United States District Court
District of Massachusetts

UNITED STATES OF AMERICA,	)	
	)	
Government,	)	
	)	
v.	)	**Criminal Action No. 15-10131-NMG**
	)	
AMIT KANODIA,	)	
	)	
Defendant.	)	
	)	

MEMORANDUM & ORDER

GORTON, J.

Defendant Amit Kanodia ("Kanodia" or "defendant") has been indicted for Conspiracy to Commit Securities Fraud (Count 1) for allegedly conspiring in 2013 to engage in insider trading of shares of Cooper Tire & Rubber Company ("Cooper Tire"), all in violation of 15 U.S.C. § 78j(b) and 78ff(a), 18 U.S.C. § 371 and 17 C.F.R. § 240.10b-5 ("Rule 10b-5"). Kanodia has also been indicted on 18 counts of securities fraud (Counts 2-19) in violation of 15 U.S.C. § 78j(b) and 78ff(a), 18 U.S.C. § 2 and Rule 10b-5.

Pending before the Court is Kanodia's motion to suppress evidence that the government obtained pursuant to a search warrant directed to Network Solutions, LLC ("Network Solutions") for e-mail communications and account data associated with the

e-mail address AK@LincolnVentures.com. For the reasons that follow, that motion will be denied.

I. Background

A. Parties

Kanodia is charged with engaging in insider trading after misappropriating material, nonpublic information that he obtained from his wife, the General Counsel of Apollo Tyres, Ltd. ("Apollo"), concerning an anticipated merger between Apollo and Cooper Tire. Kanodia purportedly disclosed that information to co-defendant Iftikar Ahmed ("Ahmed" or "co-defendant") and family friend Steven Watson ("Watson") with the understanding and intent that they use the inside information to trade in shares of Cooper Tire and share their profits with him.

The indictment alleges that Ahmed and Watson then began accumulating Cooper Tire shares and call options in April, 2013 and continued doing so until shortly before the public announcement of the merger in June, 2013. Ahmed and Watson allegedly sold their interests in Cooper Tire within a few days after the announcement and collectively garnered over one million dollars in proceeds.

In early August, 2013, Kanodia sent Ahmed an e-mail with the subject line of "Wire Instructions" from the AK@LincolnVentures.com e-mail account. He wrote:

> Dear Ifty Bhai:
> Hope all is well. Finally we have all the documents in place . . . The entity is:
> Lincoln Charitable Foundation
> Bank of America
> Account # ********7712
> ABA: *****9593
> West 33rd Street, New York, NY
> Telephone 617 713 6301

The government explains that 1) the e-mail was signed "Salaam. amit", 2) "bhai" is an Indian term for "brother", 3) "salaam" is a salutation meaning "peace" and 4) both Kanodia and Ahmed had ties to India.

During its investigation, the government applied for a warrant to search the AK@LincolnVentures.com e-mail account for evidence, fruits and instrumentalities of wire fraud, securities fraud and conspiracy. The warrant application included an affidavit from a Federal Bureau of Investigation ("FBI") agent that 1) summarized the alleged insider trading scheme and the relationship between the participants, 2) described the August, 2013 e-mail that Kanodia sent to Ahmed from the account, 3) outlined the procedures for executing the search warrant and 4) identified the "Accounts and Files to Be Copied by Network Solutions Personnel" and the "Records and Data to [B]e Searched and Seized by Law Enforcement Personnel". Magistrate Judge Marianne B. Bowler approved and issued the search warrant in October, 2014.

An FBI agent served a copy of the warrant on Network Solutions. The government received a disk of materials from Network Solutions and produced a copy of those materials to Kanodia in discovery.

In February, 2016, Kanodia moved to suppress "any substantive communications, or any fruits of such evidence," that the government unlawfully seized pursuant to the Network Solutions search warrant.

II. Motion to suppress

A. Legal standard

The Fourth Amendment of the United States Constitution protects against unreasonable searches and seizures. U.S. CONST. AMEND. IV. Law enforcement officers must generally secure a warrant supported by probable cause before conducting a search or seizure. United States v. Gifford, 727 F.3d 92, 98 (1st Cir. 2013). Under the particularity requirement, a search warrant 1) must include sufficient information to guide and control the judgment of the executing officer in deciding where to search and what to seize and 2) cannot be overbroad or include items that should not be seized. United States v. Kuc, 737 F.3d 129, 133 (1st Cir. 2013).

> An application for a search warrant must establish probable cause to believe that (1) a crime has been committed – the "commission" element, and (2) enumerated

> evidence of the offense will be found at the place to be searched – the so-called "nexus" element.

United States v. Feliz, 182 F.3d 82, 86 (1st Cir. 1999). With respect to the nexus element, the magistrate judge must consider the totality of the circumstances and make a "practical, common-sense decision" as to whether there is a "fair probability" that evidence of a crime will be found in a particular place. Id. The party seeking the warrant must present facts that would "warrant a man of reasonable caution to believe that evidence of a crime will be found" but need not show that such a belief is correct or more likely true than false. Id.

A reviewing court must treat with "considerable deference" the determination of the magistrate judge that the warrant application established probable cause. Id. The proper inquiry on review is whether the magistrate judge had a "substantial basis for concluding that probable cause existed." Id. (internal quotation marks omitted). The reviewing court should resolve doubtful or marginal cases in favor of the magistrate judge's finding of probable cause. United States v. Barnard, 299 F.3d 90, 93 (1st Cir. 2002).

If the reviewing court determines that the magistrate judge issued the warrant without probable cause, the evidence collected pursuant to the warrant will be suppressed. See Gifford, 727 F.3d at 98.

B. Application

Kanodia seeks to suppress the evidence obtained from the Network Solutions search warrant because he claims that the warrant 1) was issued outside of the territorial scope of the magistrate judge's authority, 2) was not supported by probable cause, 3) did not identify the items to be seized with particularity and 4) did not set forth a search protocol to minimize the risk of collecting materials that fell outside the scope of the warrant.

1. Judicial authority

Kanodia first contends that Magistrate Judge Bowler exceeded her judicial authority when she issued the Network Solutions warrant which authorized a search and seizure of electronic data located in the Middle District of Florida.

> The Federal Magistrates Act provides magistrate judges with all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts . . . .

28 U.S.C. § 636(a)(1). Fed. R. Crim. P. 41 regulates the issuance of search warrants and authorizes magistrate judges to issue search warrants for property 1) within the district, 2) within the district at the time of issuance but possibly outside of the district at the time of execution, 3) in connection with a terrorism investigation or 4) outside of the district but within any United States a) territory, possession

or commonwealth or b) diplomatic or consular residences or premises in a foreign state. Fed. R. Crim. P. 41(b)(1)-(3), (5).

Kanodia asserts that none of the Rule 41(b) provisions permits a magistrate judge, sitting in the District of Massachusetts, to issue a search warrant for property located in Florida at the time of the issuance and execution of the warrant. He claims that suppression is required because Magistrate Judge Bowler did not have the judicial authority to issue the Network Solutions search warrant for out-of-state property.

Kanodia's argument overlooks the fact that Rule 41(b) does not apply in this case because the rule, on its face, does not modify any statute regulating the issuance or execution of a search warrant in special circumstances. Fed. R. Crim. P. 41(a)(1).

Here, the government applied for the Network Solutions warrant pursuant to Rule 41 and the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2703. That statute permits the government to obtain warrants requiring providers of remote computing services to disclose electronic communications if the warrants are

> issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction.

§ 2703(b)(1)(A). The statute defines a "court of competent jurisdiction" as including any district court of the United States, including a magistrate judge of such a court, with jurisdiction over the investigated offense. 18 U.S.C. § 2711(3)(A)(i).

Section 2703(b)(1)(A) thus authorizes a magistrate judge to issue a particular kind of warrant in cases over which his or her district court has jurisdiction. That grant of judicial authority is not modified by Rule 41(b) because 1) section 2703(b)(1)(A) refers to the procedures in Rule 41 and 2) the Rule 41(b) provisions are substantive, rather than procedural, in that they territorially restrict the judicial authority of magistrate judges to issue warrants. See § 2703(b)(1)(A); Fed. R. Crim. P. 41(b). Indeed, Rule 41(b) stands in contrast to other subsections of that rule which set forth specific procedures and methods for obtaining, issuing, executing and returning a search warrant. See Fed. R. Crim. P. 41(d)-(f).

The Court concludes that § 2703 affords Magistrate Judge Bowler authority to issue the Network Solutions warrant and that the Rule 41(b) provisions do not apply to this case. See United States v. Berkos, 543 F.3d 392, 397-98 (7th Cir. 2008)(internal quotation marks omitted)(finding that "Rule 41(b) deals with substantive judicial authority — not procedure — and thus does not apply to § 2703(a) . . . [which] authorize[es] district

courts to issue warrants only where it has jurisdiction over the offense").

Accordingly, the motion to suppress will be denied with respect to the issue of judicial authority.

2. Probable cause

Kanodia next asserts that the search warrant lacked probable cause because the supporting affidavit did not satisfy the nexus requirement.

He characterizes the affidavit as setting forth only a "bare suspicion" that the targeted e-mail account contained evidence of the alleged crimes and accuses the government of embarking on a "fishing expedition" to find incriminating evidence against him. He contends that a general declaration that "co-conspirators frequently use e-mail to communicate regarding matters relating to the conspiracy" and the baseless allegation that he e-mailed wire instructions to Ahmed after Ahmed sold his interests in Cooper Tire do not establish the requisite nexus. He claims that the e-mail with the wire instructions was not related to Ahmed's interests in Cooper Tire and there is no evidence that he used e-mail to communicate with Ahmed before or during the sales of those interests.

As a result, defendant denies that there was a substantial basis to conclude that all of the e-mail communications and data in the account, even those that fell outside the period of the

alleged conspiracy, contained evidence of the charged crimes. He concludes that the affidavit failed to establish probable cause and seeks to suppress all evidence obtained pursuant to the warrant.

The government responds that there was ample evidence and a substantial basis for Magistrate Judge Bowler to find probable cause to believe that the e-mail account contained evidence of the insider trading scheme. It maintains that the affidavit established the nexus element through its identification of the August, 2013 e-mail which Kanodia sent to Ahmed shortly after Ahmed sold his interests in Cooper Tire.

The government contends that the e-mail with the wire instructions "could not have been more on point" because it 1) showed that Kanodia directed Ahmed to share the profits of his illegal trades, 2) illustrated how Kanodia benefitted from the insider trading scheme and 3) shed light on the relationship between Kanodia and Ahmed. It challenges Kanodia's suggestion that "a single e-mail is not sufficient [for] the probable cause finding" as unsupported by the caselaw and inconsistent with its case agent's training and experience that co-conspirators often use e-mail in furtherance of the conspiracy.

In addition, the government submits that even if the search warrant were issued without probable cause, the "good faith" exception described in United States v. Ricciardelli, 998 F.2d 8

(1st Cir. 1993), would find suppression in this case unwarranted. The government proffers that its case agent reasonably relied on the warrant in good faith because the warrant was not "so facially deficient . . . or lacking in indicia of probable cause" as to render such reliance unreasonable. See id. at 15. Kanodia responds by denying that an agent could reasonably presume the validity of a search warrant that, in effect, asked for "copies of all mail ever sent by or delivered to a certain address".

The Court finds that, considering the totality of the circumstances, it was proper for Magistrate Judge Bowler to find probable cause to believe that the e-mail account contained evidence of the insider trading scheme. The supporting affidavit satisfied the nexus element by presenting sufficient evidence to believe that Kanodia used that account to send and receive e-mails in connection with the scheme. The Court declines to consider the application of the good faith exception because that finding is dispositive.

Accordingly, Kanodia's motion to suppress will be denied with respect to his arguments that the search warrant lacked probable cause.

3. Particularity

Kanodia next asserts that the categories in Attachment B of the search warrant did not describe the items to be seized with

sufficient particularity. He insists that the categories expanded the scope of the warrant "to an impermissible and unconstitutional scope" because they individually and collectively authorized a "limitless search warrant" for all of his e-mails regardless of relevance.

Specifically, Kanodia claims that the categories in Attachment B failed to include 1) a temporal limitation to prevent the government from examining "every communication from the date of the account opening to the date of the search," including communications from before or after the period of the alleged conspiracy, and 2) a substantive limitation to prevent the government from viewing materials relating to activities other than those expressly alleged in the affidavit.

He suggests that "the lack of a temporal limitation[,] coupled with all of the content and data files obtained", is dispositive evidence that the search warrant is a general warrant prohibited by the Fourth Amendment. The Court notes that he cites no controlling authority to support that contention and does not explain why the broad scope of an otherwise lawful search warrant necessarily renders the warrant invalid under the particularity requirement.

The government responds to Kanodia's assertions by clarifying that Attachment B sets forth

> fourteen specific categories of records and data to be searched and seized by law enforcement personnel, along with references to the specific crimes of wire fraud, securities fraud and conspiracy.

(internal quotation marks omitted). Those categories, according to the government, were directly related to the insider trading scheme, its participants and the use of the e-mail account in furtherance of the scheme. The government alleges that the categories supplied sufficient information to narrow the scope of the search and to guide and control the judgment of the executing agent in deciding where to search and what to seize, see Kuc, 737 F.3d at 133.

The government discredits Kanodia's arguments as misreading the categories in Attachment B and overlooking the reality that executing agents "must necessarily search through all records in order to identify those . . . within the scope of the warrant." It further proclaims that 1) there is no blanket requirement that all search warrants contain temporal limitations and 2) it was reasonable for this warrant to allow a search over a broader period of time because a) the relationships between the co-conspirators were "critical" to the crimes charged and b) the scheme itself occurred over an extended period of time.

The categories in the search warrant properly identified the items to be seized with particularity. The first 13 categories describe items relating to evidence, fruits or

instrumentalities of violations of 15 U.S.C. §§ 78(b) and 78ff, 18 U.S.C. §§ 371 and 1343 and Rule 10b-5. The listed items include communications between the co-conspirators; communications pertaining to Copper Tire, Apollo and various trading accounts; and information on the extent of the insider trading scheme and the individuals involved. The last category refers to the subscriber, transactional and logging records for the AK@LincolnVentures.com e-mail account and any associated e-mail accounts. The categories thus contained sufficient information to restrict the search to evidence of the alleged criminal activities and to guide the judgment of the executing agent during the search and seizure.

Accordingly, the motion to suppress will be denied with respect to the alleged lack of particularity.

4. Search protocol

Fed. R. Crim. P. 41(e)(2)(B) provides that, unless otherwise specified, a search warrant seeking electronically stored information "authorizes a later review of the [] information consistent with the warrant." Id. The Advisory Committee notes explain that:

> 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 . . . [E]lectronic storage media commonly contain such large amounts of information that it is often impractical for

> law enforcement to review all of the information during execution of the warrant at the search location.

Fed. R. Crim. P. 41 advisory committee's note (2009).

Kanodia takes issue with the lack of a specific protocol in the search warrant to minimize the government's exposure to information falling outside the scope of the warrant. He claims that minimization safeguards are particularly necessary when the search involves e-mail accounts which, unlike file cabinets or drawers, can "house[] a virtually limitless amount of data." He cites caselaw from other jurisdictions to suggest that Magistrate Judge Bowler should have imposed a "neutral and detached procedure" for law enforcement agents to use during their review of the e-mail content and account data, see United States v. Carey, 172 F.3d 1268, 1275 & n.7 (10th Cir. 1999) and United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998).

He faults Magistrate Judge Bowler for not requiring the government agents to follow procedures such as those suggested by another district court in the case of In the Matter of the Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1 (D.D.C. 2013). They include:

> 1) asking the custodian of the electronically stored information to provide limited information such as e-mails containing certain keywords or sent between particular recipients,

2) appointing a special master to hire an independent vendor to screen the information for relevance and privilege,

3) prohibiting its own computer personnel from disclosing to investigators any information falling outside the scope of the warrant,

4) waiving its reliance upon the plain view doctrine, and

5) using a search protocol designed to reveal only the information for which the government has probable cause to seize.

See id. at 11-12.

The government responds that its case agent properly carried out the two-step procedure outlined in the search warrant, which Magistrate Judge Bowler approved, when he served the search warrant on Network Solutions, received the e-mail communications and account data, and later searched those materials and seized items that fell within the scope of the warrant. The government points out that this two-step procedure is expressly authorized by Fed. R. Crim. P. 41(e)(2)(B) and was upheld by the First Circuit Court of Appeals ("the First Circuit") in United States v. Upham, 168 F.3d 532 (1st Cir. 1999).

Kanodia concedes that Rule 41(e)(2)(B) authorizes the "later review of the media or information consistent with the warrant" but maintains that the two-step procedure nevertheless violated the Fourth Amendment because it did not expressly

contain a minimization protocol. He submits that the Upham decision is outdated because it was decided over 15 years ago when technology was less advanced and e-mail accounts contained less information.

The Court finds defendant's arguments unavailing. In overseeing the warrant process, the Court is "primarily concerned with identifying what may be searched or seized – not how", see Upham, 168 F.3d at 537, and generally will not interfere with the discretion of law enforcement in determining "how best to proceed with the performance of a search authorized by warrant." United States v. Tsarnaev, 53 F. Supp. 3d 450, 464 (D. Mass. 2014)(citing Dalia v. United States, 441 U.S. 238, 257 (1979) and Upham).

The Upham decision remains the law in this Circuit and the Court declines to depart from its principles. In Upham, the First Circuit upheld the two-step procedure of initially seizing all materials contained in electronic storage media, including items that were not subject to the search warrant, and searching the seized materials later for items that fell within the scope of the warrant. Id. at 535. The Upham court held that the two-step procedure did not violate the Fourth Amendment because 1) the showing of probable cause in the warrant application indicated that there was "a sufficient chance of finding some needles in the computer haystack", 2) the search of the

electronic storage media was not inherently more intrusive than the physical search of an entire house and 3) the initial seizure of all materials and subsequent search for relevant materials was justified in light of the impracticality of law enforcement agents reviewing all of the information at the time of warrant execution. Id.

The reasoning in the Upham decision can be readily applied to this case which has similar facts. The Court thus finds that the two-step procedure used in this case did not violate the Fourth Amendment because 1) there was probable cause to believe that the e-mail account contained evidence, fruits or instrumentalities of the alleged crimes, 2) a search of an e-mail account is not inherently more intrusive than a physical search of a file cabinet or an entire house and 3) practical concerns justified the initial seizure of all electronically stored materials and the subsequent search for items that fell within the scope of the warrant.

Accordingly, the Court will deny Kanodia's motion to suppress in its entirety.

ORDER

For the foregoing reasons, defendant Kanodia's motion to suppress the evidence obtained pursuant to the Network Solutions search warrant (Docket No. 82) is **DENIED.**

So ordered.

/s/ Nathaniel M. Gorton
Nathaniel M. Gorton
United States District Judge

Dated June 6, 2016