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

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Case No. 5:21-CR-50014-001**
	)	
JOSHUA JAMES DUGGAR,	)	
	)	
Defendant.	)	

DEFENDANT'S REPLY IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE AND REQUEST FOR A *FRANKS* HEARING

Defendant Joshua James Duggar ("Duggar"), by and through undersigned counsel, respectfully replies in support of his motion to suppress evidence and request for a *Franks* hearing. *See* Doc. 37 (underlying motion) and Doc. 45 (Government's response).

I. The Government's May 2019 Use of Torrential Downpour Requires Suppression

When reading the Government's response, it is easy to lose sight of the fact that Duggar is *not* arguing that law enforcement's use of Torrential Downpour—in and of itself—requires suppression. *See, e.g.,* Doc. 45 at 8 ("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") (citing *United States v. Hoeffener*, 950 F.3d 1037 (8th Cir. 2020)); Doc. 45 at 9-10 (citing *Hoeffener*). Instead, Duggar's argument is more nuanced and premised largely on the fact—which the Government fails to acknowledge or dispute in its 41-page response—that law enforcement spent 17 hours, attempting 169 times, to download only 13 of the 66 pieces that comprise only a small fraction of the "marissa.zip" file that was allegedly stored on

a shared computer located in a business 6 months before the Government applied for a search warrant.

Furthermore, rather than engaging with Duggar's argument that tracking a device allegedly containing unlawful materials for 17 straight hours but failing to download the entire file is substantively different than what even the Government acknowledges in other cases typically occurs with Torrential Downpour, the Government simply argues Torrential Downpour "gathered nothing more then [sic] what DUGGAR was offering to strangers over the same network[.]" Doc. 45 at 9 (capitalization in original). But this response misses the mark entirely. If, as the Government asserts, a computer is offering a file to strangers, Torrential Downpour would have simply downloaded it—in its entirety—within minutes. That law enforcement attempted 169 times to download a file allegedly located on a computer, but nevertheless failed to download the entire file, reveals an inconvenient truth for the Government in this case: this file was *not* being "offer[ed] to strangers," and, therefore, a warrant was required in advance of the prolonged tracking. *Id.*

The Government disparages Duggar's argument that law enforcement's use of Torrential Downpour in this case was more akin to law enforcement's use of a tracking device. However, in criticizing instead of grappling with the argument, the Government cites authority which supports Duggar's position: *United States v. Shipton*, 5 F.4th 933 (8th Cir. 2021). In that case, the Eighth Circuit discussed a defendant's challenge to law enforcement's use of peer-to-peer networks to identify possessors of child pornography and explained:

> Unlike [*United States v. Jones*, 565 U.S. 400 (2012)], 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 v. United States*, 138 S. Ct. 2206 (2018)], 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 v. California*, 573 U.S. 373 (2014)] 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.

Id. at 936. In other words, law enforcement's use of tools like Torrential Downpour typically involves a brief interaction, for a limited purpose, with a device connected to the internet. But in this case, law enforcement used Torrential Downpour to track a device for 17 hours and attempted 169 times to gather the information it sought. In that vein, law enforcement's actions here *were* akin to a situation where officers tracked a person's car with the help of a GPS device or collected a trove of information utilizing cell-site location information—both situations in which it is settled that law enforcement must first obtain a warrant. *See id.* The Government does not address the great amount of time spent or the high number of attempts made to download only a fraction of a file because the Government has no meaningful response.

When Detective Kalmer's use of Torrential Downpour failed to successfully download the zip file the first time, the interaction between the two devices should have ended—but law enforcement kept tracking this device and did so 169 times over the next 17 hours. If, as the Government now contends, the device was making this file available to the public, law enforcement would have simply downloaded the entire file on its very first attempt. This undercuts all the Government's arguments and lengthy inapposite quotations concerning an individual's lack of a reasonable expectation of privacy in things voluntarily made available to the public. *See* Doc. 45 at 11-14.

This is particularly important because, as this Court has already recognized, when law enforcement uses a device to track information—especially when the device is located outside the judicial district where the device being tracked is located—a warrant is required. *See United States v. Jean*, 207 F.Supp.3d 920, 937 (W.D. Ark. 2016). Indeed, "[i]nternet crime and surveillance defy traditional notions of place" and a warrant is required to track "mere intangible 'information.'" *Id*.

at 941 (citing Fed. R. Crim. P. 41(a)(2)(A)). The Government offers no response other than to broadly argue that the software used by law enforcement in that case differs from Torrential Downpour. *See* Doc. 45 at 13-14. But what the Government fails to acknowledge is that, in this case, Torrential Downpour operated differently from the norm. It literally tracked a device 169 times over 17 hours.

At a minimum, the Government should be required to establish at a suppression hearing how Torrential Downpour interacted with the device(s) at issue in this case because suppression will turn on the specific factual inquiry of what law enforcement actually did instead of broad generalizations about how the Government claims the software is supposed to work.

II. The Second Search Warrant Was Not Supported by Probable Cause

The Government criticizes Duggar for arguing that the standard for probable cause sufficient for issuance of a search warrant varies depending on whether the search warrant is for a residence or a business. *See* Doc. 45 at 14. And while Duggar acknowledges there is no hard and fast rule with respect to staleness in the context of child pornography investigations, the passage of 6 months between an alleged download from a device located at a business—with employees, customers, and perhaps unsecured wi-fi—is significant and renders the purported probable cause in support of law enforcement's application for the search warrant stale. *See* Doc. 37 at 13. Unlike a residence, where occupants are static and the presence of outsiders is infrequent, an allegation that unlawful material was present at a business must be made quickly to avoid any probable cause that once existed from evaporating.

The Government condemns Duggar's argument, claiming he "fails to cite any authority for this contention." Doc. 45 at 14. And the Government resorts to arguing, essentially, that staleness should never be a concern in cases like this one because the type of 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." *Id.* at 15 (quoting *United States v. Craig*, 861 F.2d 818, 823 (5th Cir. 1988)).[1] But what is most telltale about its response is that the Government fails to cite any authority whatsoever refuting Duggar's argument that the significance of the passage of time is amplified with a business—especially with transient employees using a shared computer and customers who come and go on a daily basis—because many people and devices can access the business' internet service for both long and short periods of time.

Rather than providing any actual response to this argument, the Government cites several cases: *United States v. Lemon*, 590 F.3d 612 (8th Cir. 2010); *United States v. Burkhart*, 602 F.3d 1202 (10th Cir. 2010); *United States v. Morales-Aldahondo*, 524 F.3d 115 (1st Cir. 2008); and *United States v. Vosburgh*, 602 F.3d 512 (3d Cir. 2010). *See* Doc. 45 at 15). However, without exception, each of these cases analyze staleness of probable cause in connection with an application for a search warrant for a residence, *not* a business.

This failure to provide any adverse authority on this point is significant and is perhaps indicative of the fact that, typically, law enforcement acts more expeditiously when it comes to obtaining broad search warrants for businesses that are open to the public so as to avoid any issues with the inescapable conclusion that probable cause fades far more quickly at a business than it does at a residence.

In an apparent attempt to convince this Court that no staleness inquiry is justified, the Government asks this Court to adopt a stunning and unprecedented standard: "given computer forensic abilities, it is unlikely that probable cause to search a computer *will ever be stale*." Doc.

[1] The Government's miscites this authority as *United States v. Kleinkauf*.

45 at 18 (emphasis added). The standard the Government is advocating is unconstitutional on its face.

Indeed, it is firmly established that a warrant may not issue on evidence "too stale to furnish probable cause." *Unites States v. McCall*, 740 F.2d 1331, 1336 (4th Cir. 1984). And it is also well-established that in cases involving child pornography, months-old evidence that a suspect possessed child pornography is too stale to establish probable cause absent any evidence that the suspect is a "collector." *See United States v. Doyle*, 650 F.3d 460, 474 n. 15 (4th Cir. 2011); *see also United States v. Raymonda*, 780 F.3d 105, 117 (2d Cir. 2015) (holding that evidence that suspect had "accessed thumbnails of child pornography" nine-months earlier was too stale to establish probable cause when affidavit failed to establish suspect was a collector"). To be clear, an affidavit only establishes a fair probability that a suspect is a collector child pornography if the affidavit sets forth "circumstances suggesting that [the suspect] had accessed those images willfully and deliberately, actively seeking them out to satisfy a preexisting predilection." *Raymonda*, 780 F.3d at 115.

Further, the Government's argument that staleness should be of no concern because files can rarely if ever be truly deleted from a computer misses the point. *See* Doc. 45 at 18. While it is true that files, in many instances, remain on computer devices even after their deletion, this does nothing to call into question Duggar's argument here: that where law enforcement seeks a search warrant for a business with employees and customers who are able to access wireless internet using numerous devices, the likelihood that whatever device allegedly possessed child pornography would still be at the business decreases with each passing day. While the files might not be deleted, the devices themselves are far more likely to disappear.

Finally, the Government asserts in a footnote that because the "mov_0216MP4" file was successfully downloaded by Detective Kalmer, "that file alone establishes probable cause." *See* Doc. 45 at 9 n.4. But this Court should reject this premise. Law enforcement's alleged download of a single, innocuously-named, 2-minute video 6 months earlier from an IP address used by a business does not establish sufficient probable cause to seize any and all electronic devices located at that business. Indeed, "[a]n affidavit must provide the magistrate with a substantial basis for determining the existence of probable cause[.]" *Illinois v. Gates*, 462 U.S. 213, 239 (1983). An affidavit that said a two-minute-long video entitled "mov_0216MP4" was downloaded at a business with employees and customers accessing the internet using various devices, with nothing more, falls far short of establishing probable cause.

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. When law enforcement applied for the warrant, the alleged child pornography could have been on a business device, a business owner's device, a customer's device, or a complete stranger's device using the business's Wi-Fi and, therefore, its IP address. That should not have given the Government authority to storm into the business nearly six months later seizing everything in sight.

III. The Affidavit Contained False Statements

The Government attacks Duggar's computer forensics expert's conclusion that the "marissa.zip" file at issue in this case was not "successfully" downloaded. *See* Doc. 45 at 21. The Government, in consultation with its own computer forensics expert, Robert Erdely, asserts that a "Zip file header" is "contained in the last piece, piece '65' in this instance, which was successfully

downloaded by Det. Kalmer." *Id.* Thus, the Government argues, the affidavit contained no false statements.

The Government asserts that the "file header" of a zip file is located at the end of a file, not the beginning, and therefore computer forensics expert Michele Bush's opinion that this file could not have been successfully viewed is incorrect. *See* Doc. 45 at 25. In support, the Government claims that its expert 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." Doc. 45 at 26 (citing Doc. 45-6 at ¶ 18) (bracketed portions in original). While Erdely does not actually say that in his affidavit, the substance of the argument can nevertheless be addressed.

First, Erdely's affidavit does not expressly address, as the above quote suggests, "header information." Instead, his analysis focuses on the presence of a "central directory" in a zip file. *See* Doc. 45-6 at ¶ 18. Erdely concludes that the central directory of all zip files is located at the end of a file, not the start, and that the last piece of this zip file was successfully downloaded. *Id.* Thus, in his opinion, although only 13 of 66 pieces of the zip file were downloaded, the file could be recreated. *Id.*

Ms. Bush notes that the local file header was not downloaded in this case. *See* First Supplemental Affidavit of Michele Bush at 1 (attached hereto as Exhibit 1). However, Bush explains, "[t]he central directory is an extension of the local file header[.]" *Id.* at 2. Ms. Bush further notes that the zip file at issue:

> is broken into 66 total pieces (0 through 65) and, as clarified in Mr. Erdely's affidavit, all but the last piece are 262,144 bytes in size. This means pieces 0 through 64 encompass 17,039,360 total bytes (262,144 bytes x 65 pieces) and leaves piece 65 to encompass the remaining 130,396 bytes of the file. If the central directory is larger than 130,396 bytes and begins at a file offset contained in pieces

> 58 through 64, then the zip file will likely still be corrupt and inaccessible to any user because its file header is missing, even having the last piece.

Id. Thus, while Erdely asserts in his affidavit that, through testing, he was able to recreate the partially downloaded zip file using the central directory, because the Government did not provide Bush with access to the partial zip file, Bush remains unable to independently verify Erdely's claims.

Furthermore, Erdely's affidavit explains, for the first time, that a "complete copy" of the marissa.zip file "contains 405 files." Doc. 45-6 at ¶ 18. Thus, not only did law enforcement in this case spend 17 hours and 169 attempts to only obtain 13 of 66 pieces of the file—a fact which the Government does not dispute—a "complete copy" of this zip file would actually include 405 files as opposed to the 13 of 66 pieces purportedly downloaded by law enforcement in this case.

Thus, while the Government curiously resorts to *ad hominem* attacks on Ms. Bush[2] and on defense counsel, it remains clear that the affidavit in this case *did* contain a false statement: that the marissa.zip file was "successfully downloaded." *See* Doc. 37-2. No matter how much the Government tries to complicate the situation, the marissa.zip file was *not* "successfully downloaded." *See id*. Or even close.

An *accurate* statement would be that the marissa.zip file contains 405 files but, here, only 65 files were allegedly present on a device utilizing an IP address at a business, and after 17 hours and 169 attempts, only 13 of 66 total pieces were downloaded. Had the affiant replaced the false

[2] The Government goes out of its way to gratuitously attack the credibility of Tami Loehrs—but not Bush herself—string-citing certain district court opinions. *See* Doc. 45 at 24 n.7. While it is entirely unclear why Ms. Loehrs' credibility is being questioned by the Government in this case, there are a number of courts that have credited her testimony. *See, e.g., United States v. Gonzalez et al.*, No. CR-17-01311-001 (D. Ariz. 2019); *United States v. Carter*, No. 16-20032-02 (D. Kan. 2019); *United States v. Hartman*, No. SACR 15-00063 (C.D. Cal. 2015). The Government does not claim that Ms. Bush's credibility has ever been questioned by any court.

statement with this accurate statement, the magistrate judge would not have signed the requested search warrant.

To be clear, in prior cases, the Government itself has gone out of its way to emphasize the significance of a successful and prompt download of a full file when establishing probable cause using Torrential Downpour. Most notably, the Government relies heavily in this case on *United States v. Hoeffener*, 950 F.3d 1037 (8th Cir. 2020) in its response. But when actually litigating *Hoeffener* before the Eighth Circuit, the Government emphasized to the appellate court that "[d]uring the connection, Appellant Roland Hoeffener's computer acknowledged having *all of the pieces of the files*." *See United States v. Hoeffener*, Case No. 19-1192, Appellee's Brief at 13 (filed August 14, 2019) (emphasis added). Thus, the Eighth Circuit found no problem with the Government's use of Torrential downpour in that case—where "Hoeffener's computer acknowledged having all of the pieces of the files"—to establish probable cause for issuance of the warrant. Here, in stark contrast, the Government's use of Torrential Downpour unambiguously revealed that a device at a business's IP address never once "acknowledged having all of the pieces of the file[]" but the Government, nonetheless, attested that the zip file was "successfully downloaded."

In response to the inescapable fact that the Government did *not* "successfully download" the zip file, the Government contends that Duggar is left with "an argument of semantics," asserting, "[w]hile 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." Doc. 45 at 27. But this is not an argument of semantics and the Government's steadfast refusal to acknowledge that the zip file was *not* successfully downloaded, and that it took law enforcement 17 hours and 169 attempts to only download a fraction of a portion

of the file, speaks volumes. The Government's attempts to downplay the significance of this material misrepresentation to the magistrate are unpersuasive and should be rejected by this Court.

Furthermore, neither the Government nor its expert dispute that the Torrential Downpour logs in this case reveal:

> For approximately 39 minutes between 06:00:44PM and 06:39:12PM, Torrential Downpour attempted to connect to Defendant's work IP address eight times but continued to report a failure to establish a connection. Between 06:45:12PM and 06:45:16PM, Torrential Downpour reported the ninth attempted connection was successful, that the "remote client acknowledges it has 13 of 66 pieces", and subsequently downloaded those 13 pieces within four seconds. For another 17 hours between 06:46:59PM and May 16, 2019, at 11:35:13AM, Torrential Downpour continued to attempt to connect to Defendant's work IP address 160 additional times to download Torrent 3255 but reported "Remote client indicated that it has no complete files" and ceased communication.

Doc. 37-3 at 7. That Torrential Downpour failed to establish a connection, that the device allegedly acknowledged having only 13 of 66 pieces, and that the device "indicated it has no complete files" is critical, especially when this Court considers the position the Government advanced before the Eighth Circuit in *Hoeffener*.

Specifically, in its briefing to the Eighth Circuit, the Government explained that Torrential Downpour "log files are a second-by-second detailed record of Torrential Downpour's actions and show the software was performing correctly." *See United States v. Hoeffener*, Case No. 19-1192, Appellee's Brief at 14 (filed August 14, 2019). The Government continued, "[t]he files showed exactly what happened during Det. Baine's download from Hoeffener's computer, including" among other things, "whether the download was successfully completed"; "files of child pornography completely downloaded from Hoeffener's computer to the law enforcement computer with no interruptions or problems"; and the "fact that Torrential Downpour software operated as intended." *Id.* at 14-15.

The Government made these representations in *Hoeffener* because these facts are important and benefitted the Government's argument in that case that its Torrential Downpour there was perfectly fine and provided probable cause for issuance of a search warrant. That the Government ignores that none of these facts, which were present in *Hoeffener*, apply to this situation is remarkable and sheds light on the precariousness of the Government's position here.

Finally, turning to Duggar's argument that the affidavit also misrepresented the fact that "only one (1) unique IP number can be assigned to a given customer's computer at any given time" (Doc. 37-2 at ¶ 10), the Government summarily responds that "a common sense reading of that paragraph...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[.]" Doc. 45 at 28. This is nothing more than an attempt to re-write history—and it strains credulity to argue that when Faulkner said that an IP number is assigned to a customer's computer, he really meant that multiple devices could simultaneously connect to the IP address.

These false statements—individually and collectively—warrant a *Franks* hearing and ultimately suppression. "A defendant is entitled to [a *Franks*] hearing if he 'makes a substantial preliminary showing that a false statement was knowingly and intentionally, or with reckless disregard for the truth, included by the affiant in the warrant affidavit,' and 'the allegedly false statements is necessary to the finding of probable cause.'" *United States v. Timley*, 443 F.3d 615, 623 (8th Cir. 2006) (quoting *Franks*, 438 U.S. at 155-56). In the context of a *Franks* analysis, district courts "must also insist" that the magistrate judge who signed the search warrant did "not serve merely as a rubber stamp for the police." *See Aguilar v. Texas*, 378 U.S. 108, 111 (1964). Where, as here, a defendant's attack on the warrant is "more than conclusory" and is "supported by more than a mere desire to cross-examine," a *Franks* hearing is mandated. *Franks*, 438 U.S. at

155-56, 171. Here, there are "allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations [are] accompanied by an offer of proof." *Id*. at 171.

IV. The Affidavit Omitted Important Facts Which Misled the Magistrate

A *Franks* hearing is also necessitated where, as here, an agent omits facts. *See United States v. Allen*, 297 F.3d 790, 795 (8th Cir. 2002) (a defendant must establish "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") (internal citations omitted).

Among other things, the affidavit omits entirely that the used car dealership law enforcement sought to search was a business that regularly catered to the general public in May 2019 and that regularly had transient workers and employees at that time. And the affidavit leaves out that the used car dealership law enforcement sought to search may have had unsecured Wi-Fi in May 2019.

In response to this argument, the Government asserts that these omissions could not possibly have misled the magistrate and claims that law enforcement had no way of determining whether the car dealership had unsecured Wi-Fi or whether the password to a secured network was widely disseminated. But the Government is wrong on both points.

First, it cannot be reasonably disputed that a magistrate would have benefited from disclosure of these facts. Unquestionably, probable cause would decrease if the magistrate knew that the only alleged evidence of a crime last detected 6 months prior was located at a business with internet readily accessible by countless employees and customers. Second, SA Faulkner expressly states in the affidavit that an "HSI Task Force Officer, acting in an undercover capacity" went to the business to discuss the possibility of purchasing a vehicle. *See* Doc. 37-2 at ¶ 44. While

there, the undercover officer claims to have observed Duggar using an iPhone and a laptop computer. *Id.* In this scenario, the officer could have either used his phone to access Wi-Fi or, if unsuccessful, asked whether any of the employees would be willing to share the password. If the magistrate had been informed that the search warrant being applied for was for a business with Wi-Fi accessible by countless people using countless devices, it would have altered the analysis.

These false statements and omissions were intentional or, at a minimum, the result of a reckless disregard for truth. The purpose of these false statements and omissions was clear: to overstate and misrepresent the likelihood that a device connected to an IP address had possessed numerous files on multiple days containing child pornography to persuade the magistrate judge to issue the Second Search Warrant. Without these false statements and omissions, the affidavit did not establish probable cause.

V. The Searches of the Devices Including the HP Computer Were Warrantless As They Did Not Occur Until After the Warrant Expired

Duggar notes that the devices were seized pursuant to a warrant signed on November 4, 2019 which expressly required that it be executed within 14 days. And while law enforcement seized the devices within that timeframe, the Government did not search those devices and seize items pursuant to the limitations set out in Attachment B to the warrant until months and even years after the deadline. To this day, HSI has never filed an inventory of items seized from any subsequent search of any particular computer or electronic device or hard drive.

In his affidavit in support of the Second Search Warrant, SA Faulkner stated that searching computer storage devices "can take up to several months to complete" and sought "authorization 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" and that "[i]f 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." *See* Doc. 37-2. However, after several months transpired, HSI did not request that the magistrate judge give it any additional time beyond the time frame specified in the warrant—and only requested that HSI be permitted to conduct the particularized searches offsite. Discovery reveals that government investigators have continued to perform searches of the devices as recently as February 2021. And the Government appears to concede that searches continued even beyond that date, noting, "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." Doc. 45 at 37 (Duggar was indicted on April 28, 2021).

"It is settled law that the search and seizure of evidence, conducted under a warrant, must conform to the requirements of that warrant." *United States v. Brunette*, 76 F. Supp. 2d 30, 42 (D. Me. 1999) (citing *Massachusetts v. Sheppard*, 468 U.S. 981, 988 n. 5 (1984)). In *Brunette*, the United States District Court for the District of Maine suppressed all evidence obtained by the Government's search of a computer after the deadline imposed in the search warrant. *Brunette*, 76 F. Supp. 2d at 42. The district court's analysis boiled down to a simple but legally critical underpinning: the search exceeded the temporal bounds of the warrant itself and it was therefore unconstitutional requiring suppression. The Government does not address this authority.

Instead, the Government argues that the lengthy delay in this case is not unreasonable and is allowed under a 2009 amendment to Federal Rule of Criminal Procedure 41(e). *See* Doc. 45 at 33. Indeed, it appears to be the Government's position that there is no amount of time that could possibly be unreasonable or violate Rule 41(e). *See id.* at 35 ("dissipation of probable cause is unlikely in computer search cases because evidence is 'frozen in time' when storage media is imaged or seized") ("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").

In an apparent attempt to obfuscate the fact that the Government performed searches of the devices seized pursuant to the Second Search Warrant for, at a minimum, 16 months—far in excess of the time permitted for searches to occur pursuant to the warrant—the Government cites only one case in which such a lengthy delay was upheld by a court. *See* Doc. 45 at 36 (citing *United States v. Jarman*, 847 F3d 259 (5th Cir. 2017)). However, in *Jarman*, the court noted, "Jarman waived the claim that the Government's actions violated Rule 41 because he merely mentions the issue in a footnote with little or no argument." *Jarman*, 847 F.3d at 266. The court then explained that the search there was, nonetheless, reasonable because the defendant was an attorney and a complicated "taint process" had to be undertaken in order to prevent the Government from coming into possession of attorney-client privileged documents as it searched the computer. *Id.* at 263.

That is simply not the case here and there is no good reason for the Government to be acting as though there is absolutely no temporal limitation with respect to its ability to continue searching, indefinitely, the devices seized. Remarkably, the Government's position as to Duggar's motion to suppress is that the staleness inquiry does not exist in child pornography cases and that the Government, upon seizing a device, can constitutionally search it forever. This effectively erases the reasonableness requirement set out in the Fourth Amendment.

Furthermore, in response to Duggar's argument that Rule 41(e)(2)(B) is unconstitutional, both facially and as applied to him, the Government disingenuously attempts to recharacterize Duggar's argument as being, "the law is unfair because incriminating evidence against him was discovered." Doc. 45 at 37. This is not a response at all.

First, Rule 41 is not a law, it is a Federal Rule of Criminal Procedure. Second, notwithstanding the Government's attempt to defeat this strawman argument instead of engaging with Duggar's actual argument, a Federal Rule of Criminal Procedure is only valid to the extent it does not "abridge, enlarge or modify any substantive right." 28 U.S.C. § 2072(b). While the Rules Enabling Act (28 U.S.C. § 2072) gives the Supreme Court "the power to prescribe general rules of practice and procedure and rules of evidence for cases in the United States district courts (including proceedings before magistrate judges thereof) and courts of appeals" (28 U.S.C. § 2072(a)), the Act also commands, "[s]uch rules shall not abridge, enlarge or modify any substantive right." 28 U.S.C. § 2072(b). Thus, the question turns on whether a "substantive right" is implicated. *Id*.

There can be no meaningful dispute that a substantive right is implicated: the Fourth Amendment right to be free from unconstitutional searches. Where the Government seizes a computer pursuant to a warrant, holds onto it indefinitely, and then takes the position that it has the authority to perform a particularized search of the computer from then until eternity, a defendant's constitutional rights are unquestionably violated. Thus, to the extent this Court were to read and interpret Rule 41(e)(2)(B) in such a broad capacity, the rule would undoubtedly be unconstitutional on its face. But this Court need not go so far in this case—because, here, the affidavit expressly stated the search would take "several months" and that it would return the devices within a reasonable timeframe. The devices—including all of Duggar's personal devices which the Government readily acknowledges contained no alleged contraband—remain in the Government's possession.

The Government chooses not to engage with this argument because there is no good response, as there can be no meaningful dispute that Duggar has a substantive right to not be

subjected to unreasonable searches and seizures pursuant to the Fourth Amendment to the United States Constitution. The Government's argument that it can continue to search these devices for eternity should be rejected by this Court.

VI. The Exclusionary Rule and the Good Faith Exception

In an effort to convince this Court that suppression of the evidence seized is not warranted in this case, the Government contends that the "exclusionary rule" should not be applied (*see* Doc. 45 at 12-13; 35-36) and that the "good faith exception" to the Fourth Amendment's warrant requirement applies (*see id.* at 39-40). The Government's argument on these points is unpersuasive.

A. The Exclusionary Rule Should be Applied

It is firmly established that the "exclusionary rule that, when applicable, forbids the use of improperly obtained evidence at trial." *Herring v. United States*, 555 U.S. 135, 139 (2009) (citing *Weeks v. United States,* 232 U.S. 383, 398 (1914)). The Supreme Court has repeatedly held that "this judicially created rule is 'designed to safeguard Fourth Amendment rights generally through its deterrent effect.'" *Id.* at 139-40 (quoting *United States v. Calandra,* 414 U.S. 338, 348 (1974)).

In support of its argument that the exclusionary rule should not be utilized in this case, the Government cites *Hudson v. Michigan*, 547 U.S. 586 (2006). *See* Doc. 45 at 12-13, 35). While *Hudson* addresses the exclusionary rule, its discussion arose in an entirely different context: a violation of the "knock-and-announce" rule. The facts at issue in *Hudson* are so markedly different from those in the present case that it is of little help.

In *Hudson*, there were no concerns—as there are here—with the warrant itself. *See Hudson*, 547 U.S. at 592 ("In this case, of course, the constitutional violation of an illegal *manner* of entry was *not* a but-for cause of obtaining the evidence. Whether that preliminary misstep had

occurred *or not,* the police would have executed the warrant they had obtained, and would have discovered the gun and drugs inside the house") (emphasis in original). Because there were no concerns about the warrant itself, the Court easily concluded that the manner in which law enforcement executed the warrant did nothing to alter the fact that law enforcement was permitted to enter and seize the evidence described in the warrant. *See id.* at 594 ("What the knock-and-announce rule has never protected, however, is one's interest in preventing the government from seeing or taking evidence described in a warrant. Since the interests that *were* violated in this case have nothing to do with the seizure of the evidence, the exclusionary rule is inapplicable") (emphasis in original).

Duggar's argument here has nothing to do with the manner in which law enforcement entered the business premises. As such, authority analyzing the applicability of the exclusionary rule in the context of a defective warrant is far more illuminating.

In *United States v. Hamilton*, 591 F.3d 1017 (8th Cir. 2010), the Eighth Circuit discussed the Supreme Court's decision in *Herring v. United States*, 555 U.S. 135 (2009). The Eighth Circuit noted that *Herring* counseled that the exclusionary rule should not be applied in situations arising from "nonrecurring and attenuated negligence" but that the exclusionary rule should be utilized "to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Hamilton*, 591 F.3d at 1029 (quoting *Herring*, 555 U.S. at 145).

Here, as discussed *supra*, there was deliberate, reckless, and/or grossly negligent conduct by law enforcement in obtaining the warrant. Specifically, the affiants provided false and misleading statements to the magistrate and omitted material facts—and they did so deliberately, recklessly and, at a minimum, with gross negligence.

For example, the affidavit in support of the relevant search warrant represented to the magistrate that that the "marrissa.zip" file was "successfully downloaded." *See* Doc. 37-2. But this is not true. Instead, an *accurate* statement would have been that the zip file contains 405 files but only 66 of these files were allegedly present on a device utilizing a business' IP address, and after 17 hours and 169 attempts, only 13 of those pieces were downloaded. Against this backdrop, it is remarkable that a federal agent would represent, under oath, that this file was "successfully downloaded."

Also, as discussed above, the affidavit left out material facts, depriving the magistrate of necessary information which would have provided important context to the issue of whether probable cause for issuance of a search warrant existed. Specifically, the affidavit leaves out that the used car dealership law enforcement sought to search was a business that regularly catered to the general public and that consistently had transient workers and employees. And the affidavit leaves out that the used car dealership law enforcement sought to search may have had unsecured Wi-Fi.

These misrepresentations and omissions were either deliberate, reckless, or grossly negligent and deprived the magistrate of the ability to meaningfully determine whether probable cause existed for issuance of a broad search warrant of the business. As such, this Court should apply the exclusionary rule as a deterrent to prevent law enforcement from continuing to play fast and loose with the Fourth Amendment.

B. The Good Faith Exception Does Not Apply

The Government argues that suppression is not warranted because law enforcement "acted in good faith in relying on the issuance of the search warrant." Doc. 45 at 39. But the Government also acknowledges that the good faith exception to the Fourth Amendment's warrant requirement

is categorically inapplicable in certain situations. *Id.* As relevant here, the exception does not apply "if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth." *United States v. Leon*, 468 U.S. 897, 923 (1984) (citing *Franks v. Delaware*, 438 U.S. 154, (1978)).

In this case, the Court's holding in *Leon* makes perfectly clear that the good faith exception is of no use to the Government. As already covered at length, the magistrate was misled by information in the affidavit which the affiant knew was false or should have known was false. While the false statements in the affidavit entitle Duggar to a *Franks* hearing and make clear that the exclusionary rule should be applied in this case, the false statements also render any reliance on the good faith exception unwarranted.

Moreover, the Supreme Court notes that the good faith exception only applies "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. Here, not only would the warrant not have issued if law enforcement was honest in its affidavit, but law enforcement has also not "acted within its scope." *Id.*

As discussed, the devices at issue in this case were seized pursuant to a warrant signed on November 4, 2019 which expressly required that it be executed within 14 days. And while the Government seized the devices within that timeframe, it did not search those devices and seize items pursuant to the limitations set out in Attachment B to the warrant until months and even years after the deadline. And, HSI has still never filed an inventory of items seized from any subsequent search of any particular computer or electronic device or hard drive.

In his affidavit in support of the Second Search Warrant, SA Faulkner stated that searching computer storage devices "can take up to several months to complete" and sought "authorization 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" and that "[i]f 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." *See* Doc. 37-2. However, after several months transpired, HSI did not request that the magistrate judge give it any additional time beyond the time frame specified in the warrant—and only requested that HSI be permitted to conduct the particularized searches offsite. Troublingly, investigators have apparently continued to perform searches of the devices until at least April 2021. And the Government did not timely return, as the warrant requires, any data that "has been seized that does not constitute evidence of the crimes detailed herein." *Id.*

Where, as here, an affidavit misleads a magistrate and where the Government fails to act within the scope of a warrant, the Supreme Court has made clear that the good faith exception is not to be applied.

VII. Conclusion

Based on the foregoing, Duggar respectfully requests that this Court enter an Order (1) suppressing all evidence seized from 14969 Wildcat Creek Road in Springdale, Arkansas, on November 8, 2019; (2) suppressing all evidence that was derived from information or items obtained during the search pursuant to the fruit of the poisonous tree doctrine; and (3) setting this matter for an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978).

Respectfully submitted,

Margulis Gelfand, LLC

/s/ Justin K. Gelfand
JUSTIN K. GELFAND, MO Bar No. 62265*
7700 Bonhomme Ave., Ste. 750
St. Louis, MO 63105
Telephone: 314.390.0234
Facsimile: 314.485.2264
justin@margulisgelfand.com
Counsel for Defendant
**Admitted Pro Hac Vice*

--- *and* ---

Story Law Firm, PLLC

/s/ Travis W. Story
Travis W. Story, AR Bar No. 2008278
Gregory F. Payne, AR Bar No. 2017008
3608 Steele Blvd., #105
Fayetteville, AR 72703
Telephone: (479) 448-3700
Facsimile: (479) 443-3701
travis@storylawfirm.com
greg@storylawfirm.com

Certificate of Service

I hereby certify that the foregoing was filed electronically with the Clerk of the Court to be served by operation of the Court's electronic filing system upon the Office of the United States Attorney.

/s/ Justin K. Gelfand
JUSTIN K. GELFAND, MO Bar No. 62265*
7700 Bonhomme Ave., Ste. 750
St. Louis, MO 63105
Telephone: 314.390.0234
Facsimile: 314.485.2264
justin@margulisgelfand.com
Counsel for Defendant
**Admitted Pro Hac Vice*