UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	:	**MEMORANDUM DECISION AND ORDER**
- against -	:	
JOAQUIN ARCHIVALDO GUZMAN LOERA,	:	09-cr-0466 (BMC)
Defendant.	:	

COGAN, District Judge.

Defendant has filed two motions to suppress evidence as the fruit of illegal searches and seizures. The first motion concerns evidence obtained from defendant's communication network located on servers in the Netherlands. The second relates to evidence obtained from his FlexiSpy spyware accounts located on servers in the United States. For the reasons given below, defendant's motions are denied.

The Court assumes familiarity with the facts and will discuss them below only as needed.

I. Timeliness

As a threshold matter, the Government argues that the Court should deny defendant's motions to suppress as untimely. Defendant claims that he was unaware of the basis for these motions until he received unredacted versions of related discovery after the April 9, 2018 deadline. After reviewing the discovery, I agree that defendant has put forth a good faith basis for his delay, and will therefore decide the motions on the merits.

II. Fourth Amendment Standing

Defendant moves to suppress evidence from the Dutch servers and the FlexiSpy accounts on the ground that it was obtained through violations of his Fourth Amendment rights. As the

party moving to suppress, defendant bears the burden of establishing his standing. See United States v. Osorio, 949 F.2d 38, 40 (2d Cir. 1991).

The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. "The basic purpose of this Amendment, . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (internal quotation marks and citation omitted).

Under the Fourth Amendment, a search occurs when "the government violates a subjective expectation of privacy that society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33 (2001). A seizure occurs when "there is some meaningful interference with an individual's possessory interests in that property." Soldal v. Cook Cty., 506 U.S. 56, 61 (1992) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)). The "ultimate touchstone of the Fourth Amendment is reasonableness." Riley v. California, 134 S. Ct. 2473, 2482 (2014).

To establish standing in the Fourth Amendment context, a defendant "must prove that he had a legitimate expectation of privacy that was violated by the Government's [conduct]." United States v. Montoya-Eschevarria, 892 F. Supp. 104, 106 (S.D.N.Y. 1995); see also United States v. Smith, 621 F.2d 483, 487-88 (2d Cir. 1980). This burden "is met only by sworn evidence, in the form of affidavit or testimony, from the defendant or someone with personal knowledge." Montoya-Eschevarria, 892 F. Supp. at 106. "The defendant's unsworn assertion of the Government's representations does not meet this burden." Id.; see also United States v. Singleton, 987 F.2d 1444, 1449 (9th Cir. 1993).

Montoya-Eschevarria is instructive. There, the defendant moved to suppress recorded phone calls for lack of probable cause. The defendant did not assert that the voice on the phone calls was his; instead, he claimed that the Government told his counsel that it was him. The court acknowledged the defendant's predicament – he would either have to admit that it was his voice or forego his motion to suppress. However, the Court concluded that the defendant could not establish his standing by relying on the Government's assertions.

Similarly, defendant has not demonstrated the threshold for a legitimate expectation of privacy by swearing that the information on the Dutch servers or FlexiSpy accounts is his. Instead, defendant uses Special Agent Grey's affidavit as a proxy for his own. However, Special Agent Grey does not have personal knowledge that the Dutch servers and FlexiSpy accounts are defendant's. [redacted] That is too tenuous a link to create standing for a motion to suppress, and impermissibly relies entirely on the Government's theory of the case.

Because defendant has not met his burden to establish standing, defendant's motions to suppress are denied. However, even if defendant could establish standing by relying on Special Agent Grey's affidavit, I would still deny defendant's motions for the reasons that follow.

III. Motion to Suppress the Dutch Servers Communications

Defendant challenges the FBI's search of servers that ran his encrypted communication network, including telephone calls, text communications, and information stored on that network. [redacted] At all relevant times, the servers that ran this encrypted communication network were located in the Netherlands.

The United States and the Netherlands are parties to a Mutual Legal Assistance Treaty ("MLAT"). Over the course of 2011 and 2012, the FBI obtained evidence from the Dutch servers in three ways. First, the FBI made several MLAT requests for Dutch authorities to surveil certain IP addresses connected to defendant's communication network, and the Dutch authorities intercepted and recorded phone calls and provided that surveillance to the FBI on an ongoing basis. Second, the Dutch authorities executed search warrants on the servers and provided the FBI with copies of their contents. [redacted] The Dutch authorities also leased additional servers to house the recorded conversations and created a backup server that automatically received and stored the surveilled data for the FBI.

As discussed further in Part IV.A below, the Supreme Court has characterized the Government's "acquisition" of collected, recorded data as a search, rather than a seizure. See Carpenter, 138 S. Ct. at 2221. The FBI's receipt of the communications and information stored on the Dutch servers did not interfere with defendant's possessory interests, because it did not impede his ability to use the communication network or access the data on those servers. Instead, the challenged conduct involves a possible invasion of any privacy interest defendant had in their contents – constituting a search under the Fourth Amendment, rather than a seizure.

Several searches occurred in this case. First, the Dutch authorities conducted searches by their surveillance of each IP address, and by providing the FBI with ongoing information from that surveillance.[1] [redacted]

[1] Pursuant to the so-called "international silver platter doctrine," "suppression is generally not required when the evidence at issue is obtained by foreign law enforcement officials." United States v. Lee, 723 F.3d 134, 140 (2d Cir. 2013). However, evidence obtained in a foreign country may be excluded "where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials." Id. "In order to render foreign law enforcement officials virtual agents of the United States, American officials must play some role in controlling or directing the conduct of the foreign parallel investigation." United States v. Getto, 729 F.3d 221, 230 (2d Cir. 2013). Defendant argues that the Dutch authorities acted as agents of the Government,

[redacted] Finally, the Dutch authorities conducted searches when they accessed and copied the contents of the Dutch servers pursuant to search warrants, and when they transferred those copies to the FBI.

Even if this conduct were characterized as a seizure rather than a search, the seizure would still have been reasonable in light of the Government's need to avoid the loss of evidence. "Where law enforcement authorities have probable cause to believe that a container holds contraband or evidence of a crime, . . . [officers may] seiz[e] [] the property . . . to examine its contents, if the exigencies of the circumstances demand it . . . ." United States v. Martin, 157 F.3d 46, 53 (2d Cir. 1998) (quoting United States v. Place, 462 U.S. 696, 701 (1983)).

[redacted] As a result, the Government likely had probable cause to believe that defendant and his associates used the network to discuss the Sinaloa Cartel and details of its narcotics trafficking, among other illegal activity. Over the course of the investigation, the FBI became concerned that the calls containing this evidence would be lost, [redacted] and asked the Dutch authorities to adjust their method of surveillance. Seizing the communications was therefore necessary to avoid "loss or destruction of suspected contraband." Martin, 157 F.3d at 53 (internal quotation

triggering Fourth Amendment protection for defendant. The Government nominally contests this point, but states that I do not need to decide the issue in order to dispose of the motion. I agree. For the purpose of the motion to suppress evidence obtained from the Dutch servers, I will assume that the Dutch authorities acted as agents of the Government. However, even assuming the Fourth Amendment applies to their conduct, the searches were reasonable, and the evidence obtained from them need not be suppressed.

marks omitted). The Court agrees with the Government that any seizure was reasonable under the circumstances.

A. Extraterritorial Application of the Fourth Amendment

The Supreme Court in United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990), held that the Fourth Amendment does not apply "to the search and seizure by United States agents of property that is owned by a nonresident alien and located in a foreign country." Only aliens who "have otherwise developed sufficient [voluntary connections] with this country to be considered part of [the national] community" may invoke its protections. Id. at 265.

The Second Circuit has strictly adhered to this holding. See In re Terrorist Bombings of U.S. Embassies in E. Africa, 552 F.3d 157, 174 (2d Cir. 2008) (observing that its previous holding articulated in United States v. Toscanino, 500 F.2d 267 (2d Cir. 1974), "that aliens may invoke the Fourth Amendment against searches conducted abroad by the U.S. government" was "no longer valid in light of Verdugo–Urquidez"). So too have courts within this district. See, e.g., United States v. Gasperini, No. 16-CR-441, 2017 WL 3038227, at *3 (E.D.N.Y. July 17, 2017), aff'd, 894 F.3d 482 (2d Cir. 2018); United States v. Hasbajrami, No. 11-CR-623, 2016 WL 1029500, at *7 (E.D.N.Y. Mar. 8, 2016); United States v. Defreitas, 701 F. Supp. 2d 297, 304 (E.D.N.Y. 2010). Indeed, it appears that courts in this Circuit consider the Verdugo-Urquidez holding "dispositive case law." See Defreitas, 701 F. Supp. 2d at 304.

Notably, the respondent in Verdugo-Urquidez was a citizen and resident of Mexico and was believed to be "one of the leaders of a large and violent organization in Mexico that smuggles narcotics into the United States." Id. at 262. After his arrest in Mexico and relocation to the United States, agents of the Drug Enforcement Agency and the Mexican Federal Judicial Police conducted searches of the respondent's properties in Mexico, which resulted in the seizure

of certain documents. The Supreme Court rejected the respondent's Fourth Amendment claim because, "[a]t the time of the search, he was a citizen and resident of Mexico with no voluntary attachment to the United States, and the place searched was located in Mexico." Id. at 274-75. In those circumstances, it instructed, "the Fourth Amendment has no application." Id. at 275.

Defendant claims that the searches of his Dutch servers violated the Fourth Amendment. However, the searches occurred in the Netherlands, and defendant was a citizen and resident of Mexico at that time. As a result, defendant can only invoke the Fourth Amendment if he has established substantial voluntary connections to the United States.

Defendant argues that, because the Government claims that he and the Sinaloa Cartel directed a large-scale narcotics trafficking operation into the United States and sold millions of dollars of drugs here, the Government has alleged sufficient connections to afford him Fourth Amendment protections. But defendant – not the Government – bears the burden of establishing that his Fourth Amendment rights were violated. See Osorio, 949 F.2d at 40. Because he has not provided any facts other than the Government's theory of the case, defendant has not met his burden to show substantial connections with this country that might otherwise entitle him to Fourth Amendment protections. See Montoya-Eschevarria, 892 F. Supp. at 106.

Even if defendant could establish a connection to this country through the Government's charges against him, defendant's conduct does not constitute the type of connections that the Supreme Court envisioned when it spoke of the community of people covered by the Fourth Amendment. Rather, his alleged connections are purely criminal and do not entitle him to protection. See, e.g., United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001). Ultimately, defendant's story parallels that of the respondent's in

Verdugo-Urquidez, and the Supreme Court was clear that the Fourth Amendment did not apply in that instance.

Because defendant was, at the relevant time, a citizen and resident of Mexico and has not shown substantial voluntary connections to the United States, defendant cannot invoke the Fourth Amendment for searches that occurred in the Netherlands. However, assuming defendant could invoke the Fourth Amendment, I would still deny his motion to suppress the Dutch servers evidence.

B. Challenge to the Searches of the Dutch Servers

As an initial matter, "the Fourth Amendment's warrant requirement does not govern searches conducted abroad by U.S. agents; such searches . . . need only satisfy the Fourth Amendment's requirement of reasonableness." In re Terrorist Bombings, 552 F.3d at 167. Because the challenged searches occurred in the Netherlands, the Fourth Amendment's warrant requirement does not apply, and the searches are assessed based on their reasonableness.

It is well settled that 'Fourth Amendment protections extend only to unreasonable government intrusions into . . . legitimate expectations of privacy." United States v. Reyes, 283 F.3d 446, 457 (2d Cir. 2002) (internal quotation marks and citations omitted). "As a general matter, '[t]he reasonableness of a search depends on the totality of the circumstances, including the nature and purpose of the search and the extent to which the search intrudes upon reasonable privacy expectations.'" United States v. Lambus, 897 F.3d 368, 402 (2d Cir. 2018) (quoting Grady v. North Carolina, 135 S. Ct. 1368, 1371 (2015)). "Reasonableness in the totality of the circumstances 'is determined by assessing, on the one hand, the degree to which [the search] intrudes upon an individual's privacy, and, on the other, the degree to which it is needed for the promotion of legitimate government interests.'" Id. (quoting Samson v. California, 547 U.S.

843, 848 (2006)). "For an individual's expectation of privacy to be legitimate, he must have exhibited an actual (subjective) expectation of privacy and the expectation must be one that society is prepared to recognize as reasonable." Reyes, 283 F.3d at 457 (internal quotation marks and citations omitted).

Defendant has not claimed a subjective expectation of privacy in the Dutch servers. However, his communication network was encrypted and was purportedly created to allow communication without Government interception. This suggests that defendant had a subjective expectation of privacy in the communications made on the system, and I will accept that premise as true for the purpose of this motion.

Nevertheless, defendant did not have an objectively reasonable expectation of privacy in these communications. There are two primary reasons why. First, defendant was an escapee from prison during this time, and there was a significant bounty for his capture – worth millions. From the moment he fled, defendant became a target of public and governmental investigation. It is not reasonable for defendant to think that the Government (or, for that matter, a civilian) was not monitoring his communications in an attempt to capture him. Further, defendant's status as an escapee means that he receives the same "severely curtailed" Fourth Amendment protections as prison inmates. See United States v. Roy, 734 F.2d 108, 111 (2d Cir. 1984) ("We consider an escapee to be in constructive custody for the purpose of determining his legitimate expectations of privacy; he should have the same privacy expectations in property in his possession inside and outside the prison"). Notably, the Second Circuit has instructed that "prison inmates have no reasonable expectation of privacy," United States v. Amen, 831 F.2d 373, 379-80 (2d Cir. 1987), and as a result, neither does defendant here.

[redacted]

C. The Good Faith Exception to the Exclusionary Rule

The Government argues that the good faith exception to the exclusionary rule applies, because the FBI relied in good faith on all of the binding appellate precedent discussed above (and more) in conducting the Dutch servers searches. See Davis v. United States, 564 U.S. 229, 236-37 (2011). I agree.

The Supreme Court has articulated that the "[exclusionary] rule's sole purpose . . . is to deter future Fourth Amendment violations." Id. "[W]hen the police act with an objectively

[redacted]

reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way." Id. at 238 (internal quotations and citation omitted). Here, law enforcement officials conformed their conduct to existing Supreme Court and Second Circuit law while conducting searches on the Dutch servers. This counsels against application of the exclusionary rule, because its deterrent value simply would not be furthered in this case.

D. Fifth Amendment Due Process

It is not clear whether defendant's motion argues that the Dutch servers evidence should be suppressed because the searches violate defendant's Fifth Amendment due process rights. In case that was defendant's intent, I will address the merits of this argument.

To succeed on a claim that the "government's conduct in pursuit of evidence" violates a defendant's Fifth Amendment due process rights, "the government's method of acquiring the evidence must be so egregious that it 'shocks the conscience.'" United States v. Vega, No. 7-CR-707, 2012 WL 1925876, at *6 (E.D.N.Y. May 24, 2012) (quoting United States v. Salerno, 481 U.S. 739, 746 (1987).[3] The Second Circuit has said that "[t]he concept of fairness embodied in the Fifth Amendment due process guarantee is violated by government action that is fundamentally unfair or shocking to our traditional sense of justice, or conduct that is 'so outrageous' that common notions of fairness and decency would be offended were judicial processes invoked to obtain a conviction against the accused." United States v. Schmidt, 105 F.3d 82, 91 (2d Cir. 1997) (internal citations omitted). Conduct that shocks the conscience is

[3] Another district court has recognized that "in the context of motions to suppress evidence obtained in foreign countries, the Second Circuit has articulated the 'shock the conscience' standard only in reference to the conduct of foreign officials, who are not constrained by the Fourth Amendment." United States v. Yaroshenko, No. 09-CR-524, 2015 WL 3400805, at *3 n.4 (S.D.N.Y. May 21, 2015). For the purpose of this motion, I am assuming the Dutch authorities acted as agents of the Government; but even if they were not, defendant does not articulate how the Dutch authorities' conduct shocks the conscience. Indeed, the evidence suggests they followed all necessary procedural requirements in the Netherlands.

"extreme," and "[o]rdinarily . . . must involve either coercion . . . or violation of the defendant's person." Id. (internal citations omitted); see also United States v. Coke, No. 07 CR 971, 2011 WL 3738969, at *5 (S.D.N.Y. Aug. 22, 2011).

The Second Circuit has recognized that "[t]he investigation of crime increasingly requires the cooperation of foreign and United States law enforcement officials." United States v. Paternina-Vergara, 749 F.2d 993, 998 (2d Cir. 1984). Here, the Government worked cooperatively with foreign authorities to surveil servers that were located abroad. Defendant does not point to any specific misconduct by the Government, but instead, seems to challenge the entire process. [redacted] requested the Dutch authorities to alter their method of surveillance over the course of the investigation, defendant does not explain why this conduct was impermissible, and the Court does not see how the Government's conduct was improper.

IV. Motion to Suppress the FlexiSpy Data

Defendant's argument as to the FlexiSpy data proceeds in two steps: first, he argues that his Fourth Amendment rights were violated when the Government, [redacted] twice accessed the FlexiSpy accounts through the company's website and downloaded the data from defendant's accounts. Second, defendant argues that the FBI's searches of the contents of DVD1 and DVD2 under the first two warrants and its search of the Amazon Cloud server under the third warrant all violated the Fourth Amendment because the warrants were, for various reasons, facially and procedurally invalid under Federal Rule of Criminal Procedure 41.

A. Digital Duplication as a Fourth Amendment Search

As an initial matter, this opinion assumes that defendant has a Fourth Amendment right in his data stored on the Amazon Cloud server in the United States.[4] [redacted] downloading it to DVD1, DVD2, and an FBI server (respectively) were each "searches" within the meaning of the Fourth Amendment. However, those searches were reasonable and there was no constitutional violation.

As discussed above, a search occurs when "the government violates a subjective expectation of privacy that society recognizes as reasonable." Kyllo, 533 U.S. at 33. A seizure happens when "there is some meaningful interference with an individual's possessory interests in that property." Soldal, 506 U.S. at 61 (quoting Jacobsen, 466 U.S. at 113).

Most courts that have addressed duplication, including digital duplication, have analyzed it as a seizure. For example, the Supreme Court did so with the act of recording visible information, such as by photographing it or copying it down, and held that is not a seizure. See Arizona v. Hicks, 480 U.S. 321, 324 (1987). The Second Circuit used a similar analysis in Microsoft Corp. v. United States, 829 F.3d 197, 220 (2d Cir. 2016), vacated and remanded sub nom., United States v. Microsoft Corp., 138 S. Ct. 1186 (2018), concluding that the Government

[4] As the analysis in Part III makes clear, this assumption may not be warranted. The "sufficient connection" requirement in Verdugo-Urquidez could be read to extend to *domestic* searches of papers and effects of a foreign national. A handful of district courts have adopted this approach. See United States v. Gutierrez-Casada, 553 F. Supp. 2d 1259, 1265-66 (D. Kan. 2008); United States v. Esparza-Mendoza, 265 F. Supp. 2d 1254, 1273 (D. Utah 2003). But this reading of Verdugo-Urquidez is also in tension with the portion of that opinion that emphasized that the Fourth Amendment's purpose "was to restrict searches and seizures which might be conducted by the United States in domestic matters." 494 U.S. at 266. In the interest of completeness, the Court will address defendant's arguments assuming that he had a Fourth Amendment right in his data stored on a server in the United States.

had seized a customer's data when Microsoft moved the data from a foreign server to a domestic one at the Government's request. The Supreme Court has since vacated that opinion as moot, but its reasoning and conclusion still have persuasive value.

To support its argument that the digital duplication here was not a seizure, the Government cites cases where district courts reached the opposite conclusion by applying Hicks to the copying or transfer of electronic data. See In re Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-MJ-00757, 2017 WL 3445634, at *16 (D.D.C. July 31, 2017); In re Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 720 (E.D. Pa. Feb. 3, 2017); United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001). Those cases emphasize how the copying of data does not meaningfully interfere with the data owner's possessory interest because the copying does not alter the data itself or the owner's ability to access it.

I agree with the reasoning in these district court cases – it is difficult to see how digital duplication interferes with a *possessory* interest because copying does not damage the data or interfere with its owner's ability to use it. But duplication does interfere with the owner's control over that information, which could be understood as an interference with the owner's privacy interest in its contents.[5] At least one district court has applied similar reasoning to conclude that duplication of physical documents via high-resolution photographs is both a seizure and a search. See United States v. Jefferson, 571 F. Supp. 2d 696, 704 (E.D. Va. 2008). The Jefferson Court reasoned that the defendant's interest in the documents extended not just to the physical pieces of paper, but also to their contents. From there, the court concluded that the

[5] One commentator has characterized this as the "right to delete" and concluded that it is a meaningful interference with a possessory interest. See Paul Ohm, The Fourth Amendment Right to Delete, 119 Harv. L. Rev. F. 10, 11-12, 14-16 (2005); see also Note, Digital Duplications and the Fourth Amendment, 129 Harv. L. Rev. 1046 (2016).

officials taking photographs of the documents interfered with the defendant's interest in sole possession of the document's contents.

This view is also consistent with how the Supreme Court in Carpenter, 138 S. Ct. at 2217, characterized the cell-site location information that the Government obtained from the user's wireless carrier – as the "product of a search." Later in the opinion, the Supreme Court described the Government *accessing* that information previously recorded by his carrier as an invasion of the appellant's "reasonable expectation of privacy in the whole of his physical movements." Id. at 2219. Although Carpenter was decided in the context of cell-site location information, it is significant that the Supreme Court categorized the Government's acquisition of that information as a search, not a seizure. [redacted], that act was a search within the meaning of the Fourth Amendment because it interfered with defendant's privacy interest in his data's contents.

However, the Fourth Amendment only protects against *unreasonable* searches and seizures and this one was certainly reasonable. As described above, defendant was an escaped prisoner with no objectively reasonable expectation of privacy in his electronic communications, including those recorded using the FlexiSpy software. [redacted]

Similar to the Dutch servers evidence discussed in Part III, even if the downloading of the FlexiSpy data is characterized as a seizure rather than a search, that seizure would still have been reasonable in light of the Government's need to avoid destruction of the evidence. Defendant

does not contest the Government's argument that it had probable cause to search or seize the FlexiSpy data. See Martin, 157 F.3d at 53.

Here, the first and second warrants, [redacted], were issued after two different magistrate judges determined that the Government had shown probable cause to believe that the DVDs contained evidence of criminal activity. [redacted] the Government was aware that defendant and his co-conspirators regularly accessed the FlexiSpy data and that they sometimes deleted it. Seizing the data was therefore, as with the Dutch servers information, necessary to avoid "loss or destruction of suspected contraband." Martin, 157 F.3d at 53 (internal quotation marks omitted). The risk that electronic data might be destroyed is of course frequently present; here, the Government knew that defendant and his co-conspirators had deleted the data before and had access to the information whenever they wanted, which made the Government's fear of its potential destruction particularly reasonable.[6] See id.; United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001).

Finally, [redacted], the independent source doctrine would counsel against suppression here. This doctrine grows out of the underlying rationale for exclusionary rule itself: excluding "evidence that is the fruit of unlawful police conduct . . . is

[6] It is not clear whether defendant intended to argue that there was an unconstitutional delay in procuring the first search warrant on January 6, 2012 [redacted]. See Martin, 157 F.3d at 46. But to the extent he does, the argument would fail. Courts have routinely upheld periods similar to the 15-day delay here between procuring the information and searching it, where, as here, law enforcement's retaining the thing to be searched did not interfere with defendant's ability to use it and where the delay included weekends and holidays. See id. at 54 (11 days, including two weekends and Christmas); United States v. Okparaeka, No. 17-CR-225, 2018 WL 3323822, at *7 (S.D.N.Y. July 5, 2018) (19 days, including three weekends and Passover); United States v. Mathews, No. 18-CR-124, 2018 WL 2277839, at *3 (S.D.N.Y. May 17, 2018) (17 days, including two weekends and Christmas).

needed to deter police from violations of constitutional and statutory protections," but suppressing evidence that was discovered "by means wholly independent of any constitutional violation" would neither further that goal nor promote justice generally. Nix v. Williams, 467 U.S. 431, 442 (1984). Therefore, where a search pursuant to a warrant is preceded by a warrantless search, the question is whether "(1) the warrant [was] supported by probable cause derived from sources independent of the illegal[ity]; and (2) the decision to seek the warrant [was not] prompted by information gleaned from the illegal conduct." United States v. Nayyar, 221 F. Supp. 3d 454, 466 (S.D.N.Y. 2016) (quoting United States v. Johnson, 994 F.2d 980, 987 (2d Cir. 1993)); see also Murray v. United States, 487 U.S. 533, 541-43 (1988).

As noted above, defendant does not contest that the first and second search warrants were supported by probable cause, so the first element is satisfied. That the second element is satisfied is evident from the warrant applications themselves: the application for a warrant to search DVD1 does not mention its contents as a reason for the search and the application for a warrant to search DVD2 mentions only the contents of DVD1, which was searched pursuant to the first warrant.

Therefore, [redacted] – and for all of the reasons stated above, the Court concludes that it was not – the Court would not suppress the evidence from that search because when the Government did search the DVDs, it was pursuant to untainted warrants.

B. Challenges to the Warrants' Facial and Procedural Validity

Defendant next challenges the warrants that the FBI procured to search the contents of DVD1 and DVD2 and to search the Amazon Cloud server directly as facially and procedurally invalid under Federal Rule of Criminal Procedure 41. These challenges also fail.

1. Warrants' Facial Validity

To comply with the Fourth Amendment, a warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. A warrant must therefore (1) "identify the specific offense for which the police have established probable cause"; (2) "describe the place to be searched"; and (3) "specify the items to be seized by their relation to the designated crimes." United States v. Galpin, 720 F.3d 436, 445-46 (2d Cir. 2013) (internal quotation marks and citation omitted).

Defendant argues that these warrants do not describe with sufficient particularity the place to be searched or the specific offense. Defendant only challenges the description of the place to be searched in the third warrant[7].

As defendant states, the third warrant describes the place to be searched as "FlexiSpy accounts associated with usernames: [list of 35 FlexiSpy account names], which is controlled by Amazon and stored on the Amazon Cloud Server." The 35 FlexiSpy account names, not the entire Amazon Cloud server, constitute the "place" to be searched. See, e.g., United States v. Westley, No. 17-CR-171, 2018 WL 3448161, at *12 (D. Conn. July 17, 2018). Although a user's account is not a physical location, specifying the username limits the place where information can be searched in the same way a description of an address or room or object would. Even if the third warrant had not been limited to 35 of defendant's FlexiSpy account names, the all-records exception would likely apply here and render a search of all of defendant's FlexiSpy accounts valid. See United States v. Ulbricht, 858 F.3d 71, 102 (2d Cir. 2017). The third warrant is therefore particularized as to the place to be searched.

[7] The third warrant is really two warrants, a search warrant and a tracking warrant, but the applications for both warrants were supported by the same joint materials and both have the same Attachment A.

Defendant's argument on the second point seems to be that because the first and second warrants did not list the particular statutes under which he was charged, they did not state the particular offenses as required. The Government counters that the specific statutes for which it had probable cause to search were listed in its warrant applications and in the affidavits submitted with them.

Both sides are wrong on the law. It is well established that the Government cannot rely on a representation in its warrant application or the affidavit in support of it where those documents are not incorporated by reference or attached to the warrant itself. See Groh v. Ramirez, 540 U.S. 551, 557 (2004). None of the search warrants at issue here incorporate the Government's application or its affidavit by reference and neither are attached to the warrant, so this argument fails.

Defendant, on the other hand, does not cite any caselaw to support his argument that the warrant must list a particular statute and the Court has not found any. "Attachment A" to all three warrants lists the specific offenses for which the Government had probable cause to search: "trafficking of narcotics or laundering of drug proceeds." Because Attachment A was attached to and incorporated by reference in the warrants (unlike the Government's application and affidavit), its contents are considered part of the warrant. See id. at 557-58; United States v. George, 975 F.2d 72, 76 (2d Cir. 1992).

The Second Circuit has consistently upheld warrants that do not reference a particular statutory provision where the warrant provides a description of the crime alleged similar to the one in Attachment A here. For example, in United States v. Bianco, 998 F.2d 1112, 1115-16 (2d Cir. 1993), the Second Circuit upheld the validity of a warrant[8] that described the particular

[8] In Bianco, the warrant itself did not contain any reference to a crime; the Second Circuit looked to the supporting affidavit of the special agent, which said that the agents were "looking for evidence of [defendant's] loansharking."

offense for which the evidence is sought as "loansharking." By contrast, in United States v. George, 975 F.2d 72, 75 (2d Cir. 1992), the Second Circuit concluded that a warrant authorizing the police to search for "any other evidence relating to the commission of a crime" was impermissibly broad. The George Court distinguished the warrant before it from others the Court had approved that authorized the seizure of "evidence" or generic classes of items where a more precise definition was not possible and that "identified a specific illegal activity to which the items related." Id. at 76. The George Court made clear that a warrant is insufficient in this respect only when it combines both general categories of evidence to be seized *and* general categories of criminal behavior.

Attachment A to the first and second warrants specified certain categories of information (including text messages, Blackberry messages, and call logs/toll records) that "appear to be pertinent to the trafficking of narcotics or laundering of drug proceeds," which is a sufficiently particular description of the specific offense for which the police have established probable cause under the Fourth Amendment.

2. Warrants' Procedural Validity

Finally, defendant argues that the third FlexiSpy warrant (the tracking and search warrant), violates the venue provision in Federal Rule of Criminal Procedure 41(b) and the requirement in Rule 41(e)(2)(C) that the warrant identify the property to be tracked and the judge to whom the tracked information should be returned.

Defendant's venue argument is based on the fact that the warrant was issued by a magistrate judge in the Southern District of New York for electronic data located in the Western

---

998 F.2d at 1115. Groh overruled the practice of consulting a supporting affidavit the way the Bianco Court did, unless the parameters described above are met. But the point is that "loansharking," although it appeared in the wrong place in Bianco, was a sufficiently particular description of the crime.

District of Washington. First, although Rule 41(b) does not appear to provide a basis for the magistrate judge to have issued the warrant in the Southern District of New York,[9] the Stored Communications Act, 18 U.S.C. § 2701, does. That statute "regulates search and seizure of electronic evidence" in the possession of a "remote computing service." United States v. Scully, 108 F. Supp. 3d 59, 82 (E.D.N.Y. 2015) (internal quotation marks omitted). A remote computing service is "the provision to the public of computer storage or processing services by means of an electronic communications system," 18 U.S.C. § 2711(3), which covers the Amazon Cloud server.

The venue provision in the Stored Communications Act permits a district court or magistrate judge "that . . . has jurisdiction over the offense being investigated" to issue a warrant for "any wire or electronic communication" that is held or maintained by that service "on behalf of, and received by means of electronic transmission from . . . a subscriber or customer or such remote computing service." Id. §§ 2703(b)(2), 2711(3).

Under the Stored Communications Act, such a warrant should be issued "using the procedures described in the Federal Rules of Criminal Procedure." Id. § 2703(b)(1)(A). Although the "procedures" could be understood to include the venue requirements for Rule 41(b), the Court agrees with other courts to consider this question that they are more naturally read to refer to the process-related requirements, such as those in Rule 41(d), (e), and (f). See United States v. Berkos, 543 F.3d 392, 397 (7th Cir. 2008); Scully, 108 F. Supp. 3d at 82.

[9] The Government argues that Rule 41(b)(6) did not go into effect until December 2016, so the agents here should not be penalized for failing to anticipate its requirements. That is certainly true, but the Government conveniently omits that none of the subsections of Rule 41(b) that were in effect when the warrant was issued in 2012 provided for proper venue either.

Furthermore, even if the third warrant (the Flexispy and tracking warrants) violated Rule 41(b) and was invalid under the Stored Communications Act, suppression would not be an appropriate remedy here because the purposes of the exclusionary rule are not satisfied.

As discussed above, "[a]pplication of the exclusionary rule depends on the 'efficacy of the rule in deterring Fourth Amendment violations in the future' as well as a determination that 'the benefits of deterrence . . . outweigh the costs.'" United States v. Rosa, 626 F.3d 56, 64 (2d Cir. 2010) (quoting Herring v. United States, 555 U.S. 135, 140 (2009)). Because its primary purpose is to incentivize officers to follow the law, the extent to which evidence should be excluded "varies with the culpability of law enforcement." Herring, 555 U.S. at 143. Specifically, the question is whether "a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances." Id. at 146. The Court is mindful of the Supreme Court's observation that "exclusion has always been our last resort, not our first impulse." Id. at 140.

Here, there is no evidence that the agents intentionally disregarded the venue requirement of Rule 41(b). Generally, a warrant issued by a neutral magistrate establishes that the law enforcement officer has "acted in good faith in conducting the search," so long as the officer's "reliance on the magistrate's probable-cause determination and on the technical sufficiency of the warrant . . . [is] objectively reasonable." United States v. Leon, 468 U.S. 897, 922 (1984); see also Massachusetts v. Sheppard, 468 U.S. 981, 989-90 (1984). The defects that defendant alleges in the third warrant are, at worst, mistakes made in issuing the warrant, not in the factual materials provided in the warrant application. Defendant does not, for example, allege that the magistrate judge was misled by information in the affidavit that the affiant agent knew to be

false. Nor is this the kind of warrant that is "so facially deficient" that an officer could not reasonably presume it was valid. Cf. Groh, 540 U.S. at 565.

Any lack of authority by the magistrate judge to issue the warrant has little effect on police misconduct, which is the harm that suppression is designed to disincentivize. Here, suppression is not warranted because it was objectively reasonable for the agents to rely in good faith on the search and tracking warrants in the third warrant application, which were executed by two different magistrate judges. See United States v. Raymonda, 780 F.3d 105, 118 (2d Cir. 2015).

Defendant's other arguments are also meritless. He argues that the tracking warrant does not identify the property to be tracked or the magistrate judge to whom it must be returned, but the warrant states that the property to be tracked is the "Location Data Contained in the FlexiSpy Accounts Listed in Attachment A," which in turn specifies the 35 accounts from which the FBI agents would obtain the location data. As described above, Attachment A is part of the warrant because it was explicitly incorporated by reference and attached to the warrant itself. Furthermore, even though the warrant identified the Clerk of Court, rather than a particular judge, as the person to whom the information should be returned, this technical error is just that. Defendant incurred no prejudice because of this oversight. See United States v. Turner, 781 F.3d 374, 386 (8th Cir. 2015); United States v. Salazar, No. 16-cr-264, 2017 WL 1365110, at *8 (D. Minn. Mar. 23, 2017).

CONCLUSION

Defendant's [263] and [264] motions to suppress are DENIED.

SO ORDERED.

Digitally signed by Brian M. Cogan

U.S.D.J.

Dated: Brooklyn, New York
August 29, 2018