately two minutes and eleven seconds in length and depicts two (2) prepubescent females approximately seven (7) to nine (9) years of age. The prepubescent

females are both completely naked laying on top of each other. A male subject is then seen penetrating one of the prepubescent female's vagina with his erect penis.

36. On October 15, 2019, your Affiant, utilizing ICAC software tools, conducted additional record checks of IP Address **167.224.196.113**. The search revealed that as of May 16, 2019, approximately ninety-three (93) files of investigative interest had been flagged as potential child exploitation material.

37. An Internet search on the origin of the IP Address **167.224.196.113** found it to be issued to the Internet service provider Ozarks Go. A federal summons was issued to Ozarks Go in reference to IP Address **167.224.196.113** for the specific dates and times the video and images of child pornography were successfully downloaded from the user. Documents received on or about October 7, 2019 from Ozarks Go identified the IP Address as being assigned to Joshua DUGGAR at 14993 Wildcat Creek Road in Springdale, Arkansas 72762. A connection or activation date of April 16, 2019 was listed for this account. Ozarks Go also provided a PO BOX number in Tontitown, Arkansas as an additional mailing address for DUGGAR. Law enforcement queries likewise revealed a 2004, R-Vision, Inc., model XMH motor home bearing Arkansas license plate OMJKD with a Vehicle Identification Number (VIN) ending in the last four digits 9129 was registered to DUGGAR and his wife at the same PO BOX number in Tontitown, Arkansas.

38. An additional federal summons was issued to Ozark Electric Cooperative in reference to address 14993 Wildcat Creek Road in Springdale, Arkansas 72762. Documents provided by Ozark Electric Cooperative on October 28, 2019 revealed an account service agreement assigned to DUGGAR, customer number 292144, for the service address of 14993

Wildcat Creek Road in Springdale, Arkansas 72762. A supplementary mailing address was also linked to the account at one and the same PO BOX number in Tontitown, Arkansas.

39. On October 31, 2019, contact was made with the residents of 14993 Wildcat Creek Road in Springdale, Arkansas 72762. During the encounter, HSI ICAC Special Agents and Task Force Officers determined that the residence had not been previously receiving internet services through Ozarks Go. However, per the residents of 14993 Wildcat Creek Road in Springdale, Arkansas, and based on the revealed subscriber information, they explained that DUGGAR did in fact own and operate a used car sale lot on the property adjacent to their residence. According to the home owner, he/she met with DUGGAR a few weeks prior to the law enforcement encounter and sold him a vehicle. While at the business, Wholesale Motorcars, the homeowner was informed the dealership has Internet serviced through Ozarks Go.

40. Based on the investigative findings, your Affiant contacted Ozarks Go and Ozarks Electric Cooperative who were able to determine that their internal system mapping of the Internet and electric services of the HSI subpoenaed subscribers did not properly differentiate the addresses in question. Ozarks Go and Ozarks Electric Cooperative representatives explained they utilized Washington County, Arkansas property records to identify the subpoenaed customer's address as opposed to physically determining the actual service sites. Further review by your Affiant showed Washington County, Arkansas online records currently showed only one residence located on approximately twenty-seven (27) acres of property with the listed address of 14993 Wildcat Creek Road in Springdale, Arkansas. According to the residents of 14993 Wildcat Creek Road in Springdale, Arkansas, encountered on October 31, 2019, half of the property on the approximate twenty-seven (27) acres was either sold or split years ago and the current public property records have not been updated to reflect the two separate lots. After the sale or split of the property,

Wholesale Motorcars was established and assigned or listed as a separate address. Your Affiant explained to Ozarks Go the investigative efforts made to clarify the correct subscriber address for internet services through IP Address 167.224.196.113. Representatives from Ozarks Go confirmed the subscriber address listed in their system and on the returned subpoenaed documents to HSI was in error and they believed the proper address should be reflected as 14969 Wildcat Creek Road Springdale, Arkansas 72762 (SUBJECT PREMISES) with the same registered subscriber of DUGGAR.

41. Additional Internet research of the car dealership revealed an online article published in November 2018 regarding the owner, DUGGAR, having alleged to operate the business, Wholesale Motorcars, without the proper permits. The article further explained, due to the lack of proper permits, the Washington County, Arkansas Fire Marshal addressed these issues in person with DUGGAR on multiple occasions.

42. On November 1, 2019, your Affiant contacted the Washington County, Arkansas Fire Marshal and requested documents related to his interactions with Wholesale Motorcars, its owner and their officially listed address. Shortly thereafter, your Affiant received and reviewed numerous documents provided by the Fire Marshal. A document entitled "Washington County Sheriff's Office Fire Marshal Division Inspection Form" revealed Wholesale Motorcars, with a listed "Owner or Manger" as being "Josh Dugger" was inspected by the department on July 11, 2018 at the physical location of 14969 Wildcat Creek Road Springdale, Arkansas 72762 (SUBJECT PREMISES). The Inspection Form was signed by DUGGAR on July 11, 2018 with a follow-up inspection scheduled in thirty days.

43. An additional document provided and reviewed by your Affiant from the Fire Marshal showed the Washington County, Arkansas Planning Board/Zoning Board of Adjustments

sent letters in October 2018 to neighbors of Wholesale Motorcars alerting to an upcoming public meeting to review the proposed "Conditional Use Permit" for DUGGAR to operate a business in the immediate area. An attached spreadsheet of recipients showed the same resident encountered by HSI ICAC Special Agents and Task Force Officers on October 31, 2019 was mailed one of these letters to their listed address of 14993 Wildcat Creek Road in Springdale, Arkansas 72762. This mailed document further supports the distinction between the two properties in question and the fact Ozarks Go mapping system of Internet and electric subscriber services did not properly differentiate between the two addresses.

44. On November 1, 2019, a HSI Task Force Officer, acting in an undercover capacity, arrived at Wholesale Motorcars located at the **SUBJECT PREMISES** and entered the business office to inquire about potentially purchasing a used vehicle from the dealership. Upon entering the office, the undercover HSI Task Force Officer was met by an unknown employee who identified himself as "Randy" and another employee who identified himself as "Josh". The undercover HSI Task Force Officer was able to positively identify "Josh" as being DUGGAR and further witnessed him to retrieve a believed Apple iPhone from his person with an unknown modeled laptop computer located on the desk. Verbal arrangements were made to possibly purchase a vehicle from the dealership at a later date and at the conclusion, the undercover HSI Task Force Officer departed the scene.

Conclusion

45. *Necessity of On-site and Off-site examinations of entire computers or storage media.* Based on my experience and the training and experience of other agents, many of the items sought in this Affidavit may be stored electronically. Based on my experience and consultation with computer forensic experts, I know that electronic files can be easily moved from computer or

electronic storage medium to another computer or medium. Therefore, electronic files downloaded to or created on one computer can be copied on or transferred to any other computer or storage medium at the same location. In addition, based on my experience, I know that searching computerized information for evidence of crime often requires special agents to seize most or all of a computer system's central processing unit (CPU), input/output peripheral devices, related software, documentation, and data security devices, including passwords, so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

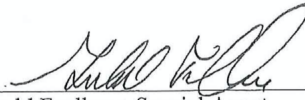
(a) Volume of evidence: Computer storage devices such as hard disks, diskettes, tapes and laser disks, can store the equivalent of thousands of pages of information. This sorting process can take up to several months to complete, depending on the volume of data stored. Therefore, it would also be impractical to attempt this type of data search on site.

(b) Technical requirements: Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional destruction (both from external sources and from destructive code embedded in the system such as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

46. Therefore, authorization is sought in this application to seize the items set forth in attachment "B" that are found on the premises to be searched, in order to examine those items for evidence. If it is determined that data has been seized that does not constitute evidence of the crimes detailed herein, the government will return said data within a reasonable time.

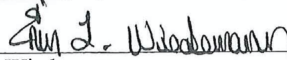
47. Based on my experience and the training and experience of other agents involved with this investigation, your Affiant knows that individuals involved in the sexual exploitation of children through child pornography almost always keep copies of their sexual explicit material. Among the reasons copies are maintained is because child pornography is illegal to openly purchase, and the most common method of acquiring it is by trading with other people with similar interests. It is also known that due to the inherent illegality of these sexually explicit materials, they are most often kept in a place considered secure, usually a residence, to avoid detection by law enforcement.

48. Based on the foregoing information, probable cause exists to believe there is located at **Wholesale Motorcars at 14969 Wildcat Creek Road, Springdale, Arkansas 72762**, the **SUBJECT PREMISES**, evidence of violations of Title 18, United States Code, Section 2522, et seq. Your Affiant prays upon his honorable court to issue a search warrant for the **SUBJECT PREMISES** for the items set forth in attachment "B" (which is attached hereto and incorporated herein by reference), that constitute evidence, fruits, and instrumentalities of violation of Title 18, United States Code, Section 2522, et seq.



Gerald Faulkner, Special Agent
Homeland Security Investigations

Affidavit subscribed and sworn to before me this 4th day of November, 2019



Erin L. Wiedemann
Chief United States Magistrate Judge