

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS**

UNITED STATES OF AMERICA,

Plaintiff,

vs.

Case No. 20-10028-11, 15, 19-EFM

KEVIN LEWIS,
OTIS PONDS, and
TRAVIS VONTRESS,

Defendants.

MEMORANDUM AND ORDER

The Government, in the course of its investigation into the alleged drug trafficking organization at the heart of this case, made three successive applications for wiretaps, each of which was granted. The three wiretaps each lasted about a month and essentially ran back-to-back—with about a week in between the end of one and the beginning of the next—from mid-April to mid-July of 2019.

The first wiretap authorized law enforcement to intercept communications on one phone used by Defendant Dorzee Hill. The second permitted continued interception on the first phone and began interception on two new phones—another phone used by Hill and a third phone used by Defendant Mario Ponds. The third wiretap permitted continued interception on Hill's two

phones and authorized the initial interception of a phone used by Defendant Travis Knighten. Knighten had somehow come to possess this phone while he was incarcerated in an Oklahoma State Penitentiary in McAlester, Oklahoma.¹

Defendants Orlando Hogan, Knighten, and Kevin Lewis moved to suppress communications and other evidence derived from the three wiretaps (Docs. 555, 558, and 564).² Each of these motions was joined by a variety of co-Defendants. Lewis and Otis Ponds joined in Hogan's motion, Lewis and Travis Vontress joined in Knighten's motion, and Vontress and Ponds join in Lewis's motion. Naturally, this complicated web of motions, joinders, and intermittent pleas leaves the active players with respect to these motions about as clear as mud. In short, Kevin Lewis, Travis Vontress, and Otis Ponds still challenge the validity of the wiretaps. After a hearing on this matter on February 10, 2022, the Court agrees with the Government that its applications and wiretap procedures satisfied the requirements of Federal law, and therefore denies Defendants' motions.

I. Factual and Procedural Background

A. First Wiretap

The Government sought approval for its first wiretap beginning in early spring of 2019. As part of this process, an application was made to the Department of Justice seeking authorization by a statutorily approved person. On April 5, 2019, a memo was sent from Brian A. Benczkowski, Assistant Attorney General in the Criminal Division, to the Assistant United States Attorney now prosecuting this case, confirming that Bruce C. Schwartz, Deputy Assistant Attorney General for

¹ All of these Defendants have now entered guilty pleas.

² Hogan and Knighten, having both pled guilty, now withdraw their motions as to themselves

the Criminal Division, authorized the application. That memo included a signature block identical to the following:

Brian A. Benczkowski
Assistant Attorney General
Criminal Division

APR 05 2019

Date



BRUCE C. SWARTZ
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

The Government thereafter presented the wiretap application to United States District Court Judge John W. Broomes, who authorized the wiretap on April 9, 2019.

This wiretap only covered interception of communications as to one cell phone, used by Defendant Dorzee Hill (“TT1”), and provided for monitoring from April 10, 2019, to May 9, 2019. The Government, through its wiretap, targeted the suspected drug trafficking activities of several named individuals, including Kevin Lewis, and sought evidence as part a larger investigation into the suspected drug trafficking organization operated by these individuals. In its application to Judge Broomes, the Government offered an affidavit from FBI Special Agent Cameron Heath, the

case agent for the overarching investigation. At the hearing on this motion, Agent Heath also testified in great detail regarding the applications.³

Agent Heath, in his affidavit, laid out the facts available to him that he believed showed probable cause to believe that Hill was using TTI in the commission of a host of drug trafficking offenses. Largely, Agent Heath focused on controlled buys made by the FBI's Confidential Human Source ("CHS") from Defendant Hill. Several of these transactions involved an intermediary, not indicted in this case, who would arrange the transactions with Hill. The CHS informed investigators that the intermediary contacted Hill by calling or texting him at TT1 to arrange a transaction, which investigators were able to corroborate through toll records. The CHS also transacted directly with Hill and his female companion in two purchases, during which the CHS communicated with Hill at TT1 to set the buy. These texts were also corroborated by toll records, and by investigators review of the CHS's phone after the fact. During each of these transactions, the CHS purchased between ¼ and 1 gram of heroin for between \$1,000 and \$2,600.

Agent Heath's affidavit also described, in great detail, why the wiretap was necessary to meet the goals of the investigation. Broadly speaking, the goal of the investigation was to "identify and subsequently dismantle the entire DTO," or drug trafficking organization. Other investigative techniques, even if used in tandem, were believed to be unequal to this task without the assistance of wiretaps. The controlled buys discussed above, for instance, did not permit agents to gain a larger picture about the suspected DTO, as Hill proved unwilling to discuss other suspected members with the CHS or to open up contact between the CHS and other members.

³ To be clear, in determining the sufficiency of the Government's wiretap applications regarding probable cause and necessity, the Court only considers the information then before the issuing Judge. This is limited to the information relayed in Agent Heath's affidavits as a part of the three applications.

Likewise, investigators believed physical surveillance of Hill had proved inadequate after numerous attempts. Agent Heath averred that this was because Hill lived on a dead-end street and his neighborhood was very sensitive to the presence of law enforcement, as investigators had been informed that Hill's family in the neighborhood was on the lookout and thus "suspicious" vehicles or persons would be easily discovered. Agent Heath had further been informed by Hill's U.S. Probation Officer, Chris Towner, that he had once been "burnt" when Hill's family member had noticed him in the neighborhood. When outside of his neighborhood, Agent Heath and other investigators noticed that Hill would often engage in counter-surveillance driving techniques that made him difficult to follow. These included using multiple different vehicles and making U-turns and turns quickly and without signaling. He would also take routes that caused him to double back and would take circuitous routes to and from his home. The affidavit reported that, as a result, investigators lost sight of Hill on five separate occasions. Because of these difficulties, Agent Heath's affidavit relayed concern that further efforts at physical surveillance alone would either prove fruitless or would lead to detection by Hill and other members of the DTO.

Investigators also used pole cameras to investigate Hill and the suspected DTO.⁴ A pole camera was covertly placed on a utility pole outside Hill's house by FBI technical agents, and thereafter began recording 24/7. Agent Heath averred that this camera was useful to identify persons going in and out of Hill's house and was further useful once investigators began engaging in controlled buys from Hill. Once a controlled buy was set, investigators could watch Hill more closely to determine his routine during a transaction, as well as the CHS's behavior. But the camera also had its limitations. Agent Health noted that the pole camera largely could not capture

⁴ The use (or misuse) of pole cameras in this case is the subject of another Order of this Court, dated February 16, 2022.

any evidence of criminal conduct unless it occurred out in the open on Hill's front lawn, and thus was limited in its value in building a case against other members of the suspected DTO.

Similarly, GPS tracking did not supply the information investigators needed to identify the scope of the suspected DTO and gather evidence on its suspected members. Agent Heath averred that GPS tracking of Hill's phone, approved by a search warrant from United States Magistrate Judge Gwynne Birzer, yielded little fruit. Apparently, Hill did not often leave his house, so the information gathered—that Hill was in his house—was largely useless. When he did leave his house, investigators had difficulty using GPS tracking to follow Hill, as the GPS would only ping every 15 minutes and it often returned location errors or would “fail to locate” Hills device. Investigators would then converge at a pinged location only to find that Hill had already left. Agent Heath also stated that GPS tracking could not accomplish the investigation's ultimate goal, which was to identify and dismantle the *entire DTO*. Unless Hill had physical contact with the entire DTO, tracking only him would not allow them to reach this goal.

In addition, the affidavit notes that searches of financial databases yielded nothing of value, as investigators could find no evidence of the large-scale movement of money that is typically associated with a DTO. Grand jury subpoenas targeted at obtaining the accounting and financial information of the suspects were similarly unsuccessful.

Several investigative tactics, though available, were deemed unlikely to succeed by Agent Heath and other investigators. For instance, investigators were dissuaded from using undercover agents by the CHS, who believed any such agents would not have access to Hill and that introducing undercover agents might endanger the CHS. Trash pulls were also ruled out. They were deemed too risky at Hill's house because of the same reasons physical surveillance was unsuccessful, and were not tried at a purported stash house because the house was in a shared

triplex and it would have been difficult, if not impossible, to tie any particular trash to a particular residence. Agent Heath averred that mail covers were not used because there was no indication the DTO was using the U.S. Postal Service in furtherance of their suspected activities.

Ultimately, the Government's application and Agent Heath's affidavit were sufficient to convince Judge Broomes to authorize the wiretap. Once authorized, investigators set up their listening post in Wichita, Kansas. But before they could begin intercepting calls and messages, Agent Heath testified that the Assistant United States Attorney assigned to the case required agents to undergo training regarding minimization. Simply put, minimization is the process by which investigators self-limit the calls and texts they intercept that are unrelated to criminal activity. Agents received both written and oral guidance on proper minimization procedures, and agents were required to attend training and review written materials prior to intercepting calls or texts.

On May 9, 2019 at 11:59 P.M., the monitoring period for the first wiretap ended. The next day, a Friday, the data was downloaded onto Blu-ray discs in Dallas, Texas, and sent via federal express mail to the FBI Field Office in Kansas City, Kansas. Agent Heath testified that while the investigator listening post was located in Wichita, Kansas, the servers to store all of the data were located in Dallas because the FBI deems it too expensive to have servers in every regional field office. Agent Heath also testified that the Dallas office sent the discs to Kansas City first because Kansas City is the headquarters for all FBI offices in the District of Kansas. The discs arrived in Kansas City on Monday, May 13, and were sent to the Wichita office the same day. On May 14, Agent Heath received the discs, and the application and order for sealing were prepared and sent to Judge Broomes. The discs were sealed the next day, May 15.

B. Second Wiretap

Investigators sought and were granted a second wiretap on May 17, 2019. This wiretap was for the continued interception of Hill's TT1, and the initial interception of TT2 and TT3. TT2 was a phone also used by Hill and TT3 was a phone used by Defendant Mario Ponds. Similar to the first application, investigators sought to further understand the contours of the suspected DTO and gather evidence on its many members.

Agent Heath again averred that investigators had probable cause to suspect the three target telephones were being used in the commission of suspected drug trafficking offenses. In support of this statement, Agent Heath detailed around 30 calls intercepted during the first wiretap. These calls helped identify that, based on the experience and knowledge of investigators, TT3 was used by Mario Ponds in drug transactions with Hill. Investigators also used toll records to learn that that Hill used TT2 to call an unindicted co-conspirator after the CHS requested to purchase drugs. The unindicted co-conspirator would then sell drugs to the CHS, which investigators confirmed via pole camera footage and through debriefs with the CHS after the transaction.

Agent Heath stated this second wiretap was again necessary to fully investigate the DTO. For this conclusion, Agent Heath relied on largely the same statements made in the first wiretap application, with some minor updates resulting from investigators' experience during the period of the first wiretap. For instance, investigators determined that Mario Ponds, like Hill, was extremely surveillance conscious, as he was known to use multiple vehicles. Investigators also found more evidence that Hill's neighborhood was surveillance conscious, as they overheard a conversation between Hill and another person about a suspicious vehicle in their neighborhood. This vehicle, as it turned out, was an FBI surveillance vehicle. It seemed to investigators that physical surveillance would remain unequal to the task of investigating the DTO.

The second wiretap ended on Sunday, June 16, 2019, at 11:59 P.M. On Tuesday, June 18, the data was downloaded in Dallas and sent to Kansas City. Agent Heath testified that he was not certain of the cause of this one-day delay, but said it may have been related to workload in the Dallas office. The discs were received in Kansas City on June 19 and shipped to Wichita that same day. The discs were received by Agent Heath in Wichita on June 20, and they were presented to Judge Broomes for sealing the next day.

C. Third Wiretap

The third and final wiretap was authorized on June 21, 2019. Agents began interception that same day. This wiretap was for the continued interception of Hill's phones, TT1 and TT2, and for the initial interception of a phone used by Defendant Travis Knighten, TT4. Knighten was, at all times relevant to the investigation, incarcerated in an Oklahoma State Penitentiary in McAlester, Oklahoma.

To show probable cause, Agent Heath cited around another 30 calls intercepted during the previous wiretaps and discussed his belief that those calls were drug-related, based on his training and experience. The majority of these were calls involving TT1 and TT2, as well as a different phone used by Knighten. Investigators learned from a confidential informant that, after a search warrant executed on May 31, 2019 at one of the DTO's suspected stash houses, Knighten had switched telephones and began using TT4. This was confirmed by toll records showing that TT4 was in contact with identified co-conspirators and an intercepted conversation in which Knighten, using TT4, confirmed to Hill that TT4 was his new number.

The necessity portions of the third applications largely tracked the first two, but also contained additional information on Knighten. In essence, Agent Heath stated Knighten was suspected to be the highest-ranking member of the DTO and stated that interception on TT4 was

necessary because Knighten had contact with other members of the organization with whom Hill did not have contact. Interception of TT4 was therefore necessary to see the whole organization, rather than just pieces of it. Because Knighten appeared to have the assistance of Oklahoma State Correctional personnel, investigators did not believe they would be able to gain access to him or learn about him through correctional personnel without risking the investigation. It also appeared to investigators that, because Knighten was in prison, the primary way with which he communicated with other members of the DTO was by telephone, and therefore only a wiretap on his cellphone would allow investigators to identify the full extent of the DTO and its members.

During the interception period for the third wiretap, investigators intercepted 3,311 phone calls. Approximately 76 of these are called into question by Knighten's motion. During the hearing, Agent Heath went through each of these calls in detail and testified that only one of them was improperly not minimized. Many of the others were shown to have discussed Knighten's construction business, which was believed to be a means for laundering money made through drug trafficking activities. Money laundering was listed by investigators as one of the Target Offenses for the third wiretap application.

The third wiretap ended on Saturday, July 20, 2019, at 11:59 P.M. On Monday, July 22, the data was downloaded on to discs at the Dallas hub and sent to Kansas City. The discs arrived in Kansas City on July 23. They were shipped to Wichita on July 24, and Agent Heath received them on Friday, July 26. The discs were presented to Judge Brooms for sealing on Monday, July 29.

II. Discussion

Together, these three motions raise a plethora of legal issues that Defendants believe plagued the process used by the Government to obtain and execute the three wiretaps discussed

above. This process finds its legal foundation in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986,⁵ which governs the use of wiretaps at the federal level. Defendants contend that (1) each of the three wiretap applications failed to establish probable cause; (2) the use of wiretaps was not shown to be necessary; (3) the Court lacked jurisdiction to authorize interception as to TT4; (4) agents failed, during the third wiretap, to properly minimize intercepted communications that were unrelated to unlawful activity; (5) the communications intercepted were not immediately sealed; and (6) the initial wiretap was not authorized by a statutorily approved person.⁶ The Court examines each of Defendants' claims in turn.⁷

A. Probable Cause

The remaining Defendants challenge probable cause as to each wiretap application. Before an application for a wiretap may be granted, the issuing judge must determine that “there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter” and that “there is probable cause for belief that particular communications concerning that offense will be obtained through such interception.”⁸ This essentially codifies Fourth Amendment probable cause principles, with the caveat that, under Title III, there must be probable cause that *certain crimes* have been or are being

⁵ 18 U.S.C § 2510 *et seq.*

⁶ The Government conceded at argument that these Defendants have standing to raise these issues.

⁷ Defendant Hogan's motion also raised the issue that the Attorney General's office did not properly authorize all three phones in the third wiretap application. Per the Court's instruction during arguments that any issues not raised by counsel would be waived, whether or not these issues were raised in briefing, this argument is waived and the Court does not consider it.

⁸ 18 U.S.C. § 2518(3)(a), (b). There is a third probable cause finding required in some cases, *see* 18 U.S.C. § 2518(3)(d), but Defendants do not dispute that issue here.

committed. There is a massive list of such crimes, but as relevant here, it includes possession of a controlled substance with intent to distribute, conspiracy and attempt to possess a controlled substance with intent to distribute, unlawful use of a communication facility to commit and facilitate the commission of drug trafficking offenses, and money laundering offenses.⁹

Other than this departure, probable cause standards remain unchanged. Probable cause exists where known facts and circumstances would lead a reasonable officer to believe there is a fair probability evidence of a crime will be found.¹⁰ The probable cause determination is a commonsense inquiry informed by the totality of the circumstances present in a particular case.¹¹ In a wiretap case, for instance, probable cause for a wiretap may be established through information about previously monitored conversations over the target telephone, telephone data linking the target telephone to drug trafficking activity, statements from confidential sources, physical surveillance or other evidence.¹² A reviewing court gives great deference to the issuing judge's determination of probable cause, for it is a determination based on common sense.¹³ This determination must be upheld if the warrant application and supporting affidavits provide a substantial basis for finding that probable cause existed.¹⁴

⁹ See 18 U.S.C. § 2516(1)(e).

¹⁰ See *Ornelas v. United States*, 517 U.S. 690, 696 (1996); *United States v. Biglow*, 562 F.3d 1272, 1281 (10th Cir. 2009).

¹¹ *United States v. Mathis*, 357 F.3d 1200, 1203–04 (10th Cir. 2004) (citing *Illinois v. Gates*, 462 U.S. 213, 230 (1983)).

¹² See *United States v. Apodaca*, 820 F.2d 348, 350 n.2 (10th Cir. 1987).

¹³ *United States v. Finnigin*, 113 F.3d 1182, 1185 (10th Cir. 1997).

¹⁴ See *Illinois v. Gates*, 462 U.S. 213, 236 (1983) (“Reflecting this preference for the warrant process, the traditional standard for review of an issuing magistrate’s probable cause determination has been that so long as the magistrate had a ‘substantial basis for . . . conclud[ing]’ that a search would uncover evidence of wrongdoing, the Fourth Amendment requires no more.”) (citation omitted).

The Target Offenses listed in each warrant application, largely offenses related to drug trafficking, fall within the purview of a Title III intercept.¹⁵ So the only inquiry that remains is whether Agent Heath's affidavit provided a substantial basis for concluding there was probable cause to believe that the target suspects had committed or were about to commit those offenses and that interception would provide particular communications concerning those offenses.

The Court has no trouble concluding each application was supported probable cause. The first wiretap application contained a detailed description of several controlled buys by the CHS from Hill, often through an intermediary. Investigators were able to confirm from toll records that Hill and the intermediary were in communication via TT1 after the CHS asked to buy narcotics. Toll records also confirmed the CHS's communications with Hill at TT1 to directly set up a narcotics purchase. After the buys, investigators were able to debrief the CHS to confirm the sale of narcotics actually took place, and to confirm the CHS's contacts with Hill and the intermediary. This provided a substantial basis to conclude that (1) Hill was engaged in the commission of the targeted drug trafficking offenses, and (2) he used TT1 as part of the commission of those offenses. The Court therefore finds no reason to disturb the issuing Judge's probable cause determination as to the first wiretap.

The second wiretap sought the continued interception of TT1 and the initial interception of TT2, used by Hill, and TT3, used by Mario Ponds. This time, investigators had the benefit of voluminous calls and texts intercepted from TT1. The second application detailed, at some length, that investigators intercepted several calls and texts from TT1 which, based on their knowledge

¹⁵ See 18 U.S.C. § 2516(1)(e) ("any offense involving . . . the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States.").

and experience, led them to believe that Ponds was using TT3 to communicate with Hill on TT1 in order to supply Hill with cocaine. Further, with regard to TT2, investigators confirmed by toll records that Hill had used TT2 to communicate with an unindicted person after the CHS requested to purchase drugs. This provides a substantial basis for concluding that there was a fair probability that the listed offenses were being committed by Hill and Ponds and that evidence of these offenses would be found on TT1, TT2 and TT3. The Court concludes probable cause was properly established by the second wiretap application.

Finally, the third wiretap application sought the continued interception of TT1 and TT2, and the initial interception of TT4, believed to be used by Knighten while he was incarcerated in McAlester, Oklahoma. Again, the voluminous intercepted calls and texts cited in Agent Heath's affidavit support the conclusion that there was more than a fair probability that Hill was using TT1 and TT2 to buy and sell narcotics. Perhaps realizing the difficulty in assailing probable cause as to either of these phones and Defendants, Defendants largely focus on probable cause that Knighten was TT4 in the commission of the target offenses.

Agent Heath's affidavit relays that, at the time of the third application, investigators had numerous calls and texts—intercepted in the first two wiretaps—in which Knighten used a different phone to discuss the purchase and sale of drugs. They learned from a confidential informant that, after law enforcement executed a search warrant at a suspected stash house for the DTO, Knighten planned to switch phones. During the earlier wiretaps, investigators became familiar with Knighten's voice on his old phone and were thus able to confirm that he was the user of TT4. And investigators heard Knighten himself, using TT4, confirm to Hill that this was his new number. Ultimately, Agent's Heath's affidavit established a fair probability, given investigator's experience with Knighten, that he would continue to use TT4 to facilitate the

purchase and sale of narcotics. Thus, the issuing Judge had a substantial basis to conclude there was probable cause Knighten was involved in the commission of the target offenses and that he used TT4 to that effect.

Because each of the three wiretap applications were properly supported by probable cause, the Court concludes that these arguments are insufficient to warrant the suppression of evidence gained from the wiretaps.

B. Necessity

Each Defendant contends that the Government's affidavits in support of its three wiretap applications failed to demonstrate that the wiretaps were necessary to the investigation. Before a wiretap may be approved, there must be "a showing the wiretap is 'necessary' to investigate a serious offense enumerated on a statutory list.¹⁶ This means that that application must contain "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."¹⁷ Such investigative techniques include standard visual and aural surveillance, questioning of witnesses, interrogation of suspected participants, including with the use of grand juries, obtaining and executing search warrants, use of informants and undercover agents, pen registers, and trap and trace devices.¹⁸

If the Government forgoes these techniques, it must explain that decision with particularity.¹⁹ Still, the necessity requirement does not require that the Government try every

¹⁶ *United States v. VanMeter*, 278 F.3d 1156, 1159 (10th Cir. 2002) (citing 18 U.S.C. § 2516).

¹⁷ 18 U.S.C. § 2518(1)(c).

¹⁸ *United States v. Foy*, 641 F.3d 455, 464 (10th Cir. 2011) (citing *United States v. Cline*, 349 F.3d 1276, 1280 (10th Cir. 2003)).

¹⁹ *United States v. Cline*, 349 F.3d 1276, 1280–81 (10th Cir. 2003) (citation omitted).

conceivable investigative technique.²⁰ Nor need the Government show necessity as to all named interceptees.²¹ The Government must cite particular facts and circumstances that make a wiretap necessary, rather than the general experience of the law enforcement affiants.²² And in the case the Government uses multiple wiretaps, it “may not simply ‘move swiftly from wiretap to wiretap,’ ” but rather must consider, after each successive wiretap, “whether normal investigative procedures could [now] be used effectively, particularly in light of any evidence obtained as a result of each succeeding wiretap.”²³ But ultimately, a reviewing court affords a great deal of deference to the initial judge’s determination regarding necessity.²⁴ “[A] wiretap authorization order is presumed proper, and a defendant carries the burden of overcoming this presumption” with regard to necessity.²⁵

Defendants’ contentions regarding necessity generally fall into one of two categories. First, Defendants believe that the affidavits did not establish that Government tried enough investigative tactics before resorting to wiretaps. For instance, Lewis, at oral argument, contended that the Government’s efforts at physical surveillance of Hill were simply insufficient. He believes the evidence shows that the FBI only attempted physical surveillance of Hill a handful of times, and that they have failed to show why more surveillance was not attempted. Ponds similarly

²⁰ *United States v. Armendariz*, 922 F.2d 602, 607 (10th Cir. 1990).

²¹ *United States v. Mitchell*, 274 F.3d 1307, 1312 (10th Cir. 2001).

²² *See Cline*, 349 F.3d at 1280–81.

²³ *United States v. Castillo-Garcia*, 117 F.3d 1179, 1196 (10th Cir. 1997) (quotation omitted), *overruled on other grounds by United States v. Ramirez-Encarnacion*, 291 F.3d 1219 (10th Cir. 2002).

²⁴ *See United States v. Oriakhi*, 57 F.3d 1290, 1298 (4th Cir. 1995).

²⁵ *United States v. Mitchell*, 274 F.3d 1307, 1310 (10th Cir. 2001) (quotation omitted).

complains that the Government did not even try trash pulls at several locations of interest in the investigation, and did not attempt to use a confidential informant for a more proactive role.

These arguments do not convince the Court that the presumption of propriety afforded the initial wiretap authorization should be set aside. Agent Heath's affidavit explained the FBI's choices regarding physical surveillance. Investigators attempted to surveil Hill on multiple occasions and attempted to follow him when he left his residence, only to encounter obstacles that caused them concern about the viability of these techniques and the integrity of the investigation. Hill was known to be surveillance conscious, and Agent Heath testified that he had serious concerns about the investigation being "burnt," or discovered by the suspects. Hill's U.S. Probation Officer had previously been "burnt" while surveilling Hill when his vehicle was identified by Hill's family member, and investigators were concerned their surveillance vehicles would be spotted as well. For later wiretaps, the affidavits relayed that Mario Ponds was also surveillance conscious and would drive multiple different vehicles to suspected drug transactions, and that Hill and his associates did in fact have the capacity to identify FBI surveillance, as investigators overheard them do so once successfully. The affidavit shows that investigators clearly attempted surveillance of Hill, the primary player known to investigators at this time, but were largely unsuccessful in identifying the full contours of the DTO. Further, Agent Heath cited particular facts and circumstances that suggested further surveillance was unlikely to succeed, and even posed a risk to the continued integrity of the investigation.

With respect to Otis Ponds' concerns, Agent Heath explained that trash pulls were not attempted at Hill's residence because he lived on a dead-end street in a surveillance conscious neighborhood, and similar concerns about being burnt cautioned against attempting trash pulls at his residence. Trash pulls at a suspected stash house located in a triplex were not attempted

because of the difficulty ascertaining, in a communal trash dump, which piece of trash is associated with which unit. Agent Heath also averred that the confidential informant identified by Ponds was not used because that person was on probation and thus could not be relied upon to engage in controlled buys. Though investigators could have tried to find a way around this, investigators are not required to try every conceivable investigative technique.²⁶

Defendants' second category of arguments generally contends that the Government was making great strides with its investigation and did not need to resort to wiretaps. Lewis, in his motion and at argument, complains that the Government's controlled buys with Hill were a smashing success and investigators could have wrapped the case up then and there. True, investigators probably had enough to arrest and indict Hill at that time. But the investigation wasn't just geared towards Hill; it was geared towards the entire DTO that investigators suspected was operating in Wichita. The handful of controlled buys did not elucidate the contours of the DTO, nor could it have, as Agent Heath averred that Hill was unwilling to introduce the CHS to other members of the DTO.

Ultimately, this Court affords great deference to the initial determination of necessity.²⁷ Defendants have the burden to change this deferential posture.²⁸ While Defendants here have tried to meet this burden by pointing to the Government's unsatisfactory attempt (in their view) at standard investigative techniques, and the Government's success with such techniques such that a wiretap was not necessary, the Court is convinced that the Government did everything required to demonstrate necessity. The affidavits in support of each wiretap application outlined the *many*

²⁶ *Armendariz*, 922 F.2d at 607.

²⁷ *Oriakhi*, 57 F.3d at 1298.

²⁸ *Mitchell*, 274 F.3d at 1310.

investigative techniques investigators had tried, and explained why they were insufficient to completely identify and dismantle the entire DTO. It further explained that techniques not attempted were left out either because investigators had serious doubts about their chance of success or because the attempt might have risked the integrity of the investigation, or both. Nor did the Government move quickly from wiretap to wiretap.²⁹ The affidavits in support of the second and third wiretap show that investigators considered whether normal investigative techniques would work on the “new” suspects, Ponds and Knighten, and ultimately concluded that they would not for the reasons outlined above.

This is all the Government was required to do.³⁰ Thus, the Court concludes that Defendants’ necessity arguments do not support the suppression of evidence garnered from the wiretaps.

C. Territorial Jurisdiction Over Target Telephone 4

Defendants raise the argument that the issuing Court lacked jurisdiction to authorize the interception of TT4. They contend that because the phone was not in the District of Kansas at any time, nor could it have come into the District, jurisdiction was lacking as to TT4.

Title III provides that a judge may authorize the “interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting.”³¹ An “intercept” is the “aural or other *acquisition* of the contents of any wire, electronic, or oral

²⁹ *Castillo-Garcia*, 117 F.3d at 1196.

³⁰ The Government is required to make “a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.” 18 U.S.C. § 2518(1)(c). The Court concludes it did precisely that in its applications, and has reiterated that here.

³¹ 18 U.S.C. § 2518(3).

communication through the use of any electronic, mechanical, or other device.³² Based on this, the Supreme Court in *Dahda v. United States*³³ appeared to accept, and the parties did not dispute, that “an intercept takes place either where the tapped telephone is located or where the Government's ‘listening post’ is located.”³⁴ Thus, when either of these places are located within the authorizing court’s territorial jurisdiction, the interception takes place within that jurisdiction as well, and the statutory requirement is satisfied.³⁵

Based on this, the Court has no trouble concluding the issuing Court had jurisdiction to authorize the interception of TT4. Though TT4 was located with Knighten in an Oklahoma prison, and thus obviously outside of the District, the statute only requires that *either* the target telephone *or* the listening post be located within the Court’s territorial jurisdiction. The FBI listening post in this case was located in Wichita, Kansas. Thus, the issuing Judge had jurisdiction to authorize the interception of TT4.

D. Minimization

Lewis, Ponds, and Vontress all challenge both the minimization procedures implemented by the Government and the actual minimization of particular calls. The statute provides that persons authorized to intercept communications must do so “in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter.”³⁶

Minimization is concerned primarily with the “the reasonableness of the agents’ efforts to refrain

³² 18 U.S.C. § 2510(4) (emphasis added).

³³ 138 S. Ct. 1491 (2018).

³⁴ *Id.* at 1495. “[A] listening post within the court’s territorial jurisdiction could lawfully intercept communications made to or from telephones located within Kansas or outside Kansas.” *Id.* at 1499.

³⁵ *Id.* (“As so interpreted, the statute generally requires that one or the other or both of these locations must be found within the authorizing judge's ‘territorial jurisdiction.’ ”).

³⁶ 18 U.S.C. § 2518(5).

from monitoring conversations deemed nonpertinent to the investigation.”³⁷ Perfection on the part of law enforcement is not required.³⁸

Of the 3,311 calls intercepted from TT4, Defendants identify 76 that they believe were not properly minimized. This accounts for roughly 2% of the total. Already then, Defendants seem off to a rough start, as a 98% success rate regarding minimization seems well within the bounds of reasonableness. Further, at the hearing, Agent Heath testified as to each of these 76 calls, and concluded that only one call was improperly not minimized. Many of the rest of the calls, though not explicitly about drugs, involved discussion of Travis Knighten’s construction company, which investigators believed was used to launder money made in the drug trade.³⁹ Thus, these calls were properly not minimized because they related to the target offense of money laundering.

At oral argument, Vontress responded that investigators had no evidence the construction company was funded by drug proceeds. But ultimately, investigators did not need such evidence. The standard for minimization is not “absolute certainty,” or “beyond a reasonable doubt.” Rather, the standard is reasonableness. Investigators behaved reasonably by not minimizing calls believed to involve discussion of the laundering of drug proceeds through Knighten’s construction company.

Further, regarding the Government’s minimization procedures, the Court heard evidence that each listener was given both oral and written training on proper minimization of calls unrelated

³⁷ *United States v. Ramirez*, 479 F.3d 1229, 1242 (10th Cir. 2007) (quoting *United States v. Willis*, 890 F.2d 1099, 1101 (10th Cir. 1989), *abrogated in part on other grounds*, *Davis v. Washington*, 547 U.S. 813 (2006)).

³⁸ *Id.* (“[W]e review minimization for the reasonableness of the efforts of law enforcement officials and not the perfection of their results.”). *See also United States v. Uribe*, 890 F.2d 554, 557 (1st Cir. 1989) (“The government is held to a standard of honest effort; perfection is usually not attainable, and is certainly not legally required.”).

³⁹ Money laundering was listed as one of the target offenses in the third wiretap application.

to criminal activity. Specifically, agents were instructed to identify within two minutes of the call if the call seemed unrelated to drug activity, and if so, to stop listening. Each agent was required to review the wiretap applications and Judge Broomes' order authorizing interception. Agent Heath testified that every agent was required to go through this training before listening, and that this process was repeated for each of the wiretaps. The statute does not require any particular minimization procedures, and the Court is satisfied that the training in this case was sufficient.

The Court concludes that the Government properly conducted the wiretaps so as to “minimize the interception of communications not otherwise subject to interception” under the statute.⁴⁰ Therefore, Defendants' request for suppression of wiretap evidence on that basis is denied.

E. Sealing

Defendants complain that the Government failed to immediately seal the communications garnered from each wiretap. Title III provides that “[i]mmediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions.”⁴¹ The statute goes on to provide that “[t]he presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom.”⁴² These requirements serve to prevent the Government from altering or tampering with the recorded conversations.⁴³ If the sealing

⁴⁰ 18 U.S.C. § 2518(5).

⁴¹ *Id.* § 2518(8)(a).

⁴² *Id.*

⁴³ *United States v. Gomez*, 67 F.3d 1515, 1524 (10th Cir. 1995) (quoting *United States v. Ojeda Rios*, 495 U.S. 257, 263 (1990)).

process is hampered by delays, “the Government [must] explain not only why a delay occurred but also why it is excusable.”⁴⁴ “Satisfactory explanation[s]” of a delay may include the unavailability of the issuing judge, intervening weekends or holidays, or the time necessary to prepare the paperwork for sealing.⁴⁵

Each of the three wiretaps came down just before midnight. With one exception, the data was downloaded on to discs the next day and sent promptly to Kansas City, the FBI headquarters for the District of Kansas. Agents in Kansas City would then, without delay, send the discs to Wichita, where they would be presented to Judge Broomes for sealing within a day, not including intervening weekends. Thus, with one exception, the only delays between the wire coming down and sealing were caused by intervening weekends or transit time, both of which seem satisfactory explanations for delay.⁴⁶

The exception to this fairly streamlined process occurred during the second wiretap. The wire came down on Sunday, June 16 just before midnight. The data was not downloaded the next day. Rather, agents in Dallas downloaded and sent the discs to Kansas City on Tuesday, June 18. What happened that Monday is anybody’s guess. The Government suggested in its response that this delay was likely caused by the workload in the Dallas office. Agent Heath testified that he did not know the reason or the delay, and only speculated that the workload in Dallas was the reason. It seems then that the Court has no evidence as to the cause of this one-day delay. Still, workload seems the likely culprit, as the Court heard testimony that the Dallas hub serves 26 FBI field offices across seven different states. And though the Court has not heard an explanation for

⁴⁴ *Ojeda Rios*, 495 U.S. 265.

⁴⁵ *Cline*, 349 F.3d at 1284.

⁴⁶ *See id.*

what happened on that Monday, the Court cannot conclude one day of unexplained delay in sealing the intercepted communications is sufficient to sink the entire wiretap. The evidence presented shows that the Government moved nearly as expeditiously as possible to seal the tapes once the wiretaps came down. This is not the case where the Government delayed sealing in bad faith, to gain an advantage or in an attempt to alter the communications.⁴⁷ Thus, the Court concludes that the Government properly sealed the recorded communication in accordance with the statute.

F. Authorization of First Wiretap.

Finally, all three Defendants challenge the authorization of the first wiretap. Before an application for a wiretap is made to a federal judge under Title III, the application must be authorized by “[t]he Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General.”⁴⁸ For the first wiretap application, law enforcement received the apparent approval of Bruce Schwartz, Deputy Assistant Attorney General (“DAAG”) in the Criminal Division. Defendants now challenge this, contending that the signature on DAAG Schwartz’s apparent authorization looks nothing like the signature of a “Bruce Schwartz.”

Defendants make a fair point. Though it is often tricky to discern a name scrawled quickly in cursive, as most signatures are, the signature at issue here is difficult to reconcile with DAAG

⁴⁷ *Gomez*, 67 F.3d at 1524 (“[T]he purpose of sealing . . . is to ensure that ‘subsequent to its placement on a tape, the Government has no opportunity to tamper with, alter, or edit the conversations that have been recorded.’ ”).

⁴⁸ 18 U.S.C. § 2516(1). In an order dated March 25, 2019, then Attorney General William Barr designated, pursuant to this section, the Deputy Assistant Attorney General in the Criminal Division as an official authorized to approve wiretap applications.

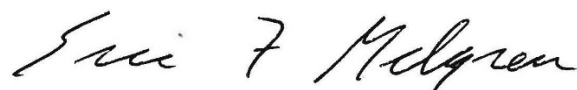
Schwartz's name.⁴⁹ But this does not mean the wiretap is automatically invalid. Crucially, "Title III does not prescribe the manner in which authorization is accomplished or shown."⁵⁰ Nowhere in the statute does it say that authorization must be accomplished by signature. Further, "a named designee whose high office gives him statutory power to authorize electronic surveillance orders is presumed to have properly exercised that power and the conditions precedent are presumed to have been met unless the defendants offer evidence, apart from mere conjecture or speculation, to rebut this presumption."⁵¹

Defendants have offered no evidence to rebut this presumption. Thus, the presumption of propriety remains in place, and the fact that the application, sent by the U.S. Attorney's Office for the District of Kansas to Main Justice seeking authorization by a statutorily approved person, was later returned bearing the name stamp of such a person along with an apparent signature, is enough for the Court to conclude that the application was properly authorized by DAAG Schwartz here.

IT IS THEREFORE ORDERED that Defendants' Motions to Suppress Wiretap Evidence (Docs. 555, 558, and 564) are **DENIED**.

IT IS SO ORDERED.

Dated this 17th day of February, 2022.



ERIC F. MELGREN
CHIEF UNITED STATES DISTRICT JUDGE

⁴⁹ The Court is, of course, not familiar with Mr. Schwartz's signature, and expresses no opinion on whether or not the signature contained in the signature block is actually his. As discussed below, whether it is or not ultimately does not matter.

⁵⁰ *United States v. Wright*, 156 F. Supp. 2d 1218, 1223 (D. Kan. 2001).

⁵¹ *United States v. O'Connell*, 841 F.2d 1408, 1416 (8th Cir. 1988) (cleaned up) (quoting *United States v. Terry*, 702 F.2d 299, 311 (2d Cir. 1983)).