UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA *v.* KENSTON HARRY	Crim. No. 3:21cr98 (JBA) February 4, 2022

ORDER DENYING DEFENDANT'S MOTION TO SUPPRESS

Defendant Kenston Harry is among eight defendants charged by indictment for engaging in an alleged drug conspiracy to distribute and possess with intent to distribute controlled substances. He moves to suppress evidence derived from the search of his cell phone executed by a warrant. (Mem. of L. in Supp. of Mot. to Suppress Evid. ("Def.'s Mem.") [Doc. # 220-1] at 1; Reply to Gov't's Opp'n to Mot. to Suppress Evid. ("Def's Reply") [Doc. # 264] at 1.) He also moves to suppress evidence gathered from a pole camera positioned by law enforcement outside of his place of business. (*Id.*) The Government opposes Defendant's motion. (*See generally* Gov't's Opp'n to the Def.'s Mot. to Suppress Evid. ("Gov't Opp'n") [Doc. # 233].) For the following reasons, Defendant's motion [Doc. # 220] is DENIED.

I. Background

Sometime in 2020, the Drug Enforcement Agency ("DEA") began investigating Tajh Wiley, who the Government alleges conspired with Defendant to illegally possess and distribute controlled substances. (Gov't Opp'n at 1-2.) During that investigation, DEA agents acquired authorizations to intercept wire and electronic communications to and from Wiley's cell phone. (*Id.* at 2.) Pursuant to those authorizations, DEA agents intercepted communications from May 14 to May 18, 2021 and again from May 18 through June 9, 2021. (*Id.*) The Government alleges that during that period, Defendant communicated with Wiley "on numerous occasions" in furtherance of the alleged drug trafficking conspiracy using a cell phone with a number ending in -4489. (*Id.*)

According to the Government, DEA authorities learned that Defendant owned the Action Audio Store, a vehicle accessary shop located at 2814 Main Street in Hartford, Connecticut, which he allegedly used, along with his Bloomfield residence, as drug storage and distribution hubs for the drug conspiracy. (*Id.* at 2-3.) For example, the Government alleges that on April 28, 2021 and May 7, 2021, Wiley traveled to the Action Audio Store and Defendant's Bloomfield residence to facilitate later drug transactions. (*Id.* at 3.) In intercepted voice communications, Wiley allegedly called Defendant's Bloomfield residence "the lab," apparently in reference to a location where Wiley and Defendant would package and distribute controlled substances. (*Id.*)

To further investigate Defendant's movements, DEA investigators installed a fixed video surveillance camera ("pole camera") on April 19, 2021 to record video surveillance of Defendant's Action Audio Store, which was and remains open for business to members of the public. (*Id.*) The camera was mounted on a utility pole across the street from the Action Audio Store and positioned to observe the exterior of the Action Audio Store, including its parking lot area and the exterior of the north and northwest portions of the building, and only viewed portions of the exterior of the building that would be visible to any individual walking or driving along the street. (*Id.* at 3-4.) The camera remained in place attached to the utility pole until June 19, 2021, but ceased surveillance on June 9, 2021, the date of Defendant's arrest. The camera did not have any advanced capabilities such as facial recognition or heat sensing technology, nor did it have its own light source. (*Id.* at 3.)

On June 8, 2021, in anticipation of Defendant's arrest, the Government obtained a warrant to seize and search Defendant's cell phone with the assigned telephone number ending in -4489, the number associated with the cell phone Defendant allegedly used to conduct drug trafficking activities. (*Id.* at 4.) United States Magistrate Judge S. Dave Vatti authorized the warrant to seize and search Defendant's cell phone, adopting the affidavit by

DEA Special Agent ("SA") Andrew Hoffman and the attachments appended to the search warrant. *See* Application for Search Warrant, 3:21-mj-577 (SDV) (D. Conn. June 10, 2021), ECF # 19. The warrant application incorporated two attachments. In Attachment A, the Government described the property to be searched, i.e., Defendant's cell phone, and the times and various locations where that cell phone may be found. *Id.* at 2-3. Attachment B requests to search:

> All records and information contained on the Target Telephone, described in Attachment A, that constitute evidence and instrumentalities of violations of Title 21, United States Code, Section 841(a)(1) (possession with intent to distribute and distribution of controlled substances), Title 21, United States Code, Section 846 (attempt and conspiracy to commit possession with intent to distribute and distribution of controlled substances), Title 21, United States Code, Section 843(b) (use of a communication facility), and Title 18, United States Code, Sections 1956 (money laundering) ("TARGET OFFENSES"), committed by the TARGET SUBJECT, described in Attachment A, and members of the WILEY drug trafficking organization, known and unknown . . . .

Id. at 4. Attachment B then seeks authorization for the Government to search "any and all data" that might relate to various drug trafficking activities or reveal members of the conspiracy in which the Government alleges Defendant participated. (*Id.* at 4-6, ¶¶ (a)-(i).) Paragraph (j) of Attachment B narrows the type of evidence which may indicate such activities or identities, such as address books, stored usernames, photographs, videos, search history, and location information. (*Id.* at 6-7, ¶ (j).) Finally, Attachment B provides for agents "to deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government for independent review." (*Id.* at 8.)

On June 9, 2021, DEA agents arrested Defendant pursuant to an arrest warrant and seized the cell phone he had on his person. (Gov't Opp'n at 8.) Agents confirmed with Defendant that this cell phone carried the assigned number -4489 and set it to "airplane mode" to prevent the phone from connecting to remote software capable of deleting its contents. (*Id.* at 8-9.) Then, DEA agents began a battery of forensic searches on the cell

phone's contents. The first of which occurred on June 11, 2021, when electronically stored information was extracted from the cell phone using forensic software, and again on and June 29, 2021. (*Id.* at 9.) On or about July 19, 2021, SA Hoffman conducted a manual or "human" search of the data. (*Id.*) DEA investigators maintain custody of Defendant's cell phone, as well as electronically stored information extracted from therefrom.

II. Discussion

A. Evidence Obtained from Defendant's Cell Phone

Defendant raises two arguments supporting his contention that the evidence obtained from his cell phone should be suppressed. First, he argues that the warrant authorizing the search violated the Fourth Amendment because it lacked particularity. (Def.'s Mem. at 3.) Defendant asserts that the warrant permitted law enforcement agents to search broad categories of information without temporal limitation. (*Id.* at 4-5.) Second, Defendant argues that, after law enforcement seized his cell phone pursuant to a search warrant, they delayed for forty-seven days before concluding their search. (*Id.* at 6.)

The Government counters that the warrant was sufficiently particular because it specified the offenses for which there was probable cause, the warrant defined the place to be searched as Defendant's cell phone assigned to the number ending in -4489, and it defined the types of information in connection with the suspected offenses sought from the cell phone. (Gov't Opp'n at 14.) Additionally, the Government argues that the lack of temporal restrictions alone does not render a warrant invalid per se, (*id.* at 15), and the lack of temporal restrictions in this warrant was appropriate given the scope of the conduct under investigation, (*id.* at 16).[1] Finally, the Government contends that the search warrant was not

[1] The Government also argues that, even if assuming the warrant violated the Fourth Amendment, the officers relied in good faith on the conclusion by the magistrate judge that the warrant was valid. (Gov't Opp'n at 22-23.) Because the Court finds that the warrant was valid, it declines to address this argument.

unreasonably delayed because it was executed within the time constraints of Federal Rule of Criminal Procedure 41. (*Id.* at 25-26.) The Court independently reviews the Government's warrant and conduct with each of Defendant's arguments in mind.

1. Particularity of the Search

The Fourth Amendment commands that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly* describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV (emphasis added). The Amendment's particularity requirement is, in essence, a prohibition against "general warrants." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). This prohibition concerns whether the warrant identifies with reasonable certainty those items to be seized. *United States v. George*, 975 F.2d 72, 75 (2d Cir. 1992). Its "manifest purpose" is to prevent "wide-ranging exploratory searches" by ensuring that searches are "carefully tailored" to their justifications. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). To be sufficiently particular, "a warrant must identify the specific offense for which the police have established probable cause[,] describe the place to be searched[, and] specify the items to be seized by their relation to designated crimes." *United States v. Galpin*, 720 F.3d 436, 445-46 (2013) (internal citations omitted); *see also United States v. Bianco*, 998 F.2d 1112, 1116 (2d Cir. 1993) (finding unconstitutional a warrant that did not mention a particular criminal statute or specify the type of criminal conduct).

In the context of electronic devices, courts "must be attuned to the technological features unique to digital media as a whole and to those relevant in a particular case," *United States v. Ganias*, 824 F.3d 199, 213 (2d Cir. 2016). Thus, "[a] warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material, without violating the particularity requirement." *United States v. Ulbricht*, 858 F.3d 71, 102-03 (2d Cir. 2017).

The warrant here, although broad, did not lack particularity in terms of data to be searched. The warrant incorporated two attachments relevant to this inquiry. *See Groh v. Ramirez*, 540 U.S. 551, 557-58 (2004) (establishing that a court may construe a warrant with reference to a supporting application or affidavit). First, in Attachment A, it clearly specified the property to be seized and searched—Defendant's cell phone—as well as the appropriate time and place such seizure may occur as further described in Attachment B. *See* Application for Search Warrant, 3:21-mj-577 (SDV), at 2-3, ECF # 19. Next, in the first paragraph of Attachment B the warrant limited itself to searching for data that might reveal evidence that Defendant violated 21 U.S.C §§ 841(a)(1), 843(b), and 18 U.S.C. § 1956, the drug trafficking offenses for which he was a suspect. *Id.* at 4. Attachment B then lists several categories of data that might have revealed evidence of this activity, such as "photographs and videos" as well as encrypted communications, contact lists, "notes, records, ledgers, and documents indicative of drug trafficking." *Id.* at 6-7, ¶ (j). By incorporating Attachments A and B, the warrant lists the charged crimes, describes the item to be seized, and describes the information to be searched in connection with the specified criminal conduct.

Defendant maintains, however, that these provisions cannot save the warrant because it uses the phrase "any and all data" throughout unaccompanied by reference to the specific offenses for which he was a suspect. (Def.'s Mem. at 5.) Defendant argues that the search warrant impermissibly authorized agents to access locations within his cell phone beyond the scope their stated probable cause. For example, he contests the search of photographs, digital notes, and ledgers stored on his cell phone because "no information from the investigation suggested that Mr. Harry had any photographs, digital notes, records, ledgers or other documents indicative of drug activity on his phone." (Def.'s Reply at 3.) He also notes that in just one paragraph does the warrant list specific types of data for which law enforcement should search but argues that "the odd juxtaposition of a few specific

locations in the same warrant that authorized a widespread general search for '[a]ny and all data" risked confusing the searching agent." (*Id.* (citing *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 460 (S.D.N.Y. 2013)). The Court is unpersuaded.

First, the warrant at issue is distinguishable from the warrant the court found insufficiently particular in *Zemlyansky*. In *Zemlyansky*, the warrant did not "direct searching officers to seize evidence *related to*, or *concerning*, any particular crime or type of crime." *Zemlyansky*, 945 F. Supp. 2d at 456. That warrant also allowed officers to seize *any* cell phone found at a certain place of business which law enforcement agents believed could be associated with unspecified criminal suspects and it authorized them to conduct boundless, discretionary searches of any electronic device found at that location. *Id.* at 458-59. The court found that these parameters were too "broad, undefined, and ambiguous," rendering the warrant unconstitutional. *Id.* at 459. By contrast, the warrant authorizing the search at issue here narrowed its scope to data related to *specific criminal offenses* stored on *one device*.

Second, use of the phrase "any and all data" throughout the warrant did not confer upon the searching agents unlimited discretion to search for data irrelevant to the criminal offense for which Defendant was under investigation. Given that law enforcement agents had probable cause that Defendant used his cell phone to engage in a drug conspiracy with others, they had a reasonable basis to expect incriminating evidence stored on that cell phone would take many different forms. As the Second Circuit has observed, "it will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes." *Ulbricht*, 858 F.3d at 102. As insurance against the possibility that the search would devolve into an aimless exploration of all the data contained on his cell phone, the searching agents were guided by the first paragraph of Attachment B, which limited the search to "all records and information

contained in the Target Telephone, described in Attachment A, that constitute evidence and instrumentalities of violations of [distribution of controlled substances, use of a communication faculty, and money laundering]." Application for Search Warrant at 4.

Even where the warrant in question authorized the search of "any and all data" without specific reference to the criminal statute, it still refers to particular criminal conduct. *See, e.g.*, *id.* at 4, ¶¶ (b)-(c) (authorizing search of "any and all data related to communications that identify the main customers of the WILEY drug trafficking organization" and "related to communications that reveal the identities and roles of all suppliers of controlled substances"). This language is another indication that the *whole* search was based on suspicion of these activities and directed searching agents to pursue evidence related only to that conduct. *See United States v. Juarez*, No. 12-CR-59 (RRM), 2013 WL 357570, at *3 (E.D.N.Y. Jan. 29, 2013) ("[A] warrant satisfies the particularity requirement when it sufficiently identifies and describes the items to be searched and seized and links that evidence to the specific criminal activity being investigated."); *see also United States v. Hernandez*, No. 09-CR-625 (HB), 2010 WL 26544, at *10 (S.D.N.Y. Jan. 6, 2010) (finding a search warrant valid when it indicated that only documents related to violations of various criminal fraud statutes related to the suspected criminal conduct).

That the warrant did not impose a time period restricting relevant data to be searched does not invalidate it either. While the lack of temporal limitations in a warrant is considered in evaluating a warrant's particularity, it is not the sole factor. *See United States v. Wey*, 256 F. Supp. 3d 355, 388 (S.D.N.Y. 2017) (concluding that the "lack of particularity [was] only compounded by the absence of any date restriction on the items to be seized"). Indeed, the "complexity and duration of the alleged criminal activities" may diminish the significance of temporal restrictions. *Wey*, 256 F. Supp. 3d at 388. The Government argues that these considerations apply here where it contends that Defendant used the cell phone targeted by

the warrant as an instrumentality of his alleged crimes over "an extended period of time." (Gov't Opp'n at 19.) Although a specified timeframe would have been beneficial, given the scope of the investigation into Defendant and his alleged co-conspirators, its absence will not invalidate the otherwise sufficiently particular warrant.

2. Unreasonable Delay

Defendant argues that the search of his cell phone was unreasonably delayed, relying on *United States v. Smith*, 967 F.3d 198 (2d Cir. 2020), for the proposition that "[a] month-long delay [to apply for a warrant] well exceeds what is ordinarily reasonable." (Def.'s Mem. at 6-7 (quoting *Smith*, 967 F.3d at 207).) According to Defendant, *Smith* "concerned the proper remedy when the government delays searching a cellphone that it has seized." (Def.'s Reply at 8.) But *Smith* was decided on the premise that "[t]he right of the police to temporarily seize a person's property *pending the issuance of a search warrant* presupposes that the police will act with diligence to apply for the warrant." 967 F.3d at 205 (emphasis added). Indeed, the case law to which *Smith* cites in support of its holding address circumstances where law enforcement delayed their acquisition of a warrant to search property they had already seized. *Id.* at 205-06 (collecting cases). Contrary to Defendant's reading, *Smith* did not contemplate delays in searching a cell phone seized pursuant to a valid warrant.

Instead, the timing of the Government's search of Defendant's cell phone is more appropriately evaluated under the requirements of the Federal Rules of Criminal Procedure. Rule 41 provides that a warrant must require law enforcement to execute it within a specified time of no longer than fourteen days. Fed. R. Crim. P. 41(e)(2)(A)(i). Regarding electronic storage media or electronically stored information, however, Rule 41(e)(2)(B) provides that the "time for executing the warrant . . . refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." Fed. R. Crim. P.

41(e)(2)(B). Anticipating disputes about the meaning of this provision, the 2009 Advisory Committee Notes explain that

> [c]omputers and other electronic storage media commonly contain such large amounts of information that it is impractical for law enforcement to review all of the information during execution of the warrant at the search location. *This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant . . . .*
>
> In addition to addressing the two-step process inherent in searches for electronically stored information, the Rule limits the 10[14] . . . day execution period to the actual execution of the warrant and the on-site activity. While consideration was given to a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place, *the practical reality is that there is no basis for a "one size fits all" presumptive period.* A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs.

Fed. R. Crim. P. 42(e)(2)(B) advisory committee's notes to the 2009 amendment (emphasis added). When a court has concluded that the Government violated Rule 41, it should not remedy the error by suppressing evidence unless "(1) there was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule." *United States v. Pangburn*, 983 F.2d 449, 455 (2d Cir. 1993) (internal citation and quotations omitted).

Here, the affidavit supporting the search warrant stated upfront that the Government's search would potentially span "weeks or months, depending on the volume of data stored" and that an on-site analysis would be "impractical." (Affidavit of SA Hoffman, Gov't Ex. C. [Doc. # 235-3] at ¶ 245(a).) The Government performed an initial search of the cell phone on the day that it was seized, meeting Rule 41's command that the Government execute the warrant within a specified time of no longer than fourteen days. *See* Fed. R. Crim.

P. 41(e)(2)(A)(i). The Government then completed a more thorough search when it deemed it technically practicable, as anticipated by the warrant application. Given these facts, the delay between seizure of the phone and extraction of the data was reasonable. But even if the delay may be fairly interpreted as unreasonable, because Defendant has not demonstrated prejudice to him caused by the delay or that it was the result of "intentional and deliberate disregard of a provision in the Rule," the suppression of any evidence the search produced is not appropriate. *See Pangburn*, 983 F.2d at 455.

B. Pole Camera Evidence

The basis for Defendant's motion to suppress the pole camera evidence appears to be that the warrantless installation of the pole camera violated his Fourth Amendment protected expectation of privacy because it monitored activities outside of his place of business. (Def.'s Mem. at 10-11.) Defendant argues that the area surveilled by the pole camera is not publicly accessible because it is mounted at a vantage point not usually available to the public without climbing up a utility pole. (*Id.* at 11.) Even if the scope of the pole camera's view covered only publicly accessible areas, Defendant further argues that filming those areas for several uninterrupted weeks is unreasonable. (Def.'s Reply at 11.) Because Defendant cannot expect an ordinary citizen to engage in that activity, he maintains that the installation of the pole camera violated his reasonable expectation of privacy. (Def.'s Mem. at 11.)

The Government argues that blanket suppression of all the surveillance footage produced from the pole camera is inappropriate because Defendant does not have a privacy interest in the areas captured, which are publicly accessible. (Gov't Opp'n at 31.)

Although the Fourth Amendment guarantees citizens a reasonable expectation of privacy, activity a person knowingly exposes to the public is not a subject of Fourth Amendment protection and is not constitutionally protected from observation. *Katz v. United*

States, 389 U.S. 347, 351 (1967). Acknowledging that tradeoff, *Katz* established a two-part inquiry: (1) whether the defendant manifested a subjective expectation of privacy in the object of the challenged search and (2) whether society recognizes that expectation as reasonable. *California v. Ciraolo*, 476 U.S. 207, 211 (1986). Although the Second Circuit has not opined on the merits of a defendant's claimed privacy expectation in the public areas captured by a pole camera, a considerable number of courts to speak on the issue have held that they do not. *See United States v. Bailey*, No. 15-CR-6082G, 2016 WL 6995067, at *33 (W.D.N.Y. Nov. 29, 2016) (collecting cases) (holding that the defendant "failed to establish that his reasonable expectations of privacy were violated by the surveillance" because "the pole camera was installed in a public place and captured activity surrounding a street that was exposed to the public").

The Court finds this authority persuasive in resolving the issue here. Defendant cannot demonstrate a subjective expectation of privacy in activity captured by the pole camera on the street, sidewalk, and parking lot outside of the Action Audio Store because those areas were not shielded from public view. *See United States v. Thomas*, No. CRIM. 3:02CR00072 (AW), 2003 WL 21003462, at *5 (D. Conn. 2003) ("There was nothing shielding the activities of a person in this area from anyone who happened to be walking or driving down [the street abutting the defendant's residence]."); *see also United States v. Nix*, No. 15-CR-6126 (EAW), 2016 WL 11268961, at *3 (W.D.N.Y. Nov. 7, 2016) ("Nix simply had no reasonable expectation of privacy from being observed walking in the parking lot of apartment complexes that, while privately owned, are easily accessible to the public.").

Nor can it be argued that Defendant's claimed expectation of privacy has been recognized by society. Defendant's contention that members of the public typically do not climb up utility poles to gain a better view of the activities below is well taken. (*See id.* at 11.) But "the Fourth Amendment does not punish law enforcement for using technology to more

efficiently conduct their investigations." *United States v. Houston*, 813 F.3d at 288 (6th Cir. 2016). For example, the average citizen usually does not fly aircraft in public airspace over another's property to access a better vantage point, but the Supreme Court nonetheless has upheld such conduct when performed by law enforcement. *Ciraolo*, 476 U.S. at 213. It follows that the placement of pole cameras in places ordinarily out of public reach, even when the surveillance is long in duration, does not violate the Fourth Amendment. *See United States v. Krawczyk*, No. CR12-01384-PHX-DGC, 2013 WL 3853213, at *1 (D. Ariz. July 25, 2013).

Because Defendant has not demonstrated that the use of the poll camera to capture the activity outside of his place of business violated his subjective and objective expectations of privacy, the Court concludes that suppression of the evidence it captured is unwarranted.

III. Conclusion

Defendant has not met his burden to show that the warrant acquired to search his cell phone was insufficiently particular, that the Government unreasonably delayed its search of the cell phone, or that the placement of a pole camera outside of his place of busines violated his constitutionally protected expectation of privacy. Therefore, Defendant's motion to suppress [Doc. # 220] is DENIED.[2]

IT IS SO ORDERED.

/s/

Janet Bond Arterton, U.S.D.J.

Dated at New Haven, Connecticut this 4th day of February 2022.

[2] "[A]n evidentiary hearing on a motion to suppress ordinarily is required if the moving papers are sufficiently definite, specific, detailed, and nonconjectural to enable the court to conclude that contested issues of fact going to the validity of the search are in question." *United States v. Watson*, 404 F.3d 163, 167 (2d Cir. 2005) (internal citations and quotation marks omitted). In the present case, there appears to be no dispute of fact presented by the parties. Therefore, the Court does not find it necessary to hold such hearing.