UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------x

UNITED STATES OF AMERICA,

Plaintiff,

-against-

MICHAEL METTER,

Defendant.

----------x

MEMORANDUM AND ORDER
10-CR-600 (DLI)

DORA L. IRIZARRY, United States District Judge:

The instant action arises out of a multi-defendant indictment alleging that defendants participated in a fraudulent scheme to publicly report false and materially overstated sales figures to create artificial demand for, and increase the share price and trading volume of, the common stock of Spongetech Delivery Systems, Inc. ("Spongetech"). Metter is charged with conspiracy to commit securities fraud, in violation of 18 U.S.C. §§ 371, 3551 *et seq.* (Count 1), conspiracy to commit obstruction of justice, in violation of 18 U.S.C. §§ 371, 3551 *et seq.* (Count 2), securities fraud, in violation of 15 U.S.C. §§ 78j(b), 78ff, 18 U.S.C. §§ 2, 3551 *et seq.* (Count 3), obstruction of justice, in violation of 18 U.S.C. §§ 2, 1505, 3551 *et seq.* (Count 4), conspiracy to commit money laundering, in violation of 18 U.S.C. §§ 1956(h), 3551 *et seq*. (Count 5), and perjury, related to Metter's testimony before the Securities and Exchange Commission ("S.E.C."), in violation of 18 U.S.C. §§ 2, 1621(1), 3551 *et seq.* (Count 9).

Metter moves to (i) dismiss the counts against him for improper venue (*see* Metter Motion to Dismiss, Doc. Entry No. 128), and (ii) suppress the evidence obtained pursuant to search warrants executed at his home and Spongetech's office, as well as a search of his personal

email account (*see* Metter Motion to Suppress, Doc. Entry No. 129).[1] The government filed a consolidated opposition to both motions. (*See* Government Opposition, Doc. Entry No. 143.) The Court, likewise, has consolidated the two motions. As set forth more fully below, Metter's motion to dismiss for improper venue is denied, without prejudice to renew at trial, and Metter's motion to suppress evidence is granted.

DISCUSSION

I. Metter's Motion to Dismiss for Improper Venue

Metter moves to dismiss Counts 1-5, and 9 of the Superseding Indictment (Superseding Indictment ("S.I."), Doc. Entry No. 38), on the ground that the government has failed to establish that venue is proper in the Eastern District of New York. In Counts 1-5, the Superseding Indictment states that the conduct at issue occurred "within the Eastern District of New York and elsewhere." (S.I. ¶¶ 24-25, 27, 30, 32, 34.) Metter's pre-trial challenge to the appropriateness of venue as to Counts 1-5 is frivolous. "The law of this Circuit is clear that the Government's burden is satisfied with regard to pleading venue by alleging that criminal conduct occurred within the venue, even if phrased broadly and without a specific address or other information." *United States v. Bronson*, 2007 WL 2455138, *4 (E.D.N.Y. Aug. 23, 2007) (denying defendant's motion to dismiss for improper venue as the indictment states that "conduct occurred in the Eastern District of New York"); *see also United States v. Bellomo*, 263 F. Supp. 2d 561, 571 (E.D.N.Y. 2003) ("[T]he indictment, alleging on its face that the offenses occurred 'within the Eastern District of New York and elsewhere,' suffices to sustain it against this pretrial attack on venue."); *United States v. Szur*, 1998 WL 132942, *9 (S.D.N.Y. Mar. 20, 1998) ("[O]n its face,

[1] Certain co-defendants joined in these motions and subsequently withdrew their joinder because they either pled guilty or will plead guilty to certain charges in satisfaction of the indictment.

the Indictment alleges that the offense occurred 'in the Southern District of New York and elsewhere,' which is sufficient to resist a motion to dismiss.").

Should the government fail to establish venue by a preponderance of the evidence at trial, Metter is not precluded from renewing his motion at the conclusion of the government's case. *See Bronson*, 2007 WL 2455138, at *4 (explaining the difference between the government's burden at pleading and at trial, and permitting the defendant to renew his motion to dismiss for lack of venue at the conclusion of the government's case, if the government failed to establish venue by a preponderance of the evidence). Accordingly, Metter's motion to dismiss with respect to Counts 1-5 is denied without prejudice to renew at the conclusion of the government's case.

Metter also moves to dismiss Count 8, the perjury charge stemming from his testimony before the S.E.C. On October 5, 2009, the S.E.C. suspended trading of Spongetech shares. On October 13, 2009, the S.E.C. deposed Metter in the District of Columbia regarding Spongetech's recent activity in the financial markets. (S.I. ¶ 47.) In March 2010, the United States Attorney's Office for the Eastern District of New York opened its investigation into Spongetech, after preliminary investigations were initiated by the Internal Revenue Service ("I.R.S.") and the Federal Bureau of Investigation ("F.B.I.") in November 2009. (*See* Gov't Letter dated Feb. 10, 2012, Doc. Entry No. 207.) On May 3, 2010, the United States Attorney's Office for the Eastern District of New York filed a sealed complaint against Michael Metter and Steven Moskowitz. (*See* Complaint, Doc. Entry No. 1.) On May 5, 2010, the S.E.C. filed a complaint against Spongetech, Metter, Moskowitz, other individuals associated with Spongetech, and other entities controlled by the individual defendants. (*See S.E.C. v. Spongetech, et al.*, 10-CV-

2031(DLI)(JMA) Complaint, Doc. Entry No. 1.) Both the civil and criminal complaints alleged wrongdoing from 2007 to the date of filing.

The record makes it clear that Metter was deposed in the District of Columbia, at the behest of S.E.C. attorneys located in that District, prior to the commencement of the criminal and civil investigations undertaken by the government in this District. As set forth above, the government's burden to establish venue at the pleadings phase is less arduous. In *United States v. Clark*, 1987 WL 13273 (S.D.N.Y. Jun. 30, 1987), the court denied a motion to dismiss for improper venue under very similar circumstances. In that case, the defendant was deposed by the S.E.C. in the District of Columbia before the government filed charges in the Southern District of New York, yet, the Court concluded that venue was proper in the Southern District. *Id*. at *4. In denying the motion to dismiss, the Court applied the substantial contacts analysis set forth in *United States v. Reed*, 773 F. 2d 477, 481 (2d Cir. 1985) (explaining that a court conducting venue analysis should consider "the site of the defendant's acts, the elements and nature of the crime, the locus of the effect of the criminal conduct, and the suitability of each district for accurate fact finding"). As set forth below, the government has satisfied the *Reed* substantial contacts factors.

In the instant action, Metter testified to the trading of Spongetech stock, which occurred in this District and elsewhere. The effect of the crime was felt in this District as several victims have submitted letters detailing the financial losses that they incurred in this District as a result of purchasing Spongetech stock. Further, the S.E.C. and the government filed charges in this District, at least in part, as a result of the S.E.C.'s depositions of defendant Metter and other co-defendants. Metter's allegedly perjured testimony would have impeded the government's and the S.E.C.'s investigations in this District. These considerations lead the Court to conclude that,

at this stage in the litigation, venue is proper in this District. Accordingly, Metter's motion to dismiss with respect to Count 8 is denied without prejudice to renew at the conclusion of the government's case.

II. Metter's Motion to Suppress

As set forth above, the government filed a sealed criminal complaint against Metter on May 3, 2010. The S.E.C. filed a civil complaint against Metter on May 5, 2010. The government then sought and executed several court authorized search warrants, which are the subject of defendant's motion to suppress certain digital evidence.

A. Background

On May 4, 2010, Special Agent Thomas McGuire of the F.B.I. submitted an affidavit in support of an application for a warrant to search Metter's home, located at 1 Tinker Lane, Greenwich, Connecticut 06830. (*See* McGuire Affidavit for Application to Search Metter's Home ("McGuire Home Aff."), attached as Ex. 3 to the Affidavit of Maranda Fritz ("Fritz Aff."), Doc. Entry No. 132.) The Affidavit set forth detailed information regarding the investigation and incorporated the Complaint by reference. (*Id.*) The Affidavit indicated that Metter used computers from his home to further the fraudulent scheme and that agents had recovered numerous computer-generated documents related to the scheme from the Metters' household trash.[2] (*Id.* ¶¶ 48-51.) The Affidavit requested permission to "search, copy, image and seize the computer hardware" and to "conduct an off-site search of the image or hardware." (*Id.* at ¶ 58.) The Affidavit included a detailed attachment, Attachment A, specifying the categories of documents to be located.

[2] The evidence obtained from the Metters' household trash is not affected by this Decision and Order as it is well-established that an individual has no expectation of privacy in his trash. *See, e.g.*, *United States v. Caputo*, 808 F. 2d 963, 967 (2d Cir.1987) (explaining that there is no privacy interest in a trash can on public street).

The Honorable Warren Eginton, United States District Judge for the District of Connecticut, granted the application for the search warrant on May 4, 2010. (*See* Metter Home Search Warrant, attached as Ex. 4 to the Fritz Aff.) The government searched Metter's home and seized four computer hard drives, paper documents, and approximately $27,000 in cash.

On May 4, 2010, Special Agent John Carrano of the I.R.S. submitted an affidavit in support of an application for a warrant to search the offices of Spongetech and RM Enterprises International Ltd. ("RM Enterprises"), both of which were located in New York, New York. (*See* Carrano Affidavit for Office Search ("Carrano Aff."), attached as Ex. 5 to the Fritz Aff.) The Affidavit set forth detailed information regarding the investigation and incorporated the Complaint by reference. (*Id*. ¶¶ 1, 5-48.) The Affidavit detailed the manner in which computers located in those offices were used to perpetrate the fraudulent scheme. (*Id*. ¶¶ 51, 53.) The Affidavit requested permission to "search, copy, image and seize the computer hardware" and to perform an off-site search for "evidence, fruits, and instrumentalities" of violations of specified criminal statutes. (*Id*. ¶ 60.) The Affidavit included a detailed attachment, Attachment A, specifying the categories of documents to be located.

The Honorable Kevin Nathaniel Fox, United States Magistrate Judge for the Southern District of New York, granted the application for the search warrant on May 4, 2010. (*See* Office Search Warrant, attached as Ex. 6 to the Fritz Aff.) The government searched Spongetech's Office and seized 61 computer hard drives and 67 boxes of paper documents.

On November 1, 2010, Special Agent McGuire submitted an affidavit in support of an application for a warrant to search the personal email accounts of defendant Metter and several of his co-defendants. (*See* McGuire Affidavit for Application to Search Email ("McGuire Email Aff."), attached as Ex. 8 to the Fritz Aff.) The Affidavit described the investigation and the

Spongetech scheme and set forth the manner in which the personal email accounts were used to further the scheme. (*Id*. ¶¶ 118-128.) The Affidavit requested permission to seize from the respective Internet Service Providers ("ISPs") "all images and all text messages" stored, explaining that:

> First, because voluminous amounts of information can be stored in a computer account, and because it might be stored in a deceptive fashion or with deceptive file names to conceal criminal activity, the searching authorities must carefully open and examine all the stored data to determine which of the various files are evidence, fruits, or instrumentalities of the crime . . . . Second, this sorting process must be done in a controlled environment, due to the extensive array of computer hardware or software that might be necessary . . . .

(*Id*. ¶ 130.) The Affidavit included a detailed attachment, Attachment A-1, specifying the categories of electronic correspondence to be located.

On November 1, 2010, the Honorable Andrew L. Carter, then United States Magistrate Judge for the Eastern District of New York, authorized the search warrant. (*See* Email Search Warrant, attached as Ex. 9 to the Fritz Aff.) The government obtained email account files from the ISPs for the personal email accounts sought in the Email Search Warrant. The government's retrieval of this evidence did not prevent the email account users from accessing or using their email accounts as the government essentially requested a snapshot of account activity for a particular period of time.

With respect to the seized computer hard drives, the government created images[3] of the hard drives, and promptly returned the computer hardware to its appropriate owner. The government promptly provided defendants with copies of the seized physical documents as well.

[3] An "image" of a hard drive is a copy of a computer's hard drive that "duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original." *United States v. Vilar*, 2007 WL 1075041, *35 n.22 (S.D.N.Y. Apr. 4, 2007).

It is the government's subsequent inactivity with respect to the imaged hard drives and email correspondence that is the subject of Metter's instant motion.

This case originally was assigned to a different district judge of this Court. The parties first appeared before this Court at a status conference held on November 22, 2010. (*See* Transcript of Nov. 22, 2010 Status Conference ("11/22/10 S/C Tr."), attached as Ex. 10 to the Fritz Aff.) At that conference, the government initially stated that it had seized roughly 50 hard drives and intended to provide the defendants with imaged copies by January 2011. (*Id*. at 5.) When questioned by the Court about the procedures in place for conducting a privilege review of the electronic evidence, the government indicated that it had not begun the privilege review and was unable to give an estimated completion date for its review. (*Id*. at 5-8.) The Court directed the parties to confer regarding discovery and to update the court as to the progress achieved. (*Id*. at 12-13.) The government provided the Court with a summary of the discovery process on January 25, 2011, to which none of the defendants filed objections.

On February 4, 2011, the parties appeared before the Court for another status conference. (*See* Transcript of Feb. 4, 2011 Status Conference ("2/4/11 S/C Tr."), attached as Ex. 11 to the Fritz Aff.) At that conference, the government represented that it would produce to defendants a list of the computers and emails seized pursuant to the search warrants by March 2011. (*Id*. at 7.) With respect to the imaged, seized hard drives and email accounts, the government indicated that it intended to set up a "taint team" to review that imaged evidence for any privilege issues. (*Id*. at 19.) The defendants agreed to provide the government with a list of attorneys for the government's privilege review within one week of the status conference. (*Id*. at 20.) The Court exhorted the parties to work together to resolve these issues. (*Id*. at 20-21.)

Upon further questioning by the Court, the government indicated that it intended to produce all of the imaged evidence (without reviewing it first) to all defendants and then, at a later time, conduct a privilege review of the imaged evidence. (*Id*. at 24-26.)

Metter's attorney expressed concern for this approach:

> It is very troubling to me that the Government would take the position that they can come in and seize a computer with probably years' worth of confidential completely irrelevant material on it and then disseminate it out to a group of other individuals. This is completely apart from attorney-client privilege. This is really a matter of irrelevant personal confidential data. Heaven only knows what's on there. Financial data, personal information, relationship information. That cannot - - that can't be permissible.

(*Id*. at 27.) Metter's counsel then suggested that each attorney review the computer of his or her client to weed out imaged evidence that fell outside the scope of the search warrant to avoid "willy-nilly distributing" of personal and unrelated imaged evidence to every party in the case. (*Id*. at 29.) The government objected, arguing that its discovery productions should not be limited to any particular defendant's determination that a document is outside the scope of the search warrant. (*Id*. at 29-30.) The Court explained that a defendant's objection would not be taken as fact, but that the government has a duty to make its own determination as to whether or not a particular imaged document fell within the scope of the warrant. (*Id*. at 30-31.) The Court ordered the government to produce an inventory of the computers seized and for defense counsel to review his or her client's computers for what he or she believed to be irrelevant and privileged evidence. (*Id*. at 32-33, 36.)

On February 28, 2011, the government filed a discovery status report with the Court. In its letter, the government stated that it would permit the defendants to inspect the various hard drives at the government's office and to lodge objections to any imaged evidence that the defendant believed fell outside the scope of the search warrant. (*See* 2/28/11 Gov't Letter, Doc.

Entry No. 101, at 2.) Yet, the government further stated that: "Any attorney can request in writing a copy of any other computers seized, and arrangements can then be made for that attorney to provide the government with appropriately-sized hard drives for the purpose of copying the requested computers." (*Id.*) Metter immediately filed a letter indicating his continued objections to the "notion that the government can seize dozens of entire hard drives, fail to conduct any review of the extent to which the material far exceeds the scope of a warrant, but then disseminate that material to others." (*See* 02/28/11 Metter Letter, Doc. Entry No. 102.)

As of the time the instant motion was fully briefed, approximately fifteen months after the government executed its search warrants, the government had not conducted its review of the evidence seized and imaged to determine whether any of that imaged evidence fell outside the scope of the search warrant. Additionally, as of the date of this Memorandum and Order, it remains uncertain when the government would complete its privilege review of the imaged evidence.

B. Analysis

Metter contends that the government's significant delay in conducting off-site searches of the imaged evidence merits blanket suppression of all seized and imaged evidence as routine delays of this duration would eviscerate the Fourth Amendment's privacy protections. The government counters that the wholesale seizure of hard drives and email accounts and off-site review of such electronic data is necessary given the nature of such evidence and has widely been deemed permissible under the Fourth Amendment. The government further contends that the search warrants were properly executed in this case. The government argues that its prompt return of the original electronic evidence (*i.e.*, the physical hard drives) negates any harm arising out of its delayed review of the imaged evidence as to whether or not that evidence fell within

the scope of the warrant. With respect to the passage of time between the seizure and off-site relevance review, the government contends that it reviewed the imaged evidence within a "reasonable" period of time, as required by the Fourth Amendment.

This case raises an interesting issue of first impression in this Circuit that may impact electronic discovery in future criminal investigations and cases: How long may the government retain seized and imaged electronic evidence before conducting a review of that evidence to determine whether any of it falls outside the scope of a search warrant? The answer to this question requires a careful case-by-case factual analysis because what may be appropriate under one set of facts and circumstances may not be so under another. For the reasons discussed below, the Court finds that the government's more than fifteen-month delay in reviewing the seized electronic evidence, under the facts and circumstances of this case, constitutes an unreasonable seizure under the Fourth Amendment.

An image of an electronic document contains all of the same information as the original electronic document. To the extent the owner or custodian of the electronic document has privacy concerns regarding the government's retention of the original document, the owner would have identical privacy concerns with the government's retention of the imaged document. For example, the seizure of a personal email account could, in addition to evidence responsive to a search warrant, yield personal communications between a cheating spouse and his or her paramour or communications between an individual and his or her family regarding an embarrassing medical condition. These hypothetical communications clearly fall outside the scope of the search warrants in this case (and arguably those in most criminal cases). Thus, the government's long-term retention of images of these communications presents the same privacy concerns as would the government's retention of the original communications.

Under the Fourth Amendment's Warrant Clause, "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 clause was intended as a bulwark against the 'general warrant' abhorred by the colonists and protects against a general, exploratory rummaging in a person's belongings." *United States v. Cioffi*, 668 F. Supp. 2d 385, 390 (E.D.N.Y. 2009) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). "Its overarching purpose is to ensure that 'those searches deemed necessary should be as limited as possible.'" *Cioffi*, 668 F. Supp. 2d at 390 (quoting *Coolidge*, 403 U.S. at 467). "To achieve its goal, the Warrants Clause requires particularity and forbids overbreadth." *Cioffi*, 668 F. Supp. 2d at 390. In addition to these threshold Fourth Amendment requirements, the manner in which the government executes the warrant must comport with the Fourth Amendment's reasonableness standard.[4] *See United States v. Graziano*, 558 F. Supp. 2d 304, 316 (E.D.N.Y. 2008); *see also United States v. Hill*, 459 F. 3d 966, 978 (9th Cir. 2006) ("The reasonableness of the officer's acts both in executing the warrant and in performing a subsequent search of seized materials remains subject to judicial review.").

Searches for documents (whether in electronic or paper form) pose unique Fourth Amendment concerns. Courts have recognized that "searching a computer for evidence of a crime can be as much an art as a science." *United States v. Vilar*, 2007 WL 1075041, *38 (S.D.N.Y. Apr. 4, 2007). Unlike warrants seeking readily identifiable evidence such as narcotics or firearms, an onsite search of a computer for the evidence sought by a warrant is not practical

[4] Metter does not challenge the Metter Home Search Warrant or the Office Search Warrant for particularity or overbreadth. His challenge with respect to the evidence seized and imaged by these warrants is the government's mishandling of the off-site review of the evidence. Metter challenges the Email Search Warrant on the same ground, in addition to overbreadth. Because the Court has granted Metter's motion to suppress on the ground of the manner the government executed the warrants, the Court need not address the overbreadth challenge to the Email Search Warrant.

or even possible in some instances. *See Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001) (discussing cases that permitted taking computers off site for forensic searches and explaining that "[b]ecause of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files"). Computers store millions of documents, and as some courts have recognized, the onsite search (and accompanying occupation to conduct such a search), might be more off putting to an individual than the seizure of a computer for an off-site determination as to whether it stores any information that falls within the scope of the warrant. *See, e.g.*, *United States v. Mutschelknaus*, 564 F. Supp. 2d 1072, 1076 (D. N.D. 2008) ("It is established that courts have recognized that a search of computer data involves more preparation than an ordinary search and a greater degree of care in the execution of the warrant; and that the search may involve much more information.").

As technology and white collar and other complex criminal litigation evolved, courts began distinguishing between the execution of search warrants seeking physical evidence such as guns or narcotics, and the execution of search warrants seeking documents (whether in electronic or paper form). As the Supreme Court explained more than thirty-five years ago, "[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." *Andresen v. Maryland* 427 U.S. 463, 482 n.11 (1976); *see also United States v. Riley*, 906 F. 2d 841, 845 (2d Cir. 1990) ("It is true that a warrant authorizing seizure of records of criminal activity permits officers to examine many papers in a suspect's possession to determine if they are within the described category. But allowing some latitude in this regard simply recognizes the reality that few people keep documents of their criminal transactions in a folder marked 'drug

records.'"); *United States v. Christine*, 687 F. 2d 749, 760 (3d Cir. 1982) ("[N]o tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision."). Thus, courts began permitting the government to examine paper documents that might otherwise fall outside the scope of a search warrant to make that determination, recognizing that different types of evidence present different tactical issues.

Computers and electronic information present a more complex situation, given the extraordinary number of documents a computer can contain and store and the owner's ability to password protect and/or encrypt files, documents, and electronic communications. As a result, the principle of permitting law enforcement some flexibility or latitude in reviewing paper documents just described, has been extended to computerized or electronic evidence. Courts have applied the principles recognized in *Andresen* "in analyzing the method used by the police in searching computers and have afforded them leeway in searching computers for incriminating evidence within the scope of materials specified in the warrant." *Graziano*, 558 F. Supp. 2d at 317; *see also United States v. Scarfo*, 180 F. Supp. 2d 572, 578 (D.N.J. 2001) ("Where proof of wrongdoing depends upon documents or computer passphrases whose precise nature cannot be known in advance, law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence which is properly specified in the warrant."). Thus, courts developed a more flexible approach to the execution of search warrants for electronic evidence, holding the government to a standard of reasonableness. *See Graziano*, 558 F. Supp. 2d at 316 ("[T]he manner of the execution of the warrant" in computer searches is "subject to judicial review under a 'reasonableness' standard.").

The warrants drafted in this case comport with modern standards of reasonableness. The warrants requested permission to seize computer hard drives and email accounts and to image

them offsite. (*See* McGuire Home Aff. ¶ 58; Carrano Aff. ¶ 60; McGuire Email Aff. ¶ 130.) The Court does not expect the government to make onsite determinations of whether a file or document contained on a hard drive or in an email account falls within the scope of the warrant and, thus, off-site imagining is a necessity of the digital era. *See, e.g.*, *United States v. Burns*, 2008 WL 4542990, *5 (N.D. Ill. Apr. 29, 2008) ("Courts have found that seizure of computer equipment before search is reasonable given the complexities of electronic searches, as long as the requirements of the Fourth Amendment are met."). Here, the warrants stated that the government would conduct an offsite review of the imaged evidence to determine whether the evidence seized and imaged fell within the scope of the warrants (*see* McGuire Home Aff. ¶ 58; Carrano Aff. ¶ 60; McGuire Email Aff. ¶ 130). Additionally, the warrants included detailed descriptions of the type of documents and information indicative of the criminal activity at issue in this case (*see* Attachment A to Metter Home Search Warrant; Attachment A to Office Search Warrant; Attachment A-1 to McGuire Email Aff.). Warrants requesting off-site review of seized electronic data are routinely upheld as reasonable. *See, e.g.*, *Graziano*, F. Supp. 2d at 316-19 (concluding that the seizure of a home computer and the off-site search of that computer for evidence of criminal activity specified in the search warrant was reasonable).

The government seized 61 computer hard drives from Spongetech, four computer hard drives from Metter's home, and a snapshot of all of the activity that had occurred in Metter's personal email account.[5] The government then promptly imaged the hard drives and returned them to their respective owners.[6] Up to this point, there is nothing problematic with the manner

[5] As discussed earlier, the government seized hard drives from other defendants, in addition to those seized from Metter at his home and Spongetech office. The evidence seized from the other defendants is not the subject of this Decision and Order, as those defendants have pleaded guilty or are in the process of pleading guilty. Accordingly, nothing in this Decision and Order should be construed as limiting the government from relying upon evidence seized from the other defendants.

[6] The government's seizure of a snapshot of Metter's personal email account had no effect on his continued access to or use of that account.

in which the government executed the warrants. The point at which the government faltered is its delay in reviewing the imaged evidence to determine whether the evidence that the government seized and imaged fell within the scope of the categories of information sought in the search warrants.

The Court recognizes that under current law there is no established upper limit as to when the government must review seized electronic data to determine whether the evidence seized falls within the scope of a warrant. *See, e.g.*, *Mutschelknaus*, 564 F. Supp. 2d at 1076 ("Neither Fed. R. Crim. P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant."). However, the Fourth Amendment requires the government to complete its review, *i.e.*, execute the warrant, within a "reasonable" period of time. Numerous cases hold that a delay of several months between the seizure of electronic evidence and the *completion* of the government's review of that evidence as to whether it falls within the scope of the warrant is reasonable. *See id.* at 1076-77 (finding a two-month delay reasonable); *see also Burns*, 2008 WL 4542990, at *8-9 (finding a ten-month delay for *completion* of the government's review reasonable).

The parties have not provided the Court with any authority, nor has the Court found any, indicating that the government may seize and image electronic data and then retain that data with no plans whatsoever to *begin* review of that data to determine whether any irrelevant, personal information was improperly seized. The government's blatant disregard for its responsibility in this case is unacceptable and unreasonable. *See United States v. Debbi*, 244 F. Supp. 2d 235, 237-38 (S.D.N.Y. 2003) (finding a Fourth Amendment violation in the search, seizure, and retention of seven boxes of documents from the defendant's home, which included "personal and

religious files, general correspondence, [and] family financial records," when "no meaningful attempt" was made to separate and retain only the items the warrant permitted to be seized). The government contends that *Debbi* is inapposite because, in that case, the government retained original paper documents, whereas, in this case, the government returned the original electronic documents and equipment and retained only the imaged electronic documents. The Court disagrees. It is a distinction without a difference. The government's retention of *all* imaged electronic documents, including personal emails, without *any* review whatsoever to determine not only their relevance to this case, but also to determine whether any recognized legal privileges attached to them, is unreasonable and disturbing. Moreover, the government repeatedly asserted its intent to release indiscriminately the imaged evidence to *every* defendant, prior to conducting any review to determine if it contained evidence outside the scope of the warrants. (*See* 2/4/11 S/C Tr. 24-26, 29-30; 2/28/11 Gov't Letter at 2.) The Court agrees with Defendant that the release to the co-defendants of any and all seized electronic data without a predetermination of its privilege, nature or relevance to the charged criminal conduct only compounds the assault on his privacy concerns. It underscores the government's utter disregard for and relinquishment of its duty to insure that its warrants are executed properly.

This conclusion leaves the Court with a final determination to make: What is the appropriate remedy in this case? It is well-settled that "[g]overnment agents 'flagrantly disregard' the terms of a warrant so that wholesale suppression is required only when (1) they effect a 'widespread seizure of items that were not within the scope of the warrant,' . . . and (2) do not act in good faith." *United States v. Liu*, 239 F. 3d 138, 140 (2d Cir. 2000) (quoting *United States v. Matias*, 836 F. 2d 744, 748 (2d Cir. 1988)). "The rationale for blanket suppression is that a search that greatly exceeds the bounds of a warrant and is not conducted in good faith is

essentially indistinguishable from a general search." *Liu*, 239 F. 3d at 141. "[T]o satisfy the first prong of the two-part test described above, the search conducted by government agents must actually resemble a general search." *Id*. Thus, "the extreme remedy of blanket suppression should only be imposed in the most extraordinary of cases." *United States v. Foster*, 100 F. 3d 846, 852 (10th Cir. 1996) (internal quotation marks omitted.)

The first prong is satisfied here as the "snapshot" the government sought permission to take resembles a general search. The warrants specifically sought, and the government was granted, permission for the widespread seizure of *all* information contained in the personal email accounts and computers at issue with imaging and review to occur off-site. (*See* McGuire Home Aff. ¶ 58; Carrano Aff. ¶ 60; McGuire Email Aff. ¶ 130.) The government subsequently "imaged" all of the seized items. There can be no doubt under these circumstances that this is a "general search" as described above.

The lack of good faith by the government can be inferred from its conduct in this case. In the affidavits in support of the search warrants issued in this case, the government promised to review the evidence seized offsite to determine whether any evidence fell outside the scope of the warrants. (*See* McGuire Home Aff. ¶ 58; Carrano Aff. ¶ 60; McGuire Email Aff. ¶ 130.) The government then failed to commence the review, despite repeated requests from defense counsel and directions from the Court to do so. In fact, the government seemed shocked that the Court would require such a review, and, as mentioned above, threatened to provide *all* of the evidence seized and imaged to *each* defendant in the case, without conducting any such review. (*See* 2/4/11 S/C Tr. 24-26, 29-30; 2/28/11 Gov't Letter at 2.) The government's own conduct and statements indicate that it had no intention of fulfilling its obligations as promised in the

search warrants. Nor has the government presented any evidence or arguments to the effect that it failed to fulfill this obligation due to limited resources, such as it has argued in other cases.

The Court has not reached this conclusion lightly. However, the Court cannot, in the interest of justice and fairness, permit the government to ignore its obligations. Otherwise, the Fourth Amendment would lose all force and meaning in the digital era and citizens will have no recourse as to the unlawful seizure of information that falls outside the scope of a search warrant and its subsequent dissemination. Accordingly, Metter's motion to suppress is granted. This conclusion is limited to the electronic evidence seized and imaged pursuant to the Metter Home Search Warrant, Office Search Warrant, and Email Search Warrant and does not include the paper documents and currency seized pursuant to those warrants.

CONCLUSION

Metter's motion to dismiss on the basis of improper venue is denied without prejudice to renew at the conclusion of the government's case at trial. Metter's motion to suppress the electronic evidence seized and imaged pursuant to the Metter Home Search Warrant, Office Search Warrant, and Email Search Warrant is granted.

SO ORDERED.

Dated: Brooklyn, New York
May 17, 2011

/s/
DORA L. IRIZARRY
United States District Judge