UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF IDAHO

UNITED STATES OF AMERICA, Plaintiff, v. PAVEL BABICHENKO, GENNADY BABITCHENKO, PIOTR BABICHENKO, TIMOFEY BABICHENKO, KRISTINA BABICHENKO, NATALYA BABICHENKO, DAVID BIBIKOV, ANNA IYERUSALIMETS, MIKHAIL IYERUSALIMETS, ARTUR PUPKO, Defendants.	Case No. 1:18-CR-00258-BLW **MEMORANDUM DECISION AND ORDER**

INTRODUCTION

Before the Court is Defendants' Joint Motion to Suppress Electronic Communications and Electronically Stored Information. Dkt. 554. The motion is fully briefed and ripe for the Court's determination. After careful review of the briefing, the Court finds there is no significant disputed factual issue relevant to resolution of the motion. *See United States v. Walczak*, 783 F.2d 852, 857 (9th

Cir.1986); *see also United States v. Howell*, 231 F.3d 615, 620–21 (9th Cir. 2000). Therefore, oral argument is unnecessary, and the Court will decide the motion on the briefs. For the reasons explained below, the Court will deny the motion.

BACKGROUND

The Defendants were arrested on charges alleging a decade-long criminal scheme to sell counterfeit cell phones and launder the proceeds. In conducting the investigation, the government obtained search warrants for three warehouses, seven residences, various email accounts, and vehicles. 18-mj-10168; 18-mj-10186; 17-mj-09912; 17-mj-09887; 18-cr-00258 Dkt. 510-3.

Agents seized 184 devices from the searched premises, and searched 27 of those devices. Dkt. 571 at 3–4. From the 27 searched devices, 24 were tagged as having evidentiary value. *Id.* at 4. The government produced to the defense the documents and media from the 24 tagged devices, totaling 49.31 GB (approximately 5,410 documents). *Id.* The government states they will not seek to admit anything from the remaining devices as evidence in its case in chief. *Id.* at 4 n.3.

Six of the 24 tagged devices were seized from the Bridger Street Warehouses, while the remaining 18 devices were seized from personal residences. All but one of those devices were seized from the Defendants' residences. The

final device, Device 24, was seized from the residence of Elizaveta Babichenko, who is the mother of some of the Defendants.

The Defendants argue the warrants violate the Fourth Amendment because they are overbroad and were improperly executed by the government. *See* Dkt. 554.

LEGAL STANDARD

The Fourth Amendment requires that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, particularly describing the place to be searched and the persons or things to be seized." U.S. Const. Amend. IV. To meet the Fourth Amendment's particularity requirement, a warrant must (1) "identify the specific offense for which the police have established probable cause," (2) "described the place to be searched," and (3) "specify the items to be seized by their relation to designated crimes." *United States v. Ulbricht*, 858 F.3d 71, 99 (2d Cir. 2017) (internal citation omitted).

A warrant may authorize the seizure of electronic data, and "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." Fed. R. Crim. P. 41(e)(2)(B). Search warrants for electronic data pose a serious risk of violating the particularity requirement because of the potential to include large amounts of irrelevant,

personal information. *Ulbricht*, 858 F.3d at 99-100. Warrants for electronic data that fail to "link the evidence sought to the criminal activity supported by probable cause" do not satisfy the particularity requirement. *Id.* (quoting *United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010)). However, search warrants for electronic data "may contain some ambiguity so long as law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant." *Ulbricht*, 858 F.3d 99-100 (internal quotation marks omitted).

ANALYSIS

The Defendants argue the search warrants were overbroad and improperly executed by the Government's agents. As explained below, the Court finds the warrants are not overbroad and were properly executed by the Government.[1] Further, even if the warrants were invalid, the good faith exception applies. Finally, because the Government has not moved to introduce any evidence beyond the scope of the warrants, suppression is not required.

[1] The Government also argues the Defendants lack standing to argue for suppression of the 6 devices seized from the Bridger Street warehouses and the residence of Elizaveta Babichenko. *See* Dkt. 571. As explained below, the Court will agree with the Government's assertions.

A. Overbreadth

The Defendants argue the search warrants, which produced over 75 terabytes of evidence, are overbroad. Dkt. 554-1. Courts consider three factors to analyze the breadth of a warrant: (1) "whether probable cause existed to seize all items of a category described in the warrant," (2) "whether the warrant set forth objective standards by which executing officers could differentiate items subject to seizure from those which were not," and (3) "whether the government could have described the items more particularly in light of the information available." *United States v. Flores*, 802 F.3d 1028, 1044 (9th Cir. 2015) (quoting *United States v. Lei Shi*, 525 F.3d 709, 731–32 (9th Cir. 2008)).

The Defendants do not contest the existence of probable cause to conduct the searches. *See* Dkt. 554-1. Rather, they argue the warrants allowing the search of the warehouses, residences, and email accounts were facially overbroad because they failed to limit the Government's search to information encompassed in the warrant. Dkt. 554-1 at 5. However, "a search warrant does not necessarily lack particularity simply because it is broad." *Ulbricht*, 858 F.3d at 100. A warrant may broadly authorize the government to search "a wide range of potentially relevant material, without violating the particularity requirement." *Id.* Further, "[w]hen the criminal activity pervades [an] entire business, seizure of all records of the

business is appropriate, and broad language used in warrants will not offend the particularity requirements." *U.S. Postal Serv. v. C.E.C. Servs.*, 869 F.2d 184, 187 (2d Cr. 1989). Some invasion of a criminal defendant's privacy is inevitable in almost any search. *Ulbricht*, 858 F.3d at 100. Even traditional searches for paper records inevitably include information irrelevant to the object of the search. *Id.*

1. Warehouses and Residences

First, the search warrants for the warehouses and residences, though vast, were not overbroad. The warrants provided objective standards by which the executing officers could determine which items to seize by limiting the search to records relating to the alleged offenses. *See* 18-mj-10168 Dkt. 1-11. The warrants and supporting affidavit describe the alleged decade-long scheme of criminal activity and each location's relation to that scheme. *Id.*

The Defendants claim the warrant allowed the Government to seize "any form of computer or electronic storage." Dkt. 554-1 at 5. However, the warrants limited the seizure to "[c]omputers or storage media used as a means to commit the violations of 18 U.S.C. §§ 1341, 1343, 1956(h), and 2320." 18-mj-10186 Dkt. 2 at 6. Moreover, the supporting affidavit describes the nature of the crimes at issue, each of the defendants, and their relation to the areas being searched. 18-mj-10168 Dkt 1. This is far different from the facts in *United States v. SDI Future Health,*

Inc., where the Ninth Circuit held a warrant overbroad because it allowed the search team to seize records wholly unrelated to the defendants by failing to describe the crimes and individuals being charged. 568 F.3d 684 (9th Cir. 2009).

The Defendants also note the Government's seizure of the computers included personal emails from Bibikov's wife, Ruth, dating back to 2009 when she was 14 years old. Dkt. 554-1 at 7. However, the alleged crimes date back to 2008. 18-mj-10186 Dkt.1 at 5. Without seizing and searching the computers, the Government had no way of knowing whether these emails would pertain to the alleged crimes. *See United States v. Cummings*, No. CR1700518001TUCRMJR, 2020 WL 1983342 (D. Ariz. Apr. 27, 2020) (holding a warrant was not overbroad because "it would be impossible for the Government to know the contents of the emails before reviewing them"); *see also United States v. Adjani*, 452 F.3d 110, 1149-50 (9th Cir. 2006) (rejecting the argument that the government should have narrowed its search of the defendant's email because restricting the search "would likely have failed to cast a sufficiently wide net to capture the evidence sought").

Further, Courts uphold broad seizures of business records where there is probable cause that the entire business was engaged in fraudulent conduct. *See United States v. Offices Known as 50 State Distrib. Co.*, 708 F.2d 1371, 1374 (9th Cir. 1983) (holding a warrant was not overbroad because "fraud permeated the

entire business operation"). Here, the affidavit in support of the warrants provided probable cause that the Defendants operated "over a hundred separate business entities to sell their counterfeit goods online to thousands of customers." 18-mj-10186 Dkt. 1 at 6. The affidavit further describes each of the warehouses and residences along with their relevance to the businesses under investigation. For example, the 9799 West Preece Street residence was listed by the Defendants multiple times as the business mailing address for their various allegedly fraudulent businesses. *Id.* at 26. The allegations of trafficking in counterfeit goods permeated the entirety of the Defendants' many businesses, and thus the broad nature of the warrants is justified.

2. Email Accounts

Next, the Defendants argue the email warrants were overbroad because they lacked temporal restrictions. Dkt. 554-1 at 9. Ten of the twelve warrants authorized the search of business emails registered with Amazon accounts from which the FBI purchased allegedly counterfeit phones. *See* 18-mj-10168 Dkt. 1. For example, bibbyselectronics@gmail.com was registered with Amazon in 2016 as the email for the account "Bibby's Electronics" from which the FBI purchased an allegedly counterfeit iPhone 6. *Id.* at 9. Because the alleged crimes date back to 2008, imposing a temporal restriction limiting the seizure of evidence to post-2008

records for an account that was not created until 2016 would be unnecessary. The other nine business email accounts are similarly situated, with the earliest account being registered in 2010. *Id.* at 12. The only warrant directly authorizing the search of a personal email account not registered with an online seller (davebibi5@gmail.com) included a temporal restriction limiting the seizure to information from February 1 to August 21, 2018. 18-cr-258 Dkt. 510-3.

Further, the Defendants note that one warrant, authorizing the search of g.distributing@gmail.com, erroneously cited offenses relating to controlled substances. Dkt. 554-1 at 8. However, the first warrant for this account was never executed (17-mj-09887 Dkt. 3) and the second was rejected by Google (17-mj-09912 Dkt. 7). Only the third warrant, which did not reference crimes relating to controlled substances, was actually executed. 18-mj-10168 Dkt. 5.

B. Improper Execution

Next, the Defendants argue the Government improperly executed the warrants by retaining the electronic data, rather than segregating and sealing the unresponsive information. Dkt. 554-1 at 10. In this argument, the Defendants cite Rule 41 of the Federal Rules of Criminal Procedure. They argue this rule mandates a two-step process wherein the Government seizes electronic information, then separates irrelevant material and seals it from further warrantless investigation. *Id.*

at 10-11. However, Rule 41 only states that a warrant for electronic data "authorizes a later review of the media or information consistent with the warrant" and allows the officers to "retain a copy of the electronically stored information that was seized or copied." Fed. R. Crim. P. 41(e)(2)(B); 41(f)(1)(B). The rule thus allows the Government to seize electronic information and later search its contents for relevant material, but does not mandate any procedural safeguards requiring the Government to segregate and seal nonresponsive information.

Though courts have referenced procedural safeguards as evidence that a warrant is not overbroad, the Ninth Circuit has made it clear that this is only a factor relevant to the warrant's breadth, rather than a constitutional requirement. *See United States v. Schesso*, 730 F.3d 1040, 1049 (9th Cir. 2013) (the search protocols suggested by the concurring opinion in *CDT* [involving a segregate-and-seal process] were not constitutional requirements, but rather mere "guidance" to offer the government a "safe harbor"). In *Schesso*, the Ninth Circuit held the warrant's lack of procedural safeguards did not violate the Fourth Amendment nor the court's previous holdings recognizing the benefits of those protocols. *Id.*

Here, the warrants' lack of procedural safeguards alone is insufficient to show their execution was improper. Instead, the descriptive information of the alleged crimes and their relation to the searched areas indicate the warrants were

not overbroad. The Government properly and timely executed the warrants according to their terms. The warrants did not prescribe the procedural safeguards urged by the Defendants, nor a time limit on the search process. Courts find time-consuming searches of computer data are not unreasonable. *See United States v. Johnston*, 789 F.3d 934 (9th Cir. 2015) (holding a five-year search was reasonable). Undoubtably, the amount of evidence seized is vast. However, considering that this is an investigation involving allegations of a decade-long criminal scheme involving ten defendants and over a hundred businesses, this large amount of evidence is not unreasonable, and the time required to search its contents is understandably lengthy.

C. Good Faith Exception

The Defendants claim the lack of procedural safeguards made the Government's reliance on the warrants unreasonable, barring an application of the good faith exception. Dkt. 554-1 at 13. The good faith exception precludes the exclusion of evidence obtained by police if the police conducted the search in "objectively reasonable reliance" on a warrant later held invalid. *United States v. Leon*, 469 U.S. 897, 922 (1984). The good faith exception does not apply when the warrant is "so facially overbroad as to preclude reasonable reliance by the executing officers." *United States v. Michaelian*, 803 F.2d 1042, 1046 (9th Cir.

1986). However, courts find the officers reasonably relied on sufficiently descriptive warrants, even if they lacked temporal limits or procedural safeguards. *See, e.g.*, *United States v. Martinez*, No. 19-CR-00662-JSW-1, 2020 WL 3050767 (N.D. Cal. June 8, 2020) (holding the officers reasonably relied on a warrant even though it lacked temporal limits because it specified the types of evidence to be seized and described the illegal activities at issue). Further, courts apply the good faith exception where the judge issuing the warrant was not misled by the information in the affidavit, the judge did not wholly abandon his judicial role, and the affidavit was not so lacking in probable cause as to render belief in it entirely unreasonable. *Schesso*, 730 F.3d at 1050.

Here, there is no allegation that the warrants lacked sufficient probable cause, the affidavits contained misleading information, or the magistrate judge abandoned her judicial role. Rather, the Defendants argue the lack of procedural safeguards rendered the officers' reliance on the warrants unreasonable. However, as stated above, the lack of procedural safeguards did not render the warrants invalid. Moreover, the executing officers reasonably relied on the warrants, which contained in-depth descriptions of the defendants, their businesses, and the illegal activity at issue. 18-mj-10186-CWD Dkt 1. Thus, even if the warrants were overbroad, the good faith exception would prevent any suppression of evidence.

D. Suppression of Evidence

Finally, even if the warrants were overbroad and the good faith exception did not apply, the Government has not moved to introduce any evidence that exceeds the scope of the warrants. Courts deny motions to suppress evidence obtained by overbroad warrants if the evidence actually admitted at trial is not beyond the scope of the warrant. For example, in *Flores* the Ninth Circuit upheld a district court's refusal to suppress evidence obtained from the defendant's Facebook account because, though the government seized over 11,000 pages of data, they only admitted 2 messages at trial. 802 F.3d at 1046. Both messages fell within the scope of the warrant. *Id. See also Cummings* at *10 (holding suppression was only necessary if the government tried to introduce evidence beyond the scope of the warrant at trial).

The Defendants broadly argue for the suppression of all evidence obtained from the search warrants at issue. However, the Government has indicated they only intend to introduce evidence from the 24 tagged devices (constituting 0.066% of the 75 terabytes of data initially seized). Dkt. 571 at 4 n.3. Thus, unless the Government moves to introduce evidence beyond the scope of the warrants at trial, the Court need not suppress all evidence obtained from the search warrants at issue.

E. Standing

Though the Court finds the Defendants' motion fails on the merits, the Court also notes the Defendants lack standing to argue a Fourth Amendment violation regarding the warrants for Elizaveta Babichenko's residence, Arthur Pupko's email accounts, and the Bridger Street warehouses.

1. Residence and Email Accounts

Regarding the warrants for Elizaveta's residence and Pupko's email accounts, the Defendants lack standing because they cannot argue a Fourth Amendment violation on behalf of a third party. *See United States v. Padilla,* 508 U.S. 77, 81 (1993) ("It has long been the rule that a defendant can urge the suppression of evidence obtained in violation of the Fourth Amendment only if that defendant demonstrates that his Fourth Amendment rights were violated by the challenged search or seizure."). A party only has standing to argue a violation of Fourth Amendment rights if his reasonable expectation of privacy has personally been infringed. *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 695 (9th Cir. 2009) ("*SDI*"). Because the residence and email accounts did not belong the Defendants and they did not have a reasonable expectation of privacy therein, they lack standing to argue a Fourth Amendment violation regarding those warrants.

2. Bridger Street Warehouses

Regarding the warrants for the Bridger Street warehouses, the Defendants

lack standing because they fail to show they had a reasonable expectation of privacy at these workplaces. "[A] criminal defendant may invoke the protections of the Fourth Amendment only if he can show that he had a legitimate expectation of privacy in the place searched or the item seized." *United States v. Ziegler*, 474 F.3d 1184, 1199 (9th Cir. 2005). "This expectation is established where the claimant can show: (1) a subjective expectation of privacy; and (2) an objectively reasonable expectation of privacy." *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

While residences are afforded a "nearly absolute protection," workplaces do not immediately offer an expectation of privacy. *SDI*, 568 F.3d at 696. In workplaces, courts determine whether there was a reasonable expectation of privacy on case-by-case basis. *Id.* The Ninth Circuit has concluded that, "except in the case of a small business over which an individual exercises daily management and control, an individual challenging a search of workplace areas beyond his own internal office must generally show some personal connection to the places searched and materials seized." *Id.* at 698.

Here, there is no evidence before the Court of the Defendant's personal connection to the Bridger Street Warehouses, nor the devices seized therein. Therefore, the Defendants lack standing to challenge the search warrants for those warehouses.

For the foregoing reasons, the Court will deny the Defendants' Motion to Suppress.

ORDER

IT IS ORDERED that:

1. Defendant's Motion to Suppress (Dkt. 554) is **DENIED**.

DATED: July 16, 2020

B. Lynn Winmill
U.S. District Court Judge