

**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 DISMISS FOR FAILURE TO PRESERVE
POTENTIALLY EXCULPATORY EVIDENCE**

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 Dismiss for Government's Failure to Preserve Potentially Exculpatory Evidence," (Doc. 40), states:

BACKGROUND

At approximately 3:00 PM on November 8, 2019, law enforcement executed a federal warrant to search the defendant's used car dealership in Springdale, Arkansas. The warrant authorized law enforcement to search the car lot and the two small, shed-like structures on the lot based on evidence that the user of the Internet Protocol ("IP") address assigned to the lot shared child sexual abuse material over a peer-to-peer network in May 2019. When the law enforcement officers arrived at the premises, they found the defendant, who had owned the dealership since approximately 2018, and two other individuals. Law enforcement determined that one of these individuals—identified as "Witness #3" in the defendant's motion—worked at the car lot and interviewed him. (Doc. 40 at 4). The individual told law enforcement that he began working at the defendant's car lot in June 2019, that he did not access the internet at work, and that the

computer in the office on the car lot belonged to and was only used by the defendant.¹ This individual also told law enforcement that he was very inexperienced with computers and did not have social media accounts. After obtaining his consent, law enforcement manually reviewed the contents of the individual's phone on scene without the use of a forensic tool, found no evidence of criminal activity on it, and returned the device to this individual.

Following the execution of the search warrant, law enforcement interviewed multiple individuals in connection with this investigation. One of these individuals—referred to as “Witness #1” in the defendant's motion—was interviewed on December 16, 2019. (Doc. 40 at 3). This individual told law enforcement that he had purchased multiple vehicles from the defendant but denied ever entering the small office on the defendant's car lot without an employee present. He demonstrated no familiarity with peer-to-peer file-sharing programs and said that he was not in the vicinity of the car lot in May 2019. During the interview, the individual allowed law enforcement to manually review the contents of his cell phone, which he had recently purchased in approximately October 2019, without the use of a forensic tool. Law enforcement found no evidence of child sexual abuse material on the phone and returned the device to this individual.

On December 20, 2019, law enforcement interviewed another individual, referred to in the defendant's motion as “Witness #2.” (Doc. 40 at 4). During the interview, the individual advised that he worked at the defendant's car lot from 2017 to approximately September 2018, after which he left to start his own business. This individual told law enforcement that the internet at the car lot was password-protected and therefore not accessible to the public. He acknowledged using the

¹ According to records obtained from the defendant's business, this individual received his first paycheck from the defendant on May 31, 2019. There are no records of payment to any employees who worked at the dealership on May 14 or May 15, 2019, when the user of the lot's IP address was sharing child sexual abuse material over the BitTorrent peer-to-peer network.

defendant's computer when he worked at the car lot but demonstrated no familiarity with peer-to-peer file-sharing programs and denied ever accessing pornography on the computer. He also advised law enforcement that the defendant's computer at the car lot had a program known as "Covenant Eyes" installed on it, which would notify the defendant's wife if the device was used to view pornography, and that the defendant told him he struggled with a pornography addiction. Finally, this individual reported that he did not believe "Witness #1" was computer savvy, and that "Witness #1" had never mentioned using peer-to-peer file-sharing software. This individual also allowed law enforcement to examine his cell phone during the interview. Law enforcement observed no evidence of child sexual abuse material during this examination and returned the device to the individual afterwards. Law enforcement did not create a forensic report or a forensic image of the device. Since speaking with this individual, law enforcement has reviewed information indicating that he was incarcerated for the entire timeframe in May 2019 when the user of the car lot's IP address was sharing child sexual abuse material online.

Evidence recovered from the defendant's electronic devices seized during the execution of the search warrant—including his Apple iPhone, his laptop computer, and his desktop computer in the small office on the lot—has established that the defendant was on the lot in May 2019 when his IP address was used to distribute child sexual abuse material over a peer-to-peer network and used the computer in the small office on the lot to download child sexual abuse material.

ARGUMENT

The defendant now moves to dismiss the indictment in its entirety, arguing that the government was required to seize for him the above three individuals' cell phones—in two instances without any semblance of legal process—extract all the data and content from those devices, and produce the complete forensic image copies of those devices to him. (Doc. 40). The

defendant asserts that the forensic image copies of these phones might have contained information indicating whether the owners of the devices used the Dark Web or peer-to-peer file-sharing software and might contain metadata that would establish that the devices were in the vicinity of the car lot when the defendant's computer was used to download child sexual abuse material. (Doc. 40 at 7). According to the defendant, the fact that the government has not provided him with the forensic image copies and developed his defense for him constitutes a due process violation that can only be remedied by dismissal of all criminal charges against him.

The defendant is incorrect. The government cannot produce what it does not possess, and the defendant's suggestion that the government somehow failed to preserve forensic image copies is baseless. As detailed above, two of these phones were manually reviewed, which could not result in the creation of a forensic image copy, and the third was not imaged either. But even assuming for the sake of argument that the opportunity to collect information qualifies as constructive possession of that information, the defendant has failed to establish that his due process rights were violated by the absence of these three forensic images under controlling Eighth Circuit precedent because (1) the image copies have no apparent or potential exculpatory value, (2) because law enforcement did not act in bad faith, and (3) comparable evidence is reasonably available to him. In fact, because of law enforcement's efforts to thoroughly investigate this matter, the government has reason to believe that none of the three individuals were present on the defendant's car lot when his computer was used to download child sexual abuse material, fatally undermining his current claims. Accordingly, his motion should be denied.

I. The Government Cannot Preserve Evidence that it Does Not Possess

As an initial matter, the defendant's motion incorrectly frames the issue. The government did not seize the cell phones belonging to the three individuals identified in his motion, nor did it

use any forensic tools to create forensic image copies of these devices.² Indeed, the government had no reason to seize those phones or create those images. There was no evidence that these individuals were present on the car lot in May 2019 and reviews of their phones uncovered no evidence of child sexual abuse material. In fact, as discussed above, there is significant evidence that these individuals were not on the car lot at the relevant time. The information gleaned from these individuals has been documented in reports provided to the defendant, along with recordings of the interviews of these individuals. And, of course, the government advised the defense that no forensic image copies of these devices were created during the investigation. (Doc. 40 at 5). Put simply, the government cannot preserve what it does not have—in this case, forensic images of various cell phones belonging to individuals who were not present on the car lot during the relevant timeframe—and the government had no obligation to take investigative steps based on what the defendant might want at some later date. See *United States v. Natson*, 276 F. App'x 933, 934–35 (11th Cir. 2008) (rejecting defendant's speculation that the government “intentionally” refused to develop evidence related to other suspects and noting that “the prosecution is not required to disclose evidence it does not possess” or “develop exculpatory evidence for the defense”).³

² The defendant claims in another motion that the government treated the warrant to search his used car dealership as “*carte blanche* authority to storm into the business nearly six months later, seizing everything in sight,” Doc. 37 at 14, which is of course irreconcilable with his criticisms of the government's investigation during the search in the instant motion.

³ See also *United States v. Kraemer*, 810 F.2d 173, 178 (8th Cir. 1987) (denying request to overturn conviction based on defendant's belief that potentially exculpatory evidence “was ‘available’ to the government and that they ‘could have checked’” to see if it was obtainable); *United States v. Riley*, 657 F.2d 1377, 1386 (8th Cir. 1981) (“While *Brady* requires the Government to tender to the defense all exculpatory evidence in its possession, it establishes no obligation on the Government to seek out such evidence.” (quoting *United States v. Walker*, 559 F.2d 365, 373 (5th Cir. 1977))).

A review of the case that the defendant primarily relies upon in his motion—*United States v. Zaragoza-Moreira*, 780 F.3d 971 (9th Cir. 2015)—confirms that he has misapprehended the issue. In *Zaragoza-Moreira*, 780 F.3d at 976–82, the Ninth Circuit found a defendant’s due process rights were violated where law enforcement recorded over a video of the defendant’s arrest solely in its possession despite her formal request to preserve it. In that case, the video was critical to corroborating a duress defense and her claim that she intentionally attracted the attention of law enforcement when she was arrested to get help. *Id.* at 978–80. In this case, on the other hand, the government did not save over or delete the forensic image copies of the three phones because, as both parties know, there was no reason to create forensic images of those devices in the first place and that asserted evidence did not exist.⁴

At base, then, the defendant’s motion is nothing more than an after-the-fact criticism of an investigation that has resulted in federal child sexual exploitation charges against him—criticism that he will no doubt seek to inject into the trial in this matter, should this case proceed that far. His perceived dissatisfactions with the investigation, however, are not grounds for dismissal of the indictment. Accordingly, his motion should be denied.

II. Even Assuming that the Government Constructively Possessed the Evidence the Defendant Now Seeks, the Defendant’s Due Process Rights Were Not Violated

Even assuming, *arguendo*, that the government constructively possessed the evidence that is the subject of the defendant’s instant motion—that is, the forensic image copies of the cell phones—his motion should be denied because his due process rights were not violated by the absence of that evidence. As the Eighth Circuit explained, “[u]nless the defendant can show bad

⁴ Based on the defendant’s motion, it appears that he may be asserting an alibi defense. The government has received no notice of his intent to introduce such a defense and formally requests that the defendant notify the government of any intended alibi defense pursuant to Federal Rule of Criminal Procedure 12.1(a).

faith on the part of law enforcement, ‘failure to preserve potentially useful evidence does not constitute a denial of due process of law.’” *United States v. Boswell*, 270 F.3d 1200, 1207 (8th Cir. 2001); *see also United States v. LeBeau*, 867 F.3d 960, 976–77 (8th Cir. 2017) (“Law enforcement’s failure to preserve potentially exculpatory evidence violates due process if the defendant can show that law enforcement acted in bad faith.”). “Moreover, the evidence must have had apparent exculpatory value and comparable exculpatory evidence must not have been reasonably available to the defendant.” *United States v. Webster*, 625 F.3d 439, 446 (8th Cir. 2010) (internal citations omitted). The Due Process Clause does not, however, “impos[e] on the police an undifferentiated and absolute duty to retain and to preserve all material that might be of conceivable evidentiary significance in a particular prosecution.” *Arizona v. Youngblood*, 488 U.S. 51, 58 (1988); *see also California v. Trombetta*, 467 U.S. 479, 488 (1984) (limiting duty to preserve evidence to evidence that “might be expected to play a significant role in the suspect’s defense.”).

Here, the defendant has failed to establish that the asserted evidence was apparently or potentially exculpatory, that the government acted in bad faith, and that the evidence is otherwise unavailable. With respect to the first prong, there was and continues to be no reason to believe that the three phones referenced in the defendant’s motion contained exculpatory information. As explained above—but omitted from the defendant’s motion—law enforcement had no reason to believe that any of the three individuals or their cell phones referenced in the defendant’s motion were present on the car lot in May 2019 when the defendant’s IP address was sharing child sexual abuse material online and when the defendant’s computer was used to download from the internet such material. Subsequent investigation has only corroborated that belief.

With respect to the individual identified by the defendant as “Witness #1,” for example, this individual denied being at the car lot in May 2019 and demonstrated no familiarity with peer-to-peer networks—a stark contrast from the information the defendant provided to law enforcement regarding his familiarity with both peer-to-peer networks and the Dark Web during his voluntary interview. This individual also consented to a manual review of his phone, which he informed law enforcement he obtained in October of 2019, and law enforcement discovered nothing of evidentiary value during this manual review. As a result, his phone was not seized, and a forensic image of the device was not created.

With respect to the individual identified by the defendant as “Witness #2,” this individual informed law enforcement that he stopped working at the defendant’s car lot in 2018 to start his own business—a fact corroborated by other evidence. He similarly denied having any familiarity with peer-to-peer networks and advised law enforcement that the defendant’s computer at the car lot had a program known as “Covenant Eyes” installed on it, which would alert the defendant’s wife if the device was used to view pornography. In explaining this detail, this individual noted that the defendant told him he struggled with a pornography addiction. Finally, this individual likewise consented to a search of his cellular phone, which was completed on scene. The examination consisted of a forensic review, which uncovered no evidence of child sexual abuse material and did not result in the creation of a forensic report or image copy of the data on the device. Law enforcement has since received information that this individual was incarcerated during the period charged in the indictment, which is the same period in which the defendant’s IP address was used to share child sexual abuse material online.

Finally, with respect to the individual identified by the defendant as “Witness #3,” this individual advised law enforcement during a voluntary interview that he began working for the

defendant in June 2019, after the defendant's IP address was used to share child sexual abuse material on the BitTorrent peer-to-peer network. Records obtained from the defendant's business confirm that this individual was not working at the defendant's car lot during the relevant timeframe. Further, this individual also demonstrated an extremely limited familiarity with computers, and a manual review of his cell phone during his voluntary interview uncovered no evidence of child sexual abuse material.

In light of the above, there is no reason to conclude that image copies of these three individuals' phones might contain exculpatory information—including, as the defendant hypothesizes, evidence related to the BitTorrent peer-to-peer file-sharing network, the Dark Web, and geolocation data placing the devices on the car lot on May 14 and May 15, 2019 (*see* Doc. 40 at 7). There is ample reason, however, to conclude that they do not contain such evidence. In other words, law enforcement had no reason to seize and forensically image these three phones, as all available evidence made clear that they contained nothing of evidentiary value. The defendant's retrospective insistence that they might contain some helpful information is simply wishful speculation and is entirely unsupported by the actual evidence in this case.

Second, there is no evidence to conclude that the government acted in bad faith. The defendant has failed to offer proof of an "official animus" or a "conscious effort to suppress exculpatory evidence." *Trombetta*, 467 U.S. at 488; *see also United States v. Red Bow*, 851 F. Supp. 2d 1176, 1180 (D.N.D. 2012) ("[I]n the context of criminal law and circumstances where the government failed to preserve evidence, bad faith is required rather than negligence, gross negligence, or recklessness."). Law enforcement did not, for example, intentionally erase or delete evidence in its possession, and the defendant has not claimed that it did. Nor did law enforcement fail to thoroughly investigate this case or seek to conceal its investigative efforts from the

defendant. Indeed, the defendant's motion is based entirely on information he has learned through the many reports and recordings prepared by law enforcement and produced in discovery.

Further, because of the thoroughness of law enforcement's investigation, the government has obtained evidence indicating that none of the three individuals identified in the defendant's motion were present on the car lot in May 2019, when the defendant's IP address was used to share child sexual abuse material online and when his computer was used to download such material. The government has also obtained and provided to the defense evidence establishing that the defendant was present on the car lot at this time. Indeed, the car lot belonged to the defendant and, based on his own business records, he appears to have been the only paid employee on the dates his computer was used to download child sexual abuse material. Forensic evidence recovered from his devices further confirms that he was, in fact, on the car lot when his computer was used to download child sexual abuse material. Rather than confronting this evidence, the defendant is seeking the extraordinary remedy of dismissal of the entire indictment against him based on his complaint that the government failed in 2019 to predict the exact contours of his defense strategy in 2021 and tailor its investigation to support that strategy. While an unsurprising litigation tactic, this sort of retrospective critique on the part of the defendant falls well short of satisfying his burden of proving that the government acted in bad faith, and his motion should be denied.⁵

As a final matter, the defendant has failed to address whether comparable evidence is reasonably available to him. *Webster*, 625 F.3d at 446. While the defendant's motion relies

⁵ The bad-faith analysis in particular lays bare the improper framing of the defendant's current claim. By equating the government's failure to conduct an investigation to suit his eventual defense with the failure to preserve evidence, the defendant is asking this Court to adopt a framework that would impose an insurmountable burden on the government's ability to investigate violations of federal criminal law and would permit defendants to obtain dismissals of indictments against them in virtually every case. The Court should therefore deny the defendant's motion.

primarily upon his own conclusory assertions regarding the exculpatory value of the information he now seeks, it appears that he believes that the forensic image copies of the three phones might contain geolocation data placing the devices on the car lot when his computer was used to download child sexual abuse material. (Doc. 40 at 7). Setting aside the ample evidence establishing that the owners of these phones were not on the car lot at that time—as well as the similarly ample evidence establishing that the defendant was on the car lot at that time, which would place him in the best position to prove those individuals’ presence on the car lot—he will have the opportunity at trial to present evidence through cross-examination and his own case, should he choose to present one, establishing that he was not the only individual who had access to the lot. Under these circumstances, dismissal of the indictment is unwarranted, *See United States v. Farmer*, 312 F.3d 933, 936 (8th Cir. 2002) (finding, in case in which a firearm that was not fingerprinted was destroyed before trial, that the defendant could not establish a due process violation because he “successfully presented the fact that the gun had not been fingerprinted to the jury; yet, the jury found a link between [appellant] and the firearm” and the evidence was therefore not “favorable to the defendant” or “material to the issue of his guilt”); *see also United States v. Bloomgren*, 42 F. App’x 147, 151 (10th Cir. 2002) (“Comparable evidence was presented at trial to show that others had access to the Ranch. . . . A police officer testified at trial that he found both men's and women's clothing in the house. The police did not destroy these items; they simply did not seize them. The presentation of this evidence means that the failure to collect [the clothing] simply was not prejudicial.”). Accordingly, the defendant’s motion should be denied.

CONCLUSION

For the foregoing reasons, the United States respectfully requests that the Court deny the defendant's "Motion to Dismiss for Government's Failure to Preserve Potentially Exculpatory Evidence," (Doc. 40).

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