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

UNITED STATES OF AMERICA

v. **Criminal No. 5:21-CR-50014-001**

JOSHUA JAMES DUGGAR

UNITED STATES' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE AND REQUEST FOR *FRANKS* HEARING

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, and William G. Clayman, Trial Attorney for the United States Department of Justice, and for its Response in Opposition to the Defendant's Motion to Suppress and for a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978) (Doc. 37), states:

I. Summary of the Argument

John Adams once argued that "facts are stubborn things; and whatever may be our wishes…they cannot alter the state of facts and evidence." This admonishment is telling in the present case, as the defendant challenges the validity of a search warrant authorized by then-Chief U.S. Magistrate Judge Erin L. Wiedemann, and in so doing, directly asserts that the affiant of the warrant, Homeland Security Investigations (HIS) Special Agent (SA) Gerald Faulkner, intentionally mislead the magistrate. However, facts are stubborn things. A simple review of the affidavit at issue reveals that there was probable cause supporting the magistrate's issuance of the warrant. As for the defendant's claims that SA Faulkner misled the magistrate, these inflammatory, yet baseless claims fail owing to an examination of the facts, a faulty and undeveloped opinion by

the defense's expert, and a review of the applicable law. As such, the defendant's motion to Suppress and request for a *Franks* hearing should be denied, as it is utterly without merit.

II. The United States' Investigation

In the present case, the activities of the defendant, Joshua DUGGAR, first came to law enforcement's attention in May of 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 utilizing the Torrential Downpour program. "Torrential Downpour is a law enforcement software program configured to search the BitTorrent network for Internet Protocol ("IP") addresses associated with individuals offering to share or possess files known to law enforcement to contain images or videos of child pornography." *United States v. Hoeffener*, 950 F.3d 1037, 1040–41 (8th Cir. 2020). During her investigation, she observed that a user connected to the network from IP address 167.224.196.113 ("the target IP") was sharing child sexual abuse material (CSAM) over the network. Using the Torrential Downpour software, Det. Kalmer downloaded CSAM directly from this user. The downloaded files include:

- Mov_0216.mp4: 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

- Marissa.zip: A zip file downloaded at approximately 6:45 PM on May 15, 2019, that included 65 compete and viewable images depicting a prepubescent female.

After downloading these files, Det. Kalmer determined that the target IP address geolocated to Northwest Arkansas. She subsequently contacted SA Faulkner, who investigates federal child pornography offenses in Northwest Arkansas, to inquire if he would further investigate the user of the target IP address. After SA Faulkner advised that he would, Det. Kalmer notified the Internet Crimes Against Children ("ICAC") Administrator, Lenore Paladino, of the

downloads, informed her that she uploaded or logged the two (2) files containing CSAM in the ICAC Data System ("IDS"), and requested that Administrator Paladino give SA Faulkner access to said files to further the investigation. ICAC Administrator Paladino subsequently granted SA Faulkner access to the two (2) files downloaded by Det Kalmer.[1]

After receiving the lead from Det. Kalmer, SA Faulkner determined that the target IP was issued by an internet service provider (ISP) known as OzarksGo and requested subscriber information associated with the user's account. On or about October 7, 2019, in response to a federal summons, OzarksGo identified the subscriber associated with the target IP as JOSHUA DUGGAR, with a service address of 14993 Wildcat Creek Road, Springdale, Arkansas.

On October 29, 2019, HSI SA Howard Aycock applied for and obtained a federal warrant from then-Chief U.S. Magistrate Judge Wiedemann to search the premises at 14993 Wildcat Creek Road, Springdale, Arkansas. On or about October 31, 2019, HSI agents, intending to execute the search warrant, contacted the residents of 14993 Wildcat Creek Road, and were quickly able to confirm that the address provided to them by OzarksGo was in error. Specifically, OzarksGo subscriber JOSHUA DUGGAR did not and had never resided at that address. Additionally, said residence did not currently, nor did it previously, receive internet service through OzarksGo. The residents of 14993 Wildcat Creek informed law enforcement that DUGGAR operated a car lot on the adjacent property and that the car lot had OzarksGo internet service. Consequently, law enforcement retuned said warrant unexecuted to Magistrate Judge Wiedemann. (See Government's (Gov.) Exhibit (Ex.) 1-Return documented as unexecuted).

[1] Both files containing CSAM that Det. Kalmer logged in the IDS system, of which SA Faulkner later described in the affidavit at issue, remain in the IDS system to date.

After confirming that DUGGAR factually operated a car lot on the adjacent property and confirming with OzarksGo the correct address related to the subscriber associated with the target IP address at issue, SA Gerald Faulkner sought a federal search warrant for DUGGAR's car lot at 14969 Wildcat Creek Road Springdale, Arkansas from Magistrate Judge Wiedemann. (See Gov. Ex. 2).

In the affidavit in support of the search warrant, SA Faulkner states, as relevant here, that "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 65 images and the other downloaded file was a single video." (Gov. Ex. 2, Affidavit ¶ 34). SA Faulkner then explains that in October of 2019, he "reviewed the two files successfully downloaded by [Det. Kalmer] from IP Address 167.224.196.113" and provided the following descriptions:

a) File Name: marissa.zip

> This zip folder contains approximately sixty-five (65) image files of a prepubescent female, many of which are 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.

Id. at ¶ 35. Additionally, SA Faulkner states in the search warrant affidavit that approximately ninety-three (93) files of interest connected to the target IP address had been flagged by law enforcement as potential child exploitation material. *Id*. at ¶ 36. As for referencing the initial search

warrant, SA Faulkner details for Magistrate Judge Wiedemann, who had approved the warrant for the mistaken residential address just days prior, the investigative steps law enforcement underwent to conclude that the correct service address corresponding to IP address from which Det. Kalmer downloaded CSAM files was DUGGAR's car lot, located at 14969 Wildcat Creek, in Springdale, Arkansas. These additional steps are outlined in paragraphs 39 through 44 of the affidavit and include: speaking with the residents of the mistaken address who indicated that the overall property was divided years back and that DUGGAR operated a car lot on the adjacent land, confirming that DUGGAR factually operated a car dealership by sending an undercover (UC) officer into the car lot itself, and confirming that a Washington County Fire Marshal conducted an inspection of DUGGAR's car lot at the address listed in the warrant. Of note, SA Faulkner presented this issue to OzarksGo and a representative thereof informed SA Faulkner that the residential address initially produced by their system was in error and the true address corresponding to the internet service at issue was 14969 Wildcat Creek.

On November 4, 2019, Magistrate Judge Wiedemann issued the warrant to search the defendant's car lot. At approximately 3:00 p.m. on November 8, 2019, law enforcement executed the warrant. In so doing, agents encountered the defendant and two other men standing outside on the car lot. Inside the small building on the lot, which operated as the business's main office, law enforcement located a HP desktop computer with a desktop background depicting DUGGAR and his family. Law enforcement also seized, as relevant here, DUGGAR's cellular phone, an Apple iPhone 11, and his laptop, a MacBook. DUGGAR was interviewed on scene and declined to provide a password to either his iPhone or MacBook.

That same month, November of 2019, HSI Computer Forensic Analyst (CFA) Marshall Kennedy created forensic copies of all three (3) devices seized from the car lot. All subsequent

forensic examinations conducted by HSI were from the forensic copies of the above identified devices. Additionally, forensic copies of the hard drive contained in the HP computer and DUGGAR's iPhone were later sent to the Department of Justice High Technology Investigative Unit (HTIU) for further analysis.

On or about November 22, 2019, CFA Kennedy created a forensic image of the hard drive contained in the HP computer, and thereafter all law enforcement's processing and analysis were conducted off the forensic image. CFA Kennedy completed his analysis and submitted a forensic report on or about June 24, 2020. In October of 2020, CFA Kennedy provided a forensic image of the HP computer to HTIU. In so doing, CFA Kennedy made the forensic image he sent to HTIU by duplicating his own forensic copy, as opposed to reprocessing DUGGAR's actual devices. HTIU Digital Investigative Analyst (DIA) Brad Gordon submitted his forensic report in November of 2020 and supplemented said report in February of 2021.

Both HSI's and HTIU's examinations revealed that an Ubuntu Linux operating system had been installed on the device on May 13, 2019. The Linux operating system created a password-protected partition on the device's hard drive separate from the original Windows operating system that came with the device. The password to access the Windows operating system on the HP Desktop is "joshuajjd," while the password to access the Linux partition is "*****1988."[2] Overall, both forensic examinations revealed that the Tor browser and, separately, the Bit-torrent client "uTorrent" had been installed on the Linux partition on or about May 13, 2019, and May 14, 2019, respectively. Thereafter the forensic evidence supports that both programs were utilized to

[2] 1988 is DUGGAR's birthyear. The full password is intentionally redacted herein.

download and view CSAM.[3] Finally, forensic evidence supports that the user of the HP computer deleted the images of CSAM from the device.

The MacBook was likewise examined by CFA Kennedy. A forensic image of the hard drive contained therein was created by CFA Kennedy on or about November 12, 2019. Thereafter, all review and analysis were conducted on the forensic image of the hard drive. From the forensic image of the MacBook, law enforcement determined that DUGGAR had backed up or synced his iPhone with said device. On the MacBook itself, law enforcement located numerous pictures and text messages that place DUGGAR at the car lot while CSAM was downloaded, accessed, and viewed on the HP computer. This evidence was all memorialized in a Report of Investigation (ROI) submitted by SA Faulkner in April of 2020. Additionally, HSI discovered during its examination that DUGGAR used the password "*****1988," or close variations, for multiple online accounts, including his bank account and social media accounts.

The iPhone 11 was forensically processed by CFA Kennedy. Because DUGGAR did not provide the password to his iPhone, law enforcement was only able to achieve a partial extraction, which was obtained on or about November 9, 2019. In March of 2021, the digital information, or extraction, pulled from DUGGAR's iPhone in November of 2019 was provided to HTIU. Both examinations again revealed the same images and text messages consistent with what was located on DUGGAR's MacBook. Both examinations likewise revealed where DUGGAR used the "*****1988" password for numerous personal online accounts.

[3] Of note, both forensic examiners located images and forensic evidence showing that the "marissa.zip" file referenced in the warrant was factually downloaded via the Bit-Torrent peer-to peer-network on May 15, 2019. Defense expert Bush was provided access to a forensic copy of the HP computer itself that contains said files prior to submitting her affidavit in which she claims the images "allegedly possessed by the remote client were in such an incomplete state that no user" could view the images. The existence of these images is likewise memorialized in the forensic reports provided to the defense in discovery.

III. Procedural Background and Relevant Case History

In April of 2021, a Grand Jury sitting in the Western District of Arkansas 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 or about August 19, 2021, the defendant caused to be filed numerous motions to dismiss and/or suppress, including the present motion. (see Docs. 36 – 40).

IV. Legal Analysis of Evidence Suppression Issues

A. The BitTorrent Network and Torrential Downpour

For his first argument, the defendant claims the warrant executed on the defendant's car lot leading to the discovery of digital evidence underpinning his current federal child pornography charges should be invalidated and all evidence should be suppressed because "the Government used a law enforcement software tool that acted more like a GPS tracking device than a BitTorrent platform" in this case. Doc. 37, p. 10. Despite the defendant's crude attempt to equate this program to GPS tracking and thereby invoke an analysis under an arguably more stringent legal fact pattern, the Eighth Circuit has upheld the use of similar peer-to-peer programs, as well as this specific Torrential Downpour program, in establishing probable cause supporting a search warrant. (See *United States v. Hoeffener*, 950 F.3d 1037 (8th Cir. 2020). Moreover, the defendant does not have a subjective expectation of privacy in an IP address, regardless of how many times law enforcement detects its involvement in the distribution of CSAM. (See *United States v. Jean*, 207 F. Supp. 3d 920, 932 (W.D. Ark. 2016), aff'd, 891 F.3d 712 (8th Cir. 2018)(citing *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010)). As such, perhaps a more apt analogy in the present

case would compare DUGGAR's use of the BitTorrent network to an individual who leaves incriminating evidence in his garbage at the curb for pickup. Any member of the public, including law enforcement, can have unlimited access to the discarded contents of the trash as long as it sits on a publicly accessible street. And so is true at present, that anyone, including law enforcement, could have connected to DUGGAR's device endless times to download the CSAM files that DUGGAR made public over the internet.

B. Current Case Law Regarding Searches on Similar Peer-to-Peer Networks

In summary, the defendant contends that law enforcement's use of Torrential Downpour on the BitTorrent peer-to-peer network required a warrant because the program repeatedly attempted to complete its download of the "marissa.zip" file from the defendant's IP address.[4] Of course, nothing about this argument is legally sufficient to warrant suppression—its very premise is simply the defendant's own *ipse dixit* and is totally unsupported by any legal authority. And that is because, the Torrential Downpour program gathered nothing more then what DUGGAR was offering to strangers over the same network-his IP address and the file he was sharing. And while the defendant may analogize otherwise, BitTorrent remains a peer-to-peer network, like other peer-to-peer networks in that its purpose is to permit users to download files that other users are sharing and making available over the program.

As noted above, the Eighth Circuit Court of Appeals has specifically addressed law enforcement's use of the Torrential Downpour program. In *United States v. Hoeffene*r, 950 F.3d 1037 (8th Cir. 2020), the Appellate court held:

> … Torrential Downpour searches for download candidates in the same way that any public user of the BitTorrent network searches, and it only searches for information that a user had already made public by the use of the uTorrent software.

[4] The defendant does not claim that Torrential Downpour program errored at all when downloading the "Mov_0216MP4" file and that file alone establishes probable cause.

> A defendant has no legitimate expectation of privacy in files made available to the public through peer-to-peer file-sharing networks. Hoeffener's attempt to distinguish BitTorrent software from other peer-to-peer programs does not alter the fact that he allowed public access to the files on his computer. The district court did not err in denying his motion to suppress evidence…

United States v. Hoeffener, 950 F.3d 1037, 1044 (8th Cir. 2020)(internal citations omitted). Moreover, the Eighth Circuit, this year, further upheld and clarified the holding in *Hoeffener* in stating "[w]e now hold explicitly what was implicit in *Hoeffener*: That nothing in *Carpenter*, *Riley*, or *Jones* calls into question our oft-repeated observation that a defendant has no reasonable expectation of privacy in materials he shares on a public peer-to-peer network. *United States v. Shipton*, 5 F.4th 933, 936 (8th Cir. 2021). Noteworthy given the current analogy advanced by DUGGAR that Torrential Downpour gathered information akin to GPS data, the Appellate Court in *Shipton* stated:

> Shipton decries what he calls the government's "dragnet surveillance" through programs like RoundUp eMule and the CRC's maintenance of vast databases of hash values connecting known or suspected child pornography to IP addresses where those files were offered for sharing, invoking images of an Orwellian dystopia. His concerns are overstated. These programs and databases contain only information that users of peer-to-peer networks have deliberately chosen not to keep private. And as the magistrate judge here explained in an admirably thorough opinion, though this "surveillance" may certainly cast a wide net, most of the information gathered pertains to people other than Shipton. Unlike *Jones*, where officers tracked a person's car for nearly a month with the help of a GPS device, the information gathered here was relatively minimal. In *Carpenter*, the Court was similarly concerned about the detailed information that a week's worth of cell-site location information generated from a mobile phone revealed about a particular person's everyday movements. Likewise, the concern in *Riley* was about the depth of detail that a person's mobile phone could reveal about him. In sum, we reject Shipton's contention that he had a reasonable expectation of privacy here.

United States v. Shipton, 5 F.4th 933, 936 (8th Cir. 2021).

While *Hoeffener* specifically addresses law enforcement's use of the Torrential Downpour program, its holding is in line with a long standing and universally accepted notion that individuals do not retain a reasonable expectation of privacy for information shared and subsequently collected

by law enforcement over peer-to-peer networks. In *United States v. Stults*, 575 F.3d 834 (8th Cir. 2009), the Court also addressed the issue of a person's expectation of privacy on peer-to-peer networks. In so doing, the Eighth Circuit followed several other federal courts and found that an individual does not have a reasonable expectation of privacy on a peer-to-peer file sharing network. Specifically the Court found:

> Several federal courts have rejected the argument that an individual has a reasonable expectation of privacy in his or her personal computer when file-sharing software, such as LimeWire, is installed. *See, e.g., United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008) (holding that the defendant lacked a reasonable expectation of privacy in the downloaded files stored on his computer, meaning that an agent's use of a file-sharing software program to access child pornography files on the computer did not violate the defendant's Fourth Amendment rights); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008) (holding that defendant had no expectation of privacy in government's acquisition of his subscriber information, including his IP address and name from third-party service providers, where the defendant voluntarily transmitted such information to Internet providers and enabled P2P file sharing on his computer, which permitted anyone with Internet access the ability to enter his computer and access certain folders); *United States v. Barrows*, 481 F.3d 1246, 1249 (10th Cir. 2007) ("[The defendant] claims that he invited no one to use his computer and therefore expected its contents to remain private. Yet he surely contemplated at least some third-party access: he knowingly networked his machine to the city computer for the express purpose of sharing files."); *United States v. Brese*, No. CR–08–52–D, 2008 WL 1376269 (W.D.Okla. April 9, 2008) (unpublished) ("The Court finds that, notwithstanding any subjective expectation that Defendant may have had in the privacy of his computer, it was not reasonable for him to expect privacy in files that were accessible to anyone else with LimeWire (or compatible) software and an internet connection."); *United States v. Borowy*, 577 F.Supp.2d 1133, 1136 (D.Nev.2008) ("In this case, [the defendant] did not have a legitimate expectation of privacy in files he made available to others using P2P software."). *Id.* at 842-43

The Sixth Circuit has likewise held in *United States v. Conner*, 521 F. App'x. 493 (6th Cir. 2013)(unpublished) that a user of a file-sharing program does not have a legitimate expectation of privacy. The Court in *Conner* further reasoned that sharing files on peer-to-peer networks is different from sending an email or a letter, explaining:

> Conner argues that under *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (*en banc*), third-party access to information on one's computer is consistent with a

> reasonable expectation of privacy in that information. In *Warshak*, we agreed that the government could not compel a commercial ISP to turn over the contents of a subscriber's e-mails without a warrant because subscribers "enjoy a reasonable expectation of privacy in the contents of emails," even though an ISP has the ability to view the contents of e-mail prior to delivery. 631 F.3d at 288. In the context of e-mail, ISPs are "the functional equivalent of a post office or a telephone company," and like an ISP, both of these entities have the ability to intrude on the contents of messages in the course of delivering them to their intended recipients. *Id.* at 286. Since the right or ability of third parties to intrude on phone calls and letters has not been deemed sufficient to defeat a reasonable expectation of privacy in those modes of communication, we agreed that "it would defy common sense to afford emails lesser Fourth Amendment protection" than telephone calls or letters. *Id.* at 285–86.
>
> *Warshak* does not control this case because peer-to-peer file sharing is different in kind from e-mail, letters, and telephone calls. Unlike these forms of communication, in which third parties have incidental access to the content of messages, computer programs like LimeWire are expressly designed to make files on a computer available for download by the public, including law enforcement. Peer-to-peer software users are not mere intermediaries, but the intended recipients of these files. Public exposure of information in this manner defeats an objectively reasonable expectation of privacy under the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *see also California v. Greenwood*, 486 U.S. 35, 40–41, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988) (finding no reasonable expectation of privacy in "plastic garbage bags left on or at the side of a public street," which are accessible by "members of the public" and left on the curb "for the express purpose of conveying [them] to a third party, the trash collector").

The current case law around the country does not support the defendant's position. Based on the above stated law, it is clear that: 1) individuals do not have a reasonable expectation of privacy on peer-to-peer file sharing networks; and 2) law enforcement can use specialized software to locate child pornography files and associated information being shared on peer-to-peer networks without violating any individual's privacy rights.

Lastly, even assuming *arguendo* some legitimacy to the defendant's arguments, the exclusionary rule, which prohibits the introduction of evidence during a criminal trial that was obtained in violation of a defendant's constitutional rights, is not constitutionally required, but instead is a "judicially created means of deterring illegal searches and seizures." *Penn. Bd. of Prob.*

& Parole v. Scott, 524 U.S. 357 (1998). It is applied "only where its deterrence benefits outweigh its substantial social costs." *Id.* (internal quotation marks omitted). Suppression of evidence through the exclusionary rule "has always been [a] last resort, not [a] first impulse." *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). At present, use of the exclusionary rule would not be supported.

C. Defendant Does Not Have a Reasonable Expectation of Privacy in his IP Address nor Files that He Shared with Third Parties on a Peer-to-Peer Network.

A defendant who is seeking to suppress evidence from a search must demonstrate that he had a "legitimate expectation of privacy" in the place searched. *United States v. Hamilton*, 538 F.3d 162, 167 (2d Cir. 2008). This inquiry involves the court to ask two separate questions. First, the court must determine whether the individual had a subjective expectation of privacy. Second, the court must determine whether that expectation of privacy is one that society accepts as reasonable. *Katz v. United States*, 389 U.S. 347, 361 (1967). The Supreme Court developed a bright-line application of the reasonable-expectation-of-privacy test that is particularly relevant here. In what has come to be known as the "third-party doctrine," the Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties ... even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979)(citing *United States v. Miller*, 425 U.S. 435, 442-44 (1976)).

The defendant at present cites in support of his GPS analogy to *United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017), *United States v. Jean*, 891 F.3d 712, 715 (8th Cir. 2018) and, to some extent, *Riley v. California, 573 U.S. 373* (2014). However, these cases all involved law enforcement searches of non-publicly accessible information on electronic devices, either by

utilizing a program to send a computer code/virus to defeat certain security or by physically searching a device without a warrant. These cases are simply not factually, legally, or even technologically, comparable to the instant. Instead, in this case, the defendant is on the internet, a publicly available space, making images of child pornography available to strangers over a peer-to-peer network. The tool used by law enforcement to download this content is not invading a non-public space on the defendant's computer. Rather, it's simply downloading the information that the defendant is voluntarily sharing with the public. And while it might benefit the defense to equate this gathering activity to GPS surveillance, no such non-public information was obtained in this case. Regardless of how many times this automated program attempted to download publicly accessible files, nothing more was garnered than what was made publicly available by DUGGAR himself.

As such, law enforcement's use of Torrential Downpour in this case did not constitute an illegal search and seizure, and the defendant's motion to suppress on this basis should be denied.

D. The Search Warrant was supported by Probable Cause and was Timely Obtained and Executed.

For his next argument, the defendant claims the search warrant at issue was not supported by probable cause because there "was no reason for the magistrate judge to conclude that evidence of child pornography would be found at a business (not a residence) simply because an unknown device allegedly contained two files approximately six months earlier… (Doc. 37, p. 13). However, the defendant fails to cite any authority for this contention. Instead, he simply cites cases that affirm residential warrants based off similar probable cause and opines that "[t]he same simply cannot be true for a business like a used car dealership that caters to the general public." *Id*.

However, the length of delay which could make information stale for purposes of obtaining a warrant "depends upon the particular facts of the case, including the nature of the

criminal activity and the type of evidence sought." *United States v. Allen*, 625 F.3d 830, 842 (5th Cir. 2010); *see also United States v. Vosburgh*, 602 F.3d 512, 528-29 (3d Cir. 2010) ("[S]taleness is not a matter of mechanically counting days."). "Courts are more tolerant of dated allegations if the evidence sought is of the sort that can reasonably be expected to be kept for long periods of time in the place to be searched." *United States v. Kleinkauf*, 861 F.2d 818, 823 (5th Cir. 1988).

The Eighth Circuit, in accordance with nearly every other circuit, has recognized the unique nature of child pornography crimes when conducting a staleness inquiry, upholding a warrant well beyond a six (6) month delay relating to child pornography offenses. *United States v. Lemon*, 590 F.3d 612 (8th Cir. 2010) (affirming search warrant in child pornography case where evidence supporting the warrant was 18 months old). Unlike other illegal contraband, child pornography is typically retained by its beholder for a prolonged, if not indefinite, period of time. *Id.* at 842-43; *United States v. Burkhart*, 602 F.3d 1202, 1206 (10th Cir. 2010) ("This court has repeatedly endorsed the view that possessors of child pornography are likely to hoard their materials and maintain them for significant periods of time."); *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008) (finding considerable support for position that "customers of child pornography sites do not quickly dispose of their cache"); *United States v. Vosburgh*, 602 F.3d 512, 528-29 (3d Cir. 2010) ("[P]ersons with an interest in child pornography tend to hoard their materials and retain them for a long time.")

Significantly, courts have also recognized the fact that a trained forensic examiner can recover files from a computer, even when they have been deleted by the user. *E.g., United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006) (("Having paid for multi-month access to a child pornography site, Gourde was also stuck with the near certainty that his computer would contain evidence of a crime had he received or downloaded images in violation of § 2252. Thanks to the

long memory of computers, any evidence of a crime was almost certainly still on his computer, even if he had tried to delete the images. FBI computer experts, cited in the affidavit, stated that 'even if ... graphic image files [ ] have been deleted ... these files can easily be restored.' In other words, his computer would contain at least the digital footprint of the images."); *United States v. Lamb*, 945 F. Supp. 441, 461 (N.D.N.Y. 1996) ("The nature and characteristics of computer storage systems leads the court to believe that five and a half months is not so long that one would expect a computer file to be erased."); *United States v. Payne*, 519 F. Supp. 2d 466, 477-78 (D.N.J. 2007) (four months); *United States v. Toups*, 2007 WL 433562 (M.D. Ala. February 6, 2007) ("Further bolstering the conclusion that the staleness calculation is unique when it comes to cases of Internet child pornography is the images and videos stored on a computer are not easily eliminated from a computer's hard drive. The mere deletion of a particular file does not necessarily mean that the file cannot later be retrieved."). *See, e.g., United States v. Eberle*, No. CRIM. 05-26, 2006 WL 1705143, at *1 (W.D. Pa. June 15, 2006) (noting that even when a computer has been 'wiped,' where 'all files and data associated with a prior user from a hard drive [are deleted],' the data may still be retrieved through forensic procedures); *United States v. Fazio*, 1:05CR00014ERW(LMB), 2006 WL 1307614, at *9 (E.D.Mo. May 9, 2006) ('Even when ... files have been 'deleted,' they are not really permanently removed from the computer but can be recovered months or years later.'); *United States v. Wiser-Amos*, 2007 WL 2669377 (W.D. Ky. September 7, 2007) (seven months).

In *United States v. Vosburgh*, 602 F.3d 512 (3d Cir. 2010), the court upheld a four-month gap, but wrote the following:

> We do not hold, of course, that information concerning child pornography crimes can never grow stale. We observe only that information concerning such crimes has a relatively long shelf life. It has not been, and should not be, quickly deemed stale. See, *e.g., Shields*, 458 F.3d at 279 n. 7. *See also United States v. Paull*, 551 F.3d

516, 522 (6th Cir.2009) (noting that the same time limitations that have been applied to more fleeting crimes do not control the staleness inquiry for child pornography). This is especially true where, as here, the crime in question is accomplished through the use of a computer. As the Ninth Circuit observed in one child pornography case, computers have "long memor[ies]." *United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir.2006) (*en banc*); *see also United States v. Frechette*, 583 F.3d 374, 379 (6th Cir.2009) ("Digital images of child pornography can be easily duplicated and ... even if they are sold or traded .... have an infinite life span."). Images stored on computers can be retained almost indefinitely, and forensic examiners can often uncover evidence of possession or attempted possession long after the crime has been completed. See, *e.g.*, *Gourde*, 440 F.3d at 1071 (crediting statement in affidavit that FBI computer experts can resurrect files from a hard drive even after they have been deleted). The staleness inquiry requires us to consider the "type of evidence" at issue, *Zimmerman*, 277 F.3d at 434, and we think it obvious that the type of evidence agents sought from Vosburgh's apartment—computers and/or computer equipment—is not the type of evidence that rapidly dissipates or degrades. Nor is it the type of property that is usually quickly or continuously discarded. *Cf. United States v. Ritter*, 416 F.3d 256, 270-71 (3d Cir.2005) (Smith, J., concurring in the judgment) (discussing the relevance to staleness of the nature of the evidence and how quickly it might reasonably be expected to be discarded). Therefore, the passage of weeks or months here is less important than it might be in a case involving more fungible or ephemeral evidence, such as small quantities of drugs or stolen music. *See id.*

The magistrate's task was to make a practical, commonsense decision as to whether there was a fair probability that evidence of criminal activity—including possession or even attempted possession of child pornography—would be found in Vosburgh's apartment four months after he attempted to access the Link. On the facts before us, and in light of our precedents, we agree that the magistrate had a substantial basis for concluding that there was. Our decision fits comfortably within the body of case law concerning staleness in the context of child pornography. *See, e.g.*, *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir.2008) (rejecting defendant's argument that three-year gap between date of download and warrant application rendered information stale, in light of testimony from the "government's knowledgeable witness" that child pornography collectors "do not quickly dispose of their cache"); *United States v. Irving*, 452 F.3d 110, 125 (2d Cir.2006) (holding that twenty-two month old information in affidavit in support of warrant to search for child pornography was not stale); *United States v. Lemon*, 590 F.3d 612, 615-16 (8th Cir.2010) (upholding probable cause determination despite eighteen-month gap between the warrant application and the incident described in the affidavit that suggested possession of child pornography); *United States v. Lacy*, 119 F.3d 742, 745 (9th Cir.1997) (rejecting staleness claim in child pornography case involving ten-month gap); *United States v. Terry*, 522 F.3d 645, 650 n. 2 (6th Cir.2008) (upholding probable cause in child pornography case involving a five-month gap).

Vosburgh, 602 F.3d at 529-30. In *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012), the court similarly held that a seven-month delay did not make the probable cause stale. More importantly, the Court's opinion recognizes that given computer forensic abilities, it is unlikely that probable cause to search a computer will ever be stale.

> "Staleness" is highly relevant to the legality of a search for a perishable or consumable object, like cocaine, but rarely relevant when it is a computer file. Computers and computer equipment are "not the type of evidence that rapidly dissipates or degrades." *United States v. Vosburgh*, 602 F.3d 512, 529 (3d Cir.2010). Because of overwriting, it is *possible* that the deleted file will no longer be recoverable from the computer's hard drive. And it is also *possible* that the computer will have been sold or physically destroyed. And the longer the interval between the uploading of the material sought as evidence and the search of the computer, the greater these possibilities. But rarely will they be so probable as to destroy probable cause to believe that a search of the computer will turn up the evidence sought; for probable cause is far short of certainty—it "requires only a probability or substantial chance of criminal activity, not an actual showing of such activity," *Illinois v. Gates*, 462 U.S. 213, 244 n. 13, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983), and not a probability that exceeds 50 percent ("more likely than not"), either. *Hanson v. Dane County*, 608 F.3d 335, 338 (7th Cir. 2010).

Seiver, 692 F.3d at 777.

In a misguided attempt to differentiate the case law applicable to staleness considerations regarding child pornography investigations, the defendant again simply claims based on his own opinion without citing legal authority that the same considerations for child pornography investigations that target residences do not hold true for a business. However, this position simply overlooks both the collecting and digital retention considerations identified in case law justifying extended search timeframes in child pornography cases.

Factually, at present, Magistrate Judge Wiedemann was informed via the affidavit that: 1) the evidence sought was digital in nature and based on digital images of images of child pornography downloaded from a peer-to-peer network, 2) as of May of 2019, ICAC software flagged "approximately ninety-three (93) files of investigative interest … as potential child

exploitation material" connected to the same IP address tied to the defendant's car lot, 3) in May of 2019, law enforcement downloaded two (2) separate files containing CSAM from an IP address connected to the car lot, 4) that "individuals involved in the sexual exploitation of children through child pornography almost always keep copies of their sexual exploitation material…because child pornography is illegal to openly purchase, and the most common method of acquiring it is by trading with other people of similar interests" Gov. Ex. 2, ¶ 47, 5- the defendant's small business consisted of an unpaved parking lot and two small, shed-like buildings *Id*., Attachment A., and 6) the premises were occupied by DUGGAR himself, and only one other employee (as opposed to many people being around) in November of 2019. Gov Ex. 2, Affidavit ¶ 44. As such, the magistrate judge was aware that digital images of child pornography, capable of being forensically located even if deleted or moved, were downloaded at a remote car lot. Additionally, the Magistrate was aware that law enforcement had flagged numerous images of similar nature being associated with this offending IP address as of May 16, 2019.

And to address the defendant's concern that collectors like to "hoard such images in a secure, private environment such as computers and electronic or digital media in their *homes*," the same logic applies with equal force with respect to a small, out-of-the way business. While it is true that most people find the privacy of their own residence more suited to downloading pornography, including child pornography, that is not the only place that individuals find the privacy to engage in such conduct. There are many cases in which offenders engage in such conduct at work. *See United States v. Pawlak*, 935 F.3d 337, 342 (5th Cir. 2019) (describing individual who used work computer to download and view child pornography); *United States v. Pruitt*, 638 F.3d 763, 765 (11th Cir. 2011) (describing deputy sheriff who used work computer

to search of child pornography); *United States v. Bailey*, 377 F. Supp. 2d 268, 269 (D. Me. 2005) (describing teacher who viewed and stored child sexual abuse material on his work computer). Indeed, if anything, it is much more probable that an employee at a remote car lot—or perhaps the owner of such a business, like DUGGAR—would utilize the business's internet service to download CSAM than a transient customer. In fact, it defies common sense to think that a customer would travel to a remote car lot, connect to that business's internet, which may or may not be password protected, while hoping to go undetected by car lot employees or security cameras, in order to *privately* download illegal images of child pornography. Regardless, such considerations do not touch on staleness, but rather the sufficiency of the probable cause available to the issuing magistrate. And at present, the magistrate judge was fully aware that the target address was that of DUGGAR's car lot and had ample basis to conclude the warrant was supported by probable cause. "When a search is authorized by a warrant, deference is owed to the issuing judge's conclusion that there is probable cause. Courts should defer to the issuing judge's initial probable cause finding if there is substantial evidence in the record that supports his decision." *United States v. Carroll*, 750 F.3d 700, 703–04 (7th Cir. 2014) (internal quotations omitted).

Given the state of the law, as well as the facts and circumstances in the present case, it is clear that the information contained in affidavits, that was presented to Magistrate Judge Erin Wiedemann, was not stale, and established probable cause. Therefore, any items recovered pursuant to these search warrants should not be suppressed.

E. The Warrant Does Not Contain False Statements or Material Omissions

Next, the defendant argues the evidence seized from his car lot should be suppressed on the grounds that the search warrant lacked probable cause due to the inclusion of a false statement

by the affiant—namely, SA Faulkner's statement that he reviewed the 65 images contained in the "marissa.zip" file downloaded from the user of the defendant's IP address—and, secondly, as a result of certain omissions pertaining to Det. Kalmer's use of the Torrential Downpour program and/or the BitTorrent network generally.

With respect to the accusation that SA Faulkner included a false statement in his affidavit, this claim is simply not supported in fact, technology, nor law. Factually, the "marissa.zip" file, containing sixty-five (65) viewable images as described in the affidavit was uploaded to *and remains* on the IDS system. In fact, these sixty-five (65) images were shown to DUGGAR's defense counsel at the HSI facility in Fayetteville earlier this year.[5] (see Gov. Ex. 3-Email). With respect to Michelle Bush's opinion, she mistakenly asserts that a Zip file header is contained in Piece "0" of a Zip file, when it is actually contained in the last piece, piece "65" in this instance, which was successfully downloaded by Det. Kalmer. Ms. Bush might have resolved the deficiencies in her mistaken opinion by simply reviewing of the downloaded file itself, instead of concluding such without physically verifying or examining the "marrissa.zip" images presented to defense counsel. And legally, the defendant fails to satisfy the basic requirements to justify a *Franks* hearing. His accusation that SA Faulkner knowingly and intentionally included a false statement in the affidavit in support of the search warrant is nothing more than an unsupported and uninformed allegation. With respect to the alleged omissions, defense counsel does nothing more

[5] While the Government can theorize why the defendant would refuse to believe that the images shown to the defense are the same images that Det. Kalmer downloaded from the user of the defendant's IP address and uploaded to IDS, the fact that these images were displayed to the defense should have, at the very least, prompted a greater inquiry on the part of the defendant before moving this Court to suppress all evidence obtained during the search of his business based on the erroneous claim that SA Faulkner could not have reviewed those same images. At a minimum, the defense could have requested that these images be presented to their expert for review prior to making a factually verifiable accusation to the contrary.

than make claims about supposed information that is either incorrect, inconsequential, or simply irrelevant to establishing probable cause.

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV. The issue before the court when reviewing the legal sufficiency of the search warrant is whether the issuing judge had a substantial basis for concluding that probable cause existed. *United States v. White*, 356 F.3d 865, 869 (8th Cir. 2004); *United States v. Terry*, 305 F.3d 818, 823 (8th Cir. 2002). "[P]robable cause does not demand the certainty we associate with formal trials." *Illinois v. Gates*, 462 U.S. 213, 246 (1983). The determination of probable cause is made by a "totality of the circumstances" review. *Id.* at 238. In the context of a search, probable cause is defined as a "fair probability that contraband or evidence of a crime will be found in a particular place." *Id.* The reviewing magistrate is to consider the facts in a practical common-sense manner. The evidence must provide the magistrate with a "substantial basis" for his findings. *Id.*,238-9.

It is well established that "to obtain relief under *Franks*, 'a defendant must first demonstrate that the law enforcement official deliberately or recklessly included a false statement or omitted a truthful statement from his warrant affidavit.'" *United States vs Mashek,* 606 F.3d 922, 928 (8th Cir. 2010). *see also United States v. McIntryre*, 646 F.3d 1107, 1113-14 (8th Cir. 2011) (quoting *Mashek*). Furthermore, before a defendant may receive such a hearing, the reviewing magistrate judge must determine that the allegedly false statement was necessary to the finding of probable cause. *Franks v. Delaware,* 438 U.S. 154 (1978); *see also United States v. Mashek,* 606 F.3d 922, 928 (8th Cir. 2010) (citing *United States v. Reinhollz,* 245 F.3d 765, 774 (8th Cir. 2001); *United States v. Jansen,* 470 F.3d 762, 765-66 (8th Cir. 2006); *United States vs. Sandoval-Rodriguez,* 452

F.3d 984, 988 (8th Cir. 2006). "Allegations of negligence or innocent mistake will not suffice to demonstrate a recklessness or deliberate falsehood." *Mashek*, 660 F.3d at 928 (citing *Franks*, 438 U.S. at 171). "In determining if 'an affiant's statements were made with a reckless disregard for the truth,' the test is whether, after viewing all the evidence, that affiant must have entertained serious doubts as to the truth of his statement or had obvious reasons to doubt the accuracy of the information he reported.'" *McIntyre*, 646 F.3d at 1114 (quoting *United States v. Butler*, 594 F.3d 955, 961 (8th Cir. 2010)). "A showing of deliberate or reckless falsehood is not lightly met." *Id.*

i. Alleged False Statement

At present, the defendant claims, based entirely on the mistaken and factually unverified representations of a defense hired expert, that "SA Faulkner's representation in the Second Search Warrant affidavit that he personally reviewed the zip file is plainly false-as Ms. Bush concludes based on the Torrential Downpour logs, he did not because he could not have." Doc. 37, p. 16. But, as stated above, this baseless claim fails when considering the actual facts and accurate explanation of the very basic technology at issue.

Factually, DUGGAR's claim that SA Faulkner could not have viewed the sixty-five (65) images from the "marissa.zip" file identified in the warrant can be easily disproven based on a simple review of the evidence collected and maintained in this case. As noted above, after Det. Kalmer downloaded the respective files described in the warrant, she contacted SA Faulkner to inquire if he would be willing to work the lead that she developed. In the ensuing weeks thereafter, she uploaded both the "mov_0216.mp4" and the "marissa.zip" file she obtained from DUGGAR's IP address onto the IDS system so that the images and corresponding information could be provided to SA Faulkner. To facilitate such, she contacted ICAC Administrator Lenore Paladino. Per the attached affidavit of Det. Kalmer, after downloading the respective two (2) files, she

verified the files she obtained during the download -meaning she actually viewed the images and video she downloaded and confirmed that they depicted illegal child pornography. (See Gov. Ex. 4). Thereafter, she contacted both SA Faulkner and ICAC administrator Lenore Paladino, as outlined above. Per Det. Kalmer's affidavit, she uploaded the two (2) respective files at issue onto the IDS system to facilitate the transfer of the lead to SA Faulkner. *Id.*

Per the attached affidavit of ICAC Administrator Lenore Paladino, whose duties include serving as the administrator of the IDS system in Arkansas, in May of 2019, Det. Kalmer advised her that she had downloaded images of CSAM from a target in Northwest Arkansas and requested that she allow SA Faulkner access to the files on the IDS system. (See Gov. Ex. 5). After Det. Kalmer uploaded both files, Administrator Paladino provided SA Faulkner access to this material. Importantly, per Administrator Paladino, the two files uploaded by Det. Kalmer remain on the IDS system to date. Gov. Ex. 5, ¶ 4. Additionally, per Administrator Paladino, the "marissa.zip" file that exists on IDS, which is the one and the same that she provided SA Faulkner access to, contains multiple viewable images depicting a prepubescent female engaging in sexually explicit conduct. Id. at ¶ 4.[6]

The fundamental defect with the defendant's argument here stems from the unverified and erroneous opinion of his expert, Michele Bush of Loehrs Forensics.[7] Ms. Bush states in her

[6] The fact that the two (2) respective files were uploaded to the IDS system was known to the defense prior to filing the instant motion, as this was clearly stated in Government's response to the Defendant's Motion to Compel Discovery (Doc. 32, pp.3-4).

[7] This would not be the first instance in which a representative from Loehrs Forensics advanced such a dubious claim. In fact, courts around the country have expressed misgivings about the foundation and reliability of claims made by representatives of Loehrs Forensics. For example, one court found that a declaration submitted by Tami Loehrs, the principal of Loehrs Forensics, in support of a motion to suppress evidence in a federal child pornography case was "misleading in several respects." *United States v. Thomas*, Nos. 5:12-cr-37, 5:12-cr-44, 5:12-cr-97, 2013 WL 6000484, at *12 (D. Vt. Nov. 8, 2013). According to that court, the "most troubling aspect of Loehrs's expert opinions" was "her reliance on her work in other cases which was either disproved

affidavit that per the Torrential Downpour logs pertaining to the "marissa.zip" file,

> Piece 0, which encompasses the first 262 megabytes of the file was not included in the 13 pieces downloaded from the Defendant's work IP address. This is significant because Piece 0 will contain the file header of the Marissa.zip file. The file header is encoding in the first several bytes which designates the file type (e.g. JPG, MOV, or ZIP) rendering the data set into a working copy that can be opened and accessed by the user. Without the file header, any system or software will render the file "corrupted" and will be inaccessible to the user. This evidence strongly suggests that the 13 pieces downloaded by Torrential Downpour and allegedly possessed by the remote client were in such an incomplete state that no user, including law enforcement, would have been able to successfully open or view any of the 65 images …"

Doc. 37-3, p. 7. However, as developed below, the file header of a "Zip" file is obtained or located at the end a file-not the beginning. Of note, Ms. Bush apparently agrees that Det. Kalmer, utilizing the Torrential Downpour program, accurately and completely downloaded the entire "mov_0216.mp4" file on May 14, 2019. See Doc. 37-3, p. 7. Separately, Ms. Bush states that Det. Kalmer factually obtained 13 pieces, comprising 262 megabytes per piece (which is a total of 3,406 megabytes) of the "marissa.zip file" on May 15, 2019. Id. However, again, she errors in concluding that the file header with respect to the "marissa.zip" file was Piece "0."

---

or rejected." *Id.* at 14. Noting that opinions she offered had been "squarely rejected" in another forum, the Court found Loehrs's claim to have not read that court opinion to have been "either incredible or reflective of a lack of concern regarding the reliability of the opinions she is offering under oath." *Id.* at 14-15. Ultimately, the Court found that "Loehrs provided little, if any, credible or reliable testimony to support her expert opinions[.]" *Id.* at 16; *see also United States v. Mitchell*, 128 F. Supp. 3d 1266, 1268-69 (E.D. Cal. 2015) (documenting discrepancies in Loehrs' declaration); *United States v. Certantes-Perez*, No. EP-12-CR-217, 2012 WL 6155914 at *3-8 (W.D. Tex. Dec. 11, 2012) (excluding portions of Loehrs's testimony that "threaten to mislead the jury with confusing logical gaps and legal conclusions" and describing her conclusions as "imprecise," "unreliable," "unsound and very misleading in this particular case"); *Mandli v. United States*, No. 09-61270-CV, 2011 WL 3349154 at *2 (S.D. Fla. Aug. 3, 2011) (finding Loehrs's affidavit made "unsupported, vague and conclusory statements regarding the content of the videos and pictures" she examined).

Instead, as set out in the attached affidavit of Computer Crimes Expert and Torrential Downpour co-creator Robert Erdely, he notes "the fact that the central directory, or header information [of a Zip file], is contained at the end of a Zip file …. [a]nd importantly, [at present] the last piece [of the marissa.zip file], in this case, "piece 65", was successfully downloaded." Gov. Ex. 6, ¶ 18. Moreover, per Erdely, the fact that a Zip file contains a header at the end of the file is "well established." Id. In fact, a simple internet search of Zip file format reveals:

> A directory is placed at the end of a ZIP file. This identifies what files are in the ZIP and identifies where in the ZIP that file is located. This allows ZIP readers to load the list of files without reading the entire ZIP archive. ZIP archives can also include extra data that is not related to the ZIP archive. This allows for a ZIP archive to be made into a self-extracting archive (application that decompresses its contained data), by prepending the program code to a ZIP archive and marking the file as executable. Storing the catalog at the end also makes possible hiding a zipped file by appending it to an innocuous file, such as a GIF image file.

See https://en.wikipedia.org/wiki/ZIP_(file_format).

However, to provide a complete and accurate opinion – instead of simply relying on an understanding, or a misunderstanding in Ms. Bush's case, of the Torrential downpour logs, Erdely conducted several tests on the "marissa.zip" file downloaded by Det. Kalmer to confirm whether the images were viewable. For his first three tests, Erdely examined a copy of the downloaded "marissa.zip" file itself- as it still exists on the IDS network- to view the contents utilizing three (3) separate zip file programs. Per Erdely, all three tests resulted in the viewer being presented with sixty-five (65) images. Id. For his fourth test, Erdely compared the 13 pieces of the "marissa.zip" file obtained by Det. Kalmer, to the same 13 pieces of the "marissa.zip" file that law enforcement maintains in the BitTorrent/Torrential downpour database and concluded that both were factually the same. Id. Finally, and most significantly, Erdely independently recreated the "marrisa.zip" that Det. Kalmer downloaded on May 15, 2019, by extracting the same 13 pieces from a complete and clean copy of the same "marissa.zip" file that has been logged by law

enforcement. In doing so, Erdely ended up with the same 65 viewable files as he did in the first three tests. Id. As such, in addition to being supported factually as set forth above, it is likewise evident that based on competent expert review, that sixty-five (65) viewable files were produced by Det. Kalmer's download of the "marrisa.zip." (See "Conclusions" Gov. Ex. 6). These files are the one and the same files identified by SA Faulkner in the search warrant affidavit.

The defendant also claims SA Faulkner misrepresented that the file was "successfully" downloaded. Doc. 37, p. 17. To the extent that this is still a viable claim based on the above, the defendant is at best left with an argument of semantics. While the entire or full file of "marissa.zip" was not obtained by Det. Kalmer, she did "successfully" obtain a file entitled "marissa.zip" that contained 65 images as SA Faulkner described in the warrant. Importantly, nowhere in the affidavit does SA Faulkner represent that the entirety of the file was obtained. To the contrary, he specifies that "[o]ne of the downloaded files was a "zip" folder containing sixty-five images." See Gov. Ex. 2, ¶ 34. Thus, while the defendant may argue about the semantic differences between "successfully" downloading a file and "entirely" downloading a larger version of that file, the difference between the two does not negate the magistrate's finding of probable cause. In fact, if the information about which the defendant now complains was presented to the Magistrate Judge Wiedemann—that the file Det. Kalmer downloaded from the user of the defendant's IP address was actually much larger and contained many more images of child sexual abuse material than described in the affidavit in support of the search warrant— were included in the affidavit, it would only further support the magistrate's probable cause determination, not negate it.

With respect to the remaining allegations that: 1- Faulkner misrepresented that only one (1) unique IP number can be assigned to a given customer's computer at any given time, and 2- SA Faulkner misrepresented that a "SHA1" hash value is called secure because its computationally

infeasible for two files with different content to have the same SHA1 hash value," both arguments fail to satisfy the requirements of *Franks*. With respect to the "IP number," a common sense reading of that paragraph in the affidavit in support of the search warrant reflects that SA Faulkner was representing that an "IP" number is specific to a customer's account on a given time, not that multiple devices could not simultaneously connect to the IP address assigned by the Internet Service Provider to the account. And while, this might be a "misstatement about technology" to the defendant, its more akin to common knowledge in 2021. With respect to the "SHA1" value argument, this again fails to satisfy the requirements for a *Franks* hearing, as the technology underpinning search warrants based on undercover peer-to-peer downloads, all of which involve the identification of CSAM files based on Sha-1 hashing, is well established.

This is true because the actual "odds of a Sha-1 hashing failing are 1 in 1,461,501,637,330,900,000,000,000,000,000,000,000,000,000,000,000." Gov. Ex. 6 ¶ 8. Either way, a hyper-technical misstatement did not affect the magistrate's determination that the warrant was supported by probable cause in the current case.

As such, the defendant has failed to show that SA Faulkner made an erroneous or false statement in the affidavit, and his request for a *Franks* hearing on this basis should be denied.

ii. Alleged Omissions

The defendant further claims that SA Faulkner omitted certain facts and information from the search warrant that rendered it invalid. But again, this argument fails based on a common sense reading of the warrant itself.

To support a request for a *Franks* hearing, the defendant must offer some evidence beyond mere assertions that an officer made an omission in the affidavit. *United States v. Castillo*, 287 F.3d 21, 26 (1st Cir. 2002). Omissions are different then misrepresentations and require a different

two-step test. The defense "must prove first that facts were omitted with the intent to make, or in reckless disregard of whether they make, the affidavit misleading, and, second, that the affidavit, if supplemented by the omitted information, could not support a finding of probable cause." *United States v. Allen*, 297 F.3d 790, 795 (8th Cir. 2002).

In this case, the affidavit provided sufficient probable cause, did not include false statements, and is not based on omissions of fact. In his motion, the defendant alleges that SA Faulkner "curiously omit[s] the fact that the Little Rock Police Department detective was using Torrential Downpour, software created by law enforcement that is not commercially available to the public." (Doc. 37, p.14). However, a close examination of the search warrant affidavit itself reveals that the magistrate was informed that "law enforcement uses special 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." Gov. Ex. 2, Affidavit, ¶12. Additionally, the magistrate was informed that this specific investigation involved an "online investigation on the BitTorrent Peer-to-Peer (P2P) network…" Id. at ¶ 34. In his argument, the defendant does not lay out how omitting the proper name of the "Torrential Downpour" program renders the affidavit misleading. Nor does the defense explain how supplementing the affidavit with this "omitted" information would negate the magistrate's probable cause determination. Ironically, the defendant likely "omitted" this part of the analysis, because the *Hoeffener* case foreclosed such arguments.

Next, the defendant claims, in a roundabout way, that the warrant omitted that law enforcement did not detect "further suspicious activity" from the target IP address on the BitTorrent network after the CSAM downloads listed in the affidavit. Doc. 37, p.18. This argument simply fails to satisfy common sense, much less the requirements of *Franks*. A magistrate reads an affidavit to determine if probable cause is supported based on the purported facts—not on the

assumption that other incriminating facts exists but are not listed. Therefore, stating that "no" criminal activity occurred outside of what is documented is unnecessary and inherently redundant. If the magistrate thought the affidavit needed more evidence of criminal activity to support a probable cause finding, she would not have issued the warrant. As for the defendant's claim that "three separate law enforcement agencies were apparently monitoring the target IP address [after May] and found nothing," that claim is simply inaccurate. Regardless, the absence of other criminal activity doesn't negate probable cause, it just does not further support it. As such, the defendant fails to show that the magistrate was misled by an intentional omission and has not—and indeed, cannot—show how supplementing the affidavit with this purported omission would negate the actual facts supporting the magistrate's probable cause finding.

Next, the defendant claims that the "affidavit omits the fact that law enforcement previously applied for and obtained the first search warrant based on the very same alleged basis for probable cause and curiously opted not to even execute the first search warrant upon making contact with the residents at the house." Doc. 37, p.19. Yet, again, an actual reading of the search warrant affidavit reveals otherwise. The affidavit illustrates that Ozark Go initially provided an address to a house adjacent to the Duggar's car lot. And paragraph 39 of the affidavit details that law enforcement contacted the residents of the adjacent home, who had no factual connection to this instant case, including that they did not obtain internet service from Ozarks Go and had no connection to the subscriber account listed under DUGGAR's name. (See Gov. Ex. 2). Instead, the residents informed law enforcement that DUGGAR owned and operated a car lot next door to their residence that did have internet service with Ozarks Go. *Id.* And then, starting with paragraph 40 and ending with Paragraph 44, SA Faulkner documented all the steps law enforcement took to verify that the correct and true address associated with the IP address during the timeframe in issue

was assigned to DUGGAR's car lot. As for the implication that the magistrate was misled by not specifically stating that a warrant was obtained prior to encountering the residents of the "first search warrant," the defendant does not acknowledge, or simply overlooks, that the warrants were issued by the same magistrate within days of each other. (See Gov. Ex. 1 & 2). Accordingly, the defendant again fails to satisfy the basic requirements to obtain a *Franks* hearing under the law.

Next, the defendant alleges that there was a lack of information in the affidavit about Torrential Downpour, including how "how it operates, and whether false positives occur." (Doc 37, p. 19). The defendant then baselessly claims that "these omissions are inherently misleading because false positives are likely to occur when investigating . . ." Id. Yet, again, the use of the very program to establish probable cause has been upheld by the Eighth Circuit in *Hoeffener*. Consequently, citing that Torrential Downpour was used and the technical underpinnings of the program would have only enhanced the probable cause finding. Further, the defendant once again fails to lay out any actual proof or describe which specific facts were intentionally left out to make the affidavit misleading, as he is required to do. Nor does he explain how supplementing the search warrant affidavit with this supposedly "omitted" information would negate the magistrate's probable cause determination.

Next, the defendant claims that SA Faulkner omitted "that the used car dealership law enforcement sought to search may have had unsecured Wi-Fi in May 2019 and/or secured Wi-Fi where the password was widely known, disseminated and used." Doc. 37, p. 20. First, as for the argument that law enforcement should have included whether the car lot's Wi-Fi was secure or not, this argument fails to reflect how the magistrate could have been misled by this lack of information. As such, the defendant confuses "omission" with the standard of proof required for probable cause. Moreover, an assertion that law enforcement could possibly determine that a

secured Wi-Fi password was widely disseminated prior to executing a warrant and interviewing witnesses is simply nonsensical.

Lastly, the defendant claims that the search warrant affidavit omits that the "ISP assigned to the [the target] IP address is to a residential account." Doc. 37, p.2 0. However, a general reading of the search warrant reveals that this fact was not obfuscated, but rather highlighted. Paragraph 37 is entirely dedicated to the fact that OzarksGo returned subscriber information stating that the IP address at issue was assigned to Joshua DUGGAR at 14993 Wildcat Creek in Springdale. Starting with paragraph 39, SA Faulkner details how law enforcement contacted the residents of 14993 Wildcat Creek in Springdale and learned that DUGGAR did not reside there, and that the residence did not have OzarksGo internet. The residents did however note that DUGGAR owned and operated a used car dealership on the adjacent piece of property and that the property that their residence and DUGGAR's car lot occupied was "either split or sold years ago and the current public records have not been updated to reflect the two separate lots." Gov. Ex. 2. Based on this information, law enforcement, as detailed in paragraphs 40 through 44, specifically laid out sufficient information establishing DUGGAR's car lot as the true location that was utilizing the target IP address during the timeframe at issue—as opposed to the residence first identified by OzarksGo. In other words, the defendant's claim that essential information was omitted again fails based on a plain reading of the search warrant affidavit.

Overall, the defendant has failed to make the substantial preliminary showing required for him to obtain a *Franks* hearing in this case. He has failed to meet his burden of showing that the affiant in this case knowingly and intentionally made false statements in the affidavit that were material to the magistrate's probable cause determination, and he has similarly failed to show that

the affiant omitted material facts with the intent to mislead the magistrate. In short, the search warrant is valid on its face and there is no evidence that material, intentional omissions occurred.

F. Forensic Examinations of the Defendant's Devices

For his final argument, the defendant claims that the forensic examinations conducted on DUGGAR's devices were warrantless searches. Specifically, the defendant asks this Court to conclude that Federal Rule of Criminal Procedure 41(e), allowing for subsequent forensic examinations, is both facially unconstitutional and unconstitutional as applied to DUGGAR. Doc. 37, p. 24. But, again, the defendant advances no specific factual reason nor law that supports his assertions. As such, this challenge fails, like the others, based on the facts of this case and the applicable law.

Neither the Fourth Amendment nor Rule 41 imposes any specific limitation on the time of the government's forensic examination. The government ordinarily may retain the seized computer and examine its contents in a careful and deliberate manner, subject only to the reasonableness requirement of the Fourth Amendment, and the reasonableness of the government's search is determined primarily by whether probable cause for the search has dissipated. The absence of a specific time frame for forensic examination is governed by a 2009 Amendment to Rule 41(e):

> A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off- site copying or review.

Since the enactment of this Amendment, Courts have agreed that neither the Fourth Amendment nor Rule 41 places explicit limits on the duration of any of forensic analysis, and courts have upheld forensic analyses begun months after investigators acquire a computer or

data. *See United States v. Burns*, 2008 WL 4542990, at *8-9 (N.D. Ill. Apr. 29, 2008) (ten month delay); *United States v. Gorrell*, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) (ten month delay); *United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 66 (D. Conn. 2002); *cf. United States v. New York Tel. Co.*, 434 U.S. 159, 169 n.16 (1977) (applying Fourth Amendment standards to pen registers before the enactment of the pen register act, holding that "the requirement … that the search be conducted within 10 days of its issuance does not mean that the duration of a pen register surveillance may not exceed 10 days").

Moreover, the Fourth Amendment itself does require that forensic analysis of a computer be conducted within a reasonable time. *See United States v. Mutschelknaus*, 564, F. Supp. 2d 1072, 1077 (D.N.D. 2008) ("[T]he Federal Rules of Criminal Procedure do not require that the forensic analysis of computers and other electronic equipment take place within a specific time limit. Any subsequent search only needs to be conducted within a reasonable time."); *Burns*, 2008 WL 4542990, at *8 ("A delay must be reasonable, but there is no constitutional upper limit on reasonableness."); *United States v. Grimmett*, 2004 WL 3171788, at *5 (D. Kan. Aug. 10, 2004), *aff'd* 439 F.3d 1263 (10th Cir. 2006). In judging the reasonableness of time for forensic analysis, courts may recognize analysis of computers is a difficult and time-consuming process. *See Triumph Capital Group, Inc.*, 211 F.R.D. at 66 (finding that time to complete search reasonable because "computer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search, more preparation and a greater degree of care in their execution").

Importantly, courts usually treat the dissipation of probable cause as the chief measure of the "reasonableness" of a search's length under the Fourth Amendment. For example, in *United States v. Syphers*, 426 F.3d 461 (1st Cir. 2005), the First Circuit stated that the Fourth

Amendment "contains no requirements about *when* the search or seizure is to occur or the *duration*," but cautioned that "unreasonable delay in the execution of a warrant that results in the lapse of probable cause will invalidate a warrant." *Id.* at 469 (quotations omitted). *see also Burns*, 2008 WL 4542990 at *9 (upholding search despite "lengthy" delay because "Burns does not assert that the time lapse affected the probable cause to search the computer (nor could he, given that suspected child pornography had already been found on the hard drive), that the government has acted in bad faith, or that he has been prejudiced in any way by the delay"). Significantly, dissipation of probable cause is unlikely in computer search cases because evidence is "frozen in time" when storage media is imaged or seized. *Triumph Capital Group, Inc.*, 211 F.R.D. at 66.

Additionally, applying the exclusionary rule to police delays by forensic examiners is even more questionable after *Hudson v. Michigan*, 547 U.S. 586 (2006). In *Hudson*, in which the Supreme Court rejected a suppression remedy for violation of the knock-and-announce rule, the Court held that "but-for causality is only a necessary, not a sufficient, condition for suppression." *Id.* at 592. In rejecting suppression, the Court also relied on the conclusion that suppression would not "vindicate the interests protected by the [constitutional] requirement [at issue]," *Id.* at 593, and that "the exclusionary rule has never been applied" when its "substantial social costs" outweigh its deterrent benefits. *Id.* (citation omitted). Once a computer seized pursuant to a warrant has been reviewed and information within the computer has been determined to fall within the scope of the warrant, subsequent review of those items should not implicate the Fourth Amendment. As the Ninth Circuit has explained, "once an item in an individual's possession has been lawfully seized and searched, subsequent searches of that item, so long as it remains in the legitimate uninterrupted possession of the police, may be conducted without a

warrant." *United States v. Turner*, 28 F.3d 981, 983 (9th Cir. 1994) (quoting *United States v. Burnette*, 698 F.2d 1038, 1049 (1983)).

Although "there is no established upper limit as to when the government must review seized electronic data to determine whether the evidence seized falls within the scope of a warrant," courts have found that "the Fourth Amendment requires the government to complete its review ... within a 'reasonable' period of time." *United States v. Mendlowitz*, 2019 WL 1017533, at *11 (S.D.N.Y. Mar. 2, 2019). However, there is no "one size fits all time period." *Id*. (citing *United States v. Ganias*, 755 F.3d 125, 136 (2d Cir. 2014) ("*Ganias I*") (noting Rule 41 recognizes severable variables—e.g., storage capacity of media, difficulties created by encryption or electronic booby traps, and computer-lab workload—that may influence the duration of a forensic analysis)), *rehearing en banc*, 824 F.3d 199 (2d Cir. 2016) ("*Ganias II*"). Courts have long recognized the "practical need for law enforcement to exercise dominion and control over documents and other physical evidence not within the scope of a warrant in order to determine whether they fall within the warrant." *United States v. Kaleta*, 2017 WL 11404638, at *12 (E.D. Mo. Aug. 10, 2017), *report and recommendation adopted sub nom. United States v. Kelta*, 2017 WL 11404639 (E.D. Mo. Sept. 18, 2017). "Numerous cases hold that a delay of several months or even years between the seizure of electronic evidence and the completion of the government's review of it is reasonable." *United States v. Jarman*, 847 F.3d 259, 266-67 (5th Cir. 2017) (upholding a twenty-three-month long review of electronic evidence).

In this case, all the devices at issue were seized on or about November 8, 2019, pursuant to a warrant that allowed for searches of such for evidence related to receipt and possession of child pornography. Within weeks thereafter, forensic copies of all devices were made by CFA Kennedy. These forensic copies were searched for the very evidence outlined in the warrant via

law enforcement forensic tools. And it is this same evidence that supports the current prosecution for essentially the crimes outlined in the warrant. CFA Kennedy submitted his forensics findings in a report on about July of 2020. Approximately nine (9) months later, a Grand Jury returned an Indictment against DUGGAR. Noteworthy, in 2019, the HSI ICAC in Northwest Arkansas investigated a majority of all child exploitation cases federally prosecuted in the Western District of Arkansas. The computer forensics underpinning such cases were almost exclusively handled by the HSI forensics lab in which CFA Kennedy works. This heavy workload continued into 2020. Even more astounding is that all the forensic analysis and processing, which can't be done remotely, was completed during the outbreak of and during the COVID-19 pandemic.

Importantly, the fact that forensic images were created maintained the integrity of evidence at issue, as opposed to allowing it to dissipate. Factually, through the examinations of these devices, CFA Kennedy was able to confirm that: DUGGAR installed a password protected Linux partition on his hard drive to mask his criminal activities; DUGGAR utilized not one, but two, separate programs to obtain CSAM (the TOR browser is designed to avoid detection); and DUGGAR's MacBook and iPhone contain pictures and text messages placing him at the car lot during the timeframe at issue. Based on this properly persevered and maintained evidence, law enforcement was able to recreate the defendant's computer-based crimes, and even place him essentially behind the keyboard. And while the defendant asks this Court to deem Rule 41(e)(2)(A) unconstitutional, his claims amount to generalized notion that the law is unfair because incriminating evidence against him was discovered. Additionally, these complicated forensic examinations collectively took over a span of at most, sixteen months, which represents the time at which the devices were seized until the time in which the defendant was indicted. Consequently, this type of forensic work is exactly what Rule 41(e)(2)(A) was designed and passed into law to

allow. Forensic examiners are by and large not investigators. By necessity, their work involves producing certain digital evidence, presenting such to an investigator or prosecutor, and then taking direction on what else to locate or analyze to aid the criminal case.

Accordingly, the defendant's undeveloped and legally unsupported constitutional challenges to this rule of criminal procedure as unconstitutional must fail. As such, the primary examination by CFA Kennedy, who finalized his forensic report as of July of 2020 was timely. And HTIU's supplemental examinations, which were based off CFA Kennedy's image and overall confirmed the same evidence discovered by CFA Kennedy, were also timely.

Confusingly, the defendant claims that both CFA Kennedy's and HTIU's review should collectively be deemed warrantless searches, yet he fails to differentiate between the timeframes of the two respective searches (i.e.: provide to this Court what CFA Kennedy's earlier examination missed and HTIU's located). This is because the evidence recovered by CFA Kennedy and later confirmed by HTIU, did not change nor dissipate. Rather, both simply confirmed that DUGGAR had been downloading and viewing images in violation of federal child pornography laws.

Lastly, the defendant argues that the examination conducted by HTIU DIA Bradley Gordon should be deemed warrantless as "they were conducted pursuant to an invalid warrant that law enforcement represented to this Court was not executed." (Doc. 37. p. 26). Apparently, the defendant is asking this Court to declare a search pursuant to a warrant invalid, because a computer forensic examiner noted the wrong warrant number when finalizing his forensic report. In response, the Government simply asserts that a scrivener's error in a forensic report- that is not a part of the search warrant itself-does not present as a reason to declare an entire search invalid under the Fourth Amendment.

G. Good Faith Exception

The information contained in the affidavit was sufficient to support a probable cause determination and did not contain false nor misleading information. Should this Honorable Court conclude otherwise, however, the evidence seized pursuant to the warrant should not be suppressed because the officers acted in good faith in relying on the issuance of the search warrant. In *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court considered whether the Fourth Amendment exclusionary rule should be modified so as not to bar evidence obtained by officers acting in reasonable reliance on a search warrant issued by a neutral and detached magistrate, but ultimately found not to be supported by probable cause.

The *Leon* Court ultimately ruled that, "suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause." *Id*. at 926. "Because the disputed evidence was seized pursuant to a warrant, it will not be excluded, even if a reviewing court determines that the supporting affidavit failed to establish probable cause, as long as the executing officers relied in objectively reasonable good faith upon the warrant." *United States v. Vinson*, 414 F.3d 924, 930 (8th Cir. 2005)(quoting *Leon* at 922).

There are four situations where the good-faith exception to the warrant requirement does not apply. Those situations are (1) if the magistrate or judge was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth; (2) where the issuing magistrate "wholly abandoned his judicial role" when issuing the warrant; (3) when the affidavit is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) where the warrant is "facially

deficient – i.e., in failing to particularize the place to be searched or things to be seized – that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923.

In the present case, the defendant did not address good faith at all. According to *Leon*, application of the good faith exception is "particularly true . . . when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." *Leon*, 468 U.S. at 920. When issuing a search warrant, a judge is only required to answer the "common sense, practical question whether there is probable cause to believe that contraband is located in a particular place." *See United States v. McArthur*, 573 F.3d 608, 613 (8th Cir. 2009). Courts give "great deference to the decision of the judicial officer who issued the warrant." *United States v. Maxim*, 55 F.3d 394, 397 (8th Cir. 1995). Consequently, this Court should find that law enforcement relied on the instant warrant in good faith.

CONCLUSION

The government submits the search warrant was supported by probable cause, was executed in a timely manner pursuant to applicable law and did not contain materially false or misleading statement nor omissions. In the event this Honorable Court finds insufficient probable cause existed to issue the search warrant, the motion to suppress should nevertheless be denied because the *Leon* good faith exception applies.

The United States Requests Defendant's Motion to Suppress be denied.

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 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
Dustin Roberts
Assistant United States Attorney