UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

---

x

UNITED STATES OF AMERICA,

-against-

RALPH CIOFFI and MATTHEW TANNIN,

Defendants.

---

x

MEMORANDUM AND ORDER
Case No. 08-CR-415 (FB)

Appearances:
For the United States of America:
BENTON J. CAMPBELL, ESQ.
United States Attorney
Eastern District of New York
By: JAMES G. MCGOVERN, ESQ.
ILENE JAROSLAW, ESQ.
PATRICK SEAN SINCLAIR, ESQ.
BRIAN SANO, ESQ.
Assistant United States Attorneys
271 Cadman Plaza East
Brooklyn, NY 11201

For Defendant Ralph Cioffi:
DANE BUTSWINKAS, ESQ.
MARGARET A. KEELEY, ESQ.
Williams & Connolly LLP
725 Twelfth Street, N.W.
Washington, DC 20005

For Defendant Matthew Tannin:
SUSAN E. BRUNE, ESQ.
NINA M. BEATTIE, ESQ.
MARYANN J. SUNG, ESQ.
THERESA TRZASKOMA, ESQ.
Brune & Richard LLP
80 Broad Street
New York, NY 10004

BLOCK, Senior District Judge:

Defendant Matthew Tannin ("Tannin") is charged with conspiracy, securities fraud and wire fraud in connection with two hedge funds he managed for Bear Stearns Asset Management ("BSAM"). He moves to suppress evidence seized from his personal email account on the ground that the warrant authorizing the seizure did not comply with the Warrants Clause of the Fourth Amendment.[1] For the following reasons, the motion is granted.

---

[1]Defendant Ralph Cioffi ("Cioffi") is charged with the same crimes as Tannin, in addition to insider trading; he is not a party to the motion.

I

On July 7, 2009, FBI Special Agent Mark Munster ("Munster") applied to Magistrate Judge Cheryl Pollak for a warrant to search Tannin's personal email account. *See* Letter from P. Sinclair (Oct. 12, 2009), Ex. ("Search Warrant"). An affidavit executed by Munster accompanied the application. *See id.*, Ex. ("Affidavit in Support of a Search Warrant").

A. The Affidavit

The Affidavit began with a boilerplate description of the Internet, email and Google (the company who hosted the targeted account). It then set forth Munster's proffered bases for issuing the Warrant.

First, the Affidavit expressly incorporated by reference the 27-page indictment to demonstrate probable cause that Tannin had committed the charged crimes. To connect those crimes to Tannin's personal email account, the Affidavit alluded to paragraph 41 of the indictment, which excerpted an email sent by Tannin from his personal account to Cioffi on April 22, 2007 ("the April 22nd Email"):

> [T]he subprime market looks pretty damn ugly. . . . If we believe the [CDO report is] ANYWHERE close to accurate I think we should close the funds now. The reason for this is that if [the CDO report] is correct then the entire subprime market is toast. . . . If AAA bonds are systemically downgraded then there is simply no way for us to make money – ever.

Indictment ¶ 41 (alterations in original).[2]

As recounted in the Affidavit, the April 22nd Email was produced to BSAM's counsel in the course of an investigation into the funds' collapse. BSAM turned the email over to the Securities Exchange Commission ("SEC") and the United States Attorney's Office in November

[2]The government has introduced the April 22nd Email as evidence of Tannin's knowledge and intent.

2007. Munster opined that Tannin's use of his personal email account, instead of his Bear Stearns account, to discuss work-related matters made it "likely that Matthew Tannin purposely used THE SUBJECT E-MAIL ACCOUNT to facilitate the charged conspiracy" because the conspirators "were able to communicate privately by using THE SUBJECT E-MAIL ACCOUNT, in that their communications would not be subject to capture and review by Bear Stearns." Affidavit ¶ 15.

The Affidavit then quoted at length from the Stored Communications Act, 18 U.S.C. §§ 2701-12. As pertinent here, the Act allows government agents to obtain from companies such as Google the contents of their subscribers' accounts pursuant to a warrant issued by the "court with jurisdiction over the offense under investigation." *Id.* § 2703(b)(A).

In the Affidavit's next section, Munster described the procedures necessary to adequately execute the search. First, he averred that the search would be limited to emails created on or before August 12, 2007, "the day prior to Tannin's retention of private counsel, to prevent the danger of intercepting privileged communications." Affidavit ¶ 22. He then stated that the nature of electronically stored data required "the searching authorities [to] carefully open and examine all the stored data to determine which of the various files are evidence, fruits, or instrumentalities of the crime," and that such a procedure "would be impractical to do at Google's offices" and would instead need to be carried out off-site "in a controlled environment." *Id.* ¶ 23. Finally, he averred that "[f]ederal law enforcement officials will review the records sought by the search warrant and will segregate any messages and content constituting evidence of violations of federal criminal law." *Id.* ¶ 24.

The final paragraph of the Affidavit recited Munster's belief, based on the facts set forth, that "there is probable cause to search THE SUBJECT E-MAIL ACCOUNT for evidence of activities relating to conspiracy to commit securities fraud and wire fraud, in violation of 18 U.S.C.

§ 371; securities fraud, in violation of 15 U.S.C. §§ 78j(b) and 78ff; and wire fraud, in violation of 18 U.S.C. § 1343." *Id.* ¶ 25.

B. The Warrant

Magistrate Judge Pollak signed the Warrant, which authorized a search of "the premises known and described as electronic mail address 'matt.tannin@gmail.com'." The Warrant contained a boilerplate statement reflecting the magistrate judge's "satisf[action] that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property . . . described is now concealed on the . . . premises above-described and establish grounds for the issuance of this warrant."[3] The government concedes, however, that the Affidavit was not attached to or incorporated by reference into the Warrant.

The Warrant authorized Munster (or "any Authorized Officer of the United States") to seize from the Tannin's email account the items set forth in "Attachment A" to the Warrant. The attachment listed seven categories of "records and other stored information" relating to Tannin's account; the category pertinent here was described as "all e-mail up through August 12, 2007, including any attachments, and all instant messages, sent by or received by the accounts [sic], whether saved or deleted, whether contained directly in the e-mail account or in a customized 'folder.'"[4] There was no provision limiting the emails to be seized to those containing evidence of the crimes charged in the indictment or, indeed, of any crime at all.

Attachment A also set forth procedures for obtaining the account from Google. It directed Google employees to "locate, isolate, and create an exact duplicate" of all records sought,

---

[3]The Warrant erroneously states that it is based on the affidavit of a "Special Agent Elizbeth [sic] Brance."

[4]Broadly speaking, the other categories involved a wide range of information about the account, such as billing records, activity logs and user preferences.

and to produce the duplicate to the executing officer "in electronic form." The attachment did not, however, describe any procedures for the executing officer to follow in searching the account and seizing particular records.

C. Execution of the Warrant

The Warrant was served on Google. On July 17, 2009, Google wrote to the government that it was "no longer able to extract the information requested in the Search Warrant" because Tannin's account had been "deleted." Letter from K. Untiedt to I. Jaroslaw (July 17, 2009). On the eve of trial, however, Google advised the government that it had located a copy of the account as it existed on November 7, 2007. Google promptly sent the government a CD-ROM containing that version of the account.

Members of the prosecution team searched the account. *See* Letter from I. Jaroslaw (Oct. 8, 2009) ("Today the government received via Federal Express from Google the contents of defendant Matthew Tannin's G-Mail account as it existed on November 7, 2007 on a CD-ROM. We have not had an opportunity to review the account in its entirety."). During an "initial look" at the account, the government isolated a November 23, 2006 email from Tannin to himself ("the November 23rd Email"). The lengthy email is essentially a diary entry, in which Tannin recorded his thoughts about such sundry matters as recent vacations and medical issues; however, several paragraphs were devoted to Tannin's anxiety about work and the state of the market.[5]

D. The Motion to Suppress

On October 8, 2009, the government informed me and defense counsel that it intended to offer the November 23rd Email into evidence as bearing on Tannin's "knowledge and

[5]Since I conclude that the search that yielded the November 23rd Email violated the Fourth Amendment, it would be inappropriate to repeat the contents of the email.

intent on all the pending charges against him." Letter from I. Jaroslaw (Oct. 8, 2009). Tannin moved to suppress the email (which has been marked for identification as Government Exhibit 100); he argued that the Warrant was "invalid on its face because it failed to describe with particularity the materials that would be the proper subject of a search" and that "[s]uch a warrant is unreasonably broad and therefore unconstitutional." Tannin's Mem. of Law at 2.[6] The government has filed a series of letter memoranda in response.

Taken collectively, the parties' submissions frame the following three issues for my determination:

1. Did the Warrant violate the Warrants Clause of the Fourth Amendment?

2. If so, is the November 23rd Email nevertheless admissible under the "good-faith exception" of *United States v. Leon*, 468 U.S. 897 (1984)?

3. If not, is the November 23rd Email nevertheless admissible under the "inevitable discovery" doctrine?

I address these issues in turn.[7]

---

[6]Tannin also moved to exclude the November 23rd Email under Federal Rule of Evidence 403. As I explained in open court, I agree with the government that the email is relevant because it tends to show Tannin's knowledge of potential problems with the funds and its investments; although the email predates the dates of the crimes charged in the indictment (March-June 2007) by several months, it is not implausible that a jury could reasonably conclude that Tannin's knowledge of problems in November 2006 spurred him to enter into a conspiracy to cover up those problems in March 2007.

[7]One preliminary matter is *not* in question: The government does not dispute that Tannin has a reasonable expectation of privacy in the contents of his personal email account. *See United States v. Zavala*, 541 F.3d 562, 577 (5th Cir. 2008) ("[C]ell phones contain a wealth of private information, including emails, text messages, call histories, address books, and subscriber numbers. [The defendant] had a reasonable expectation of privacy regarding this information."); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) ("E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment

II

A. The Warrants Clause

The Fourth Amendment's Warrants Clause provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." 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." *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." *Id.*

To achieve its goal, the Warrants Clause requires particularity and forbids overbreadth. "Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited to the probable cause on which the warrant is based." *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006). Thus, as I recently explained in *United States v. Cohan*, 628 F. Supp. 2d 355 (E.D.N.Y. 2009), a warrant can violate the clause "either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries." *Id.* at 359.

A warrant is sufficiently particular if it "enable[s] the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized him to seize." *United States v. George*, 975 F.2d 72, 75 (2d Cir. 1992). "Courts tend to tolerate a greater degree of ambiguity where 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

---

protection, but the address and size of the package do not.").

could be expected to cover, and have insured that all those facts were included in the warrant." *United States v. Buck*, 813 F.2d 588, 590 (2d Cir. 1987) (quoting *United States v. Young*, 745 F.2d 733, 759 (2d Cir. 1984)); *see also United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986) ("Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible."). Nevertheless, "[a] failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary." *George*, 975 F.2d at 76.

The level of specificity required by the Warrants Clause depends on many factors. The nature of the crime, for example, may require a broad search. *See, e.g., Andresen v. Maryland*, 427 U.S. 463, 481 n.10 (1976) ("Like a jigsaw puzzle, the whole 'picture' of petitioner's false-pretense scheme . . . could be shown only by placing in the proper place the many pieces of evidence that, taken singly, would show comparatively little."); *United States v. Regan*, 706 F. Supp. 1102, 1113 (S.D.N.Y. 1989) ("The degree to which a warrant must state its terms with particularity varies inversely with the complexity of the criminal activity investigated."). The type of evidence sought is also relevant; in particular, courts have recognized that documentary evidence may be difficult to describe *ex ante* with the same particularity as a murder weapon or stolen property. *See, e.g., 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. Zanche*, 541 F. Supp. 207, 210 (W.D.N.Y. 1982) ("Unlike other forms of property, business records are often incapable of being itemized one

by one, particularly when their existence, but not their precise names or quantity, is all that is known.").

Document searches pose unique Fourth Amendment concerns. As the Supreme Court noted more than 30 years ago:

> [T]here are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In 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. . . . [R]esponsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.

Andresen, 427 U.S. at 482 n.11. The dawn of the Information Age has only heightened those concerns. The risk of exposing intimate (and innocent) correspondence to prying eyes is magnified because "[c]omputers . . . often contain significant intermingling of relevant documents with documents that the government has no probable cause to seize." *United States v. Vilar*, 2007 WL 1075041, at *35 (S.D.N.Y. 2007) (citation and internal quotation marks omitted); *see also United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1005 (9th Cir. 2009) ("Seizure of . . . Google's email servers to look for a few incriminating messages could jeopardize the privacy of millions."). However, "it is precisely because computer files can by intermingled and encrypted that the computer is a useful criminal tool." *Vilar*, 2007 WL 1075041, at *35.

Courts and commentators have wrestled with how best to balance privacy interests and legitimate law-enforcement concerns in the context of computer searches. One approach would require law-enforcement officials to specify a search protocol *ex ante* and to use, whenever possible, "key word searches . . . to distinguish files that fall within the scope of a warrant from files that fall outside the scope of the warrant." Raphael Winick, *Searches and Seizures of Computers and*

Computer Data, 8 Harv. J.L. & Tech. 75, 108 (1994). Another would require the creation of "firewalls" to prevent investigators and prosecutors from obtaining the results of a computer search until documents within the scope of the warrant had been segregated by a third party. The Ninth Circuit recently endorsed variants of both procedures, among others, to minimize the intrusiveness of computer searches. *See Comprehensive Drug Testing*, 579 F.3d at 1006 ("Segregation and redaction must be either done by specialized personnel or an independent third party. . . . The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents."). As Judge Karas noted in *Vilar*, however, the majority of courts to have considered the question have not required the government to specify its search protocol in advance. *See* 2007 WL 1075041, at 37-38 (citing cases); *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 572 (2005) ("[T]he [computer] forensics process is too contingent and unpredictable for judges to establish effective ex ante rules.").

To date, the Second Circuit has not taken sides in the debate on the particularity required for computer searches. There is, however, one form of particularity whose absence the Second Circuit has unequivocally and unqualifiedly condemned: "[A]uthorization to search for 'evidence of *a* crime,' that is to say, any crime, is so broad as to constitute a general warrant." *George*, 975 F.2d at 76. "[*A*] *fortiori* a warrant not limited in scope to *any crime at all* is . . . unconstitutionally broad." *Id.* at 77. *George* represents not simply a majority view, but the unanimous view of courts across the nation. *See Spilotro*, 800 F.2d at 964 ("The use of generic descriptions in the . . . warrant still might not have been fatal had the warrant more specifically identified the alleged criminal activities in connection with which the items were sought."); *cf. United States v. Maxwell*, 920 F.2d 1028, 1033 (D.C. Cir. 1990) ("References to broad statutes

realistically constitute no limitation at all on the scope of an otherwise overbroad warrant and therefore cannot save it."); *United States v. Roche*, 614 F.2d 6, 8 (1st Cir. 1980) ("[S]ection 1341 makes illegal all frauds that utilize the mails; limitation by so broad a statute is no limitation at all." (footnote omitted)). Thus, whatever new challenges computer searches pose in terms of particularity, it is always necessary -- and hardly onerous -- to confine *any* search to evidence of particular crimes. *See, e.g., United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005) ("[W]arrants for computer searches must affirmatively limit the search to evidence of specific federal crimes or specific types of material.").

B. Reliance on Affidavits

In *George*, the government attempted to save the fatally overbroad warrant by relying on the probable-cause affidavit to show a connection between the warrant and a particular crime. *See* 975 F.2d at 76. The Second Circuit rejected the attempt:

> A sufficiently specific affidavit will not itself cure an overbroad warrant. Resort to an affidavit to remedy a warrant's lack of particularity is only available when it is incorporated by reference in the warrant itself and attached to it.

Id.

The circuit court confronted the same argument less than a year later in *United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993). The search warrant at issue in *Bianco* authorized officers to search a defendant's home and seize, without limitation, "[N]otes, Ledgers, Envelopes, Papers, and Records Containing Initials, Names, Addresses, Dollar Amounts, Codes, Figures, and the Like: United States Currency." *Id.* at 1115. The affidavit supporting the warrant explained that the search was for evidence of the defendant's loansharking activities. *See id.* William Hutton, an FBI agent who supervised the search team and decided which items were to be seized, "had familiarized

himself with the warrant and its supporting affidavit, and was aware that he was looking for evidence of loansharking." *Id.* In addition, the defendant was made aware of the purpose and limitations on the search. *See id.* at 1117.

The Second Circuit began by "focusing solely on the warrant itself," and concluded that it was overbroad because "when viewed by itself, [it] describe[d] neither the precise items to be seized nor the possible crimes involved." *Id.* at 1116. The court then noted that the supporting affidavit was neither expressly incorporated into nor physically attached to the warrant; nonetheless, it allowed the affidavit's limitations on the search to be read into the warrant, eschewing the "formal requirements of incorporation and attachment" in favor of a "commonsense" approach because "the functional purposes of those two requirements -- to insure that all parties involved are informed of the scope of and limits upon the authorized search -- were fully satisfied," *id.* at 1117:

> In this case, it is clear that both the federal agents and [the defendant] were apprised of [the scope of and limitations on the search.] The affidavit was present at the time of the search, and spells out quite clearly the nature and purpose of the proposed search. It explains in detail the motivation behind the search and the nature of the documents sought. When the warrant and affidavit are read together, there is no ambiguity. Moreover, although the warrant may not have explicitly incorporated the affidavit, the presence and activity of agent Hutton, who had read the affidavit and who approved each seizure, satisfies us that the limitations included in the affidavit were observed.

Id.

However, as I explained in *Cohan*, the exception carved out in *Bianco* can no longer be viewed as the law of the Second Circuit in light of the Supreme Court's subsequent decision in *Groh v. Ramirez*, 540 U.S. 551 (2004). Two of my colleagues have reached the same conclusion. *See Vilar*, 2007 WL 1075041, at *22 n.13 ("*Bianco* is of questionable use to the Government [because *Groh*'s] holding sheds doubt on whether an unincorporated document may ever be used

to satisfy the particularity requirements of the Fourth Amendment."); *United States v. Ryan*, 2008 WL 901538, at *2 (D.Vt. Mar. 31, 2008) ("[*Bianco*] does not survive the Supreme Court's decision in *Groh*.").

In *Groh*, -- a *Bivens* action -- the defendant, an ATF agent, applied for a warrant to search the plaintiff's ranch. The application was supported "with a detailed affidavit, which [the defendant] also prepared and executed, that set forth the basis for his belief that [weapons] were concealed on the ranch." *Id.* at 554. The warrant, however, "failed to identify any of the items that [the defendant] intended to seize" and "did not incorporate by reference the itemized list contained in the application." *Id.* at 554-55. The defendant led the search team executing the warrant. *See id.* at 555.

In the Supreme Court, the defendant conceded that the warrant was invalid on its face, but argued that it was saved by the limitations contained in his supporting affidavit. The Court squarely rejected that argument: "The fact that the *application* adequately described the 'things to be seized' does not save the *warrant* from its facial invalidity. The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents." *Id.* at 557. The Court recognized that "most Courts of Appeals have held that a court may construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant." *Id.* at 557-58. Since the affidavit at issue had not been attached and formally incorporated by reference, the Court did not "further explore the matter of incorporation." *Id.* at 558.

Therefore, as I explained in *Cohan*, *Bianco*'s "commonsense" exception to formal incorporation and attachment did not survive *Groh*. *See* 628 F. Supp. 2d at 363. After noting that my conclusion was in accord with *Vilar* and *Ryan*, I pointed out that the Second Circuit recently held

in *United States v. Waker*, 534 F.3d 168 (2d Cir. 2008), that *Groh* did not preclude reliance on the supporting affidavit since it was attached to the search warrant and the warrant contained "deliberate and unequivocal language of incorporation." *Id.* at 172. I then clearly summarized my view of the state of the law:

> [I]n light of *Groh* and *Waker*, the Government cannot rely on language in a warrant simply referencing the underlying affidavit to satisfy the particularity prong of the Fourth Amendment; rather, it must attach the affidavit to the warrant and incorporate it by reference using "deliberate and unequivocal language."

Cohan, 628 F. Supp. 2d at 363 (quoting *Waker*, 534 F3d. at 172).

In addition to the clarity of *Groh*'s holding, the factual similarity between *Groh* and *Bianco* now reinforces my conclusion. As Justice Thomas noted in dissent, the defendant -- who had prepared the supporting affidavit -- had "briefed the search team and provided a copy of the search warrant application, the supporting affidavit, and the warrant for the officers to review." *Id.* at 576 (Thomas, J., dissenting). The defendant and the search team "then conducted the search entirely within the scope of the warrant application and warrant; that is, within the scope of what the Magistrate had authorized." *Id.* If anything, the facts of *Groh* present a stronger case for excusing the lack of formal incorporation and attachment than *Bianco*. The majority, however, thought those facts irrelevant and made no exception for situations in which the executing officer was aware of the affidavit's contents.

C. Application

The Warrant did not, on its face, limit the items to be seized from Tannin's personal email account to emails containing evidence of the crimes charged in the indictment, or, indeed, any crime at all. It was, therefore, unconstitutionally broad under *George*.

Before 2004, the Affidavit might have saved the Warrant under *Bianco*. It clearly shows that Munster was seeking authority to seize only "evidence of activities relating to conspiracy to commit securities fraud and wire fraud, in violation of 18 U.S.C. § 371; securities fraud, in violation of 15 U.S.C. §§ 78j(b) and 78ff; and wire fraud, in violation of 18 U.S.C. § 1343." Affidavit ¶ 25. Both Munster and the prosecution team were undoubtedly aware that they were to

search Tannin's personal email account only for evidence relating to those crimes. Because, however, the Affidavit was not attached to or formally incorporated into the Warrant, *Groh* renders it an irrelevancy.

My conclusion that the Warrant violates the Fourth Amendment does not end the inquiry. The remedy for an overbroad search and seizure is suppression of the resulting evidence. *See United States v. Matias*, 836 F.2d 744 (2d Cir. 1988).[8] The government, however, invokes two exceptions to that rule: the "good faith" exception and the "inevitable discovery" doctrine.

III

In *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court held that a violation of the Fourth Amendment does not justify exclusion of the resulting evidence "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." *Id.* at 920. The good-faith inquiry "is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Id.* at 922 n.23. In that regard, it "requires officers to have a reasonable knowledge of what the law prohibits." *Id.* at 919 n.19. Thus, the exception will not apply if the warrant is "so facially deficient -- i.e., in failing to particularize the place to be searched or the things to be seized -- that the executing officers cannot reasonably

---

[8]In that regard, it bears noting that, under the doctrine of severance, only the evidence seized pursuant to the invalid portions of the warrant are suppressed; evidence seized under any valid portions of the warrant remains admissible. *See George*, 975 F.2d at 79 ("When a warrant is severed (or redacted) the constitutionally infirm portion -- usually for lack of particularity or problem cause -- is separated from the remainder and evidence seized pursuant to that portion is suppressed; evidence seized under the valid porition may be admitted."). Here the lack of particularity pervades the entire Warrant; there is, therefore, no valid portion under which the November 23rd Email could have been seized.

presume it to be valid." *Id.* at 923.[9]

As noted, there many unresolved questions regarding the parameters of a search for computer documents. *See supra* Part II. In light of the Second Circuit's silence on these thorny issues, an officer could reasonably believe that search protocols and similar procedures are not constitutionally mandated.

This case, however, is not about search terms or firewalls. It is, rather, about the fundamental and venerable prohibition on general warrants. Since "it is obvious that a general warrant authorizing the seizure of evidence without mentioning a particular crime or criminal activity to which the evidence must relate is void under the Fourth Amendment," "no reasonably well-trained officer could believe otherwise." *George*, 975 F.2d at 77.

Before *Groh*, an executing officer might reasonably (and correctly) believe that his or her knowledge of the probable-cause affidavit would, under *Bianco*, cure a facially overbroad warrant. But *Groh* has been on the books since 2004. Indeed, the Supreme Court believed no reasonable officer could question its holding even then. Since *Groh* was a civil case, the Court was not called upon to directly apply *Leon*'s good-faith exception; however, it did address -- and reject -- the defendant's claim of qualified immunity, the doctrine upon which *Leon* was based:

> Given that the particularity requirement is set forth in the text of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid . . . . [A]s we observed in [*Leon*], 'a warrant may be so facially deficient – i.e., in failing to particularize the place to be searched or the things to be seized – that the executing officers cannot reasonably presume it to

[9]The exception will also not apply (1) "if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth"; (2) "in cases where the issuing magistrate wholly abandoned his judicial role"; or (3) if the warrant is "based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Leon*, 468 U.S. at 923 (citation and internal quotation marks omitted). Those circumstances are not present here.

be valid.' This is such a case.

540 U.S. at 564-65 (quoting *Leon*, 468 U.S. at 923).

IV

The government has also invoked the "inevitable discovery" doctrine, under which unlawfully seized evidence is not suppressed if "the prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means." *Nix v. Williams*, 467 U.S. 431, 444 (1984). The Second Circuit has held that "[t]he exception requires the district court to determine, viewing affairs as they existed at the instant before the unlawful search, *what would have happened* had the unlawful search never occurred." *United States v. Eng*, 997 F.2d 987, 990 (2d Cir. 1993) (emphasis in original).

The government does not -- and could not -- argue that the November 23rd Email *would* have been discovered by lawful means had the Warrant never been executed. Rather, it argues that the email *could* lawfully be obtained through another, more particularized warrant *now that the Warrant has been invalidated.* This distinction is dispositive because for purposes of the doctrine, timing is everything.

In *United States v. Whitehorn*, 829 F.2d 1225 (2d Cir. 1987), FBI agents conducted a warrantless "bomb sweep" of the defendant's apartment; during the sweep, they found a false passport and driver's license. Prior to the sweep, however, other agents had begun preparing a search-warrant application for the same premises; the warrant, which was issued later the same day, authorized the seizure of, *inter alia*, "false identities of federal fugitives." *Id.* at 1228. In those circumstances, the Second Circuit held, the doctrine was applicable:

> Agents at the F.B.I. office actually began the warrant application process over an hour before the illegal bomb sweep of [the defendant's] apartment occurred. They had already pinpointed the

> apartment to be searched. Through interviews with neighbors as well as prior extensive investigation, they knew that two of the apartment's occupants, Evans and Buck, had a history of trafficking in false identification documents, weapons, and explosives; indeed, the night before Evans and Buck had been arrested carrying all but the latter. In short, the agents had overwhelming probable cause before the bomb sweep to search the apartment in the belief that it was being used . . . as a "safe house" for federal fugitives in which false identification documents and other types of information detected by the bomb sweep reasonably could be expected to be found. Under these circumstances, and given that the agents were then proceeding to secure a warrant which specifically authorized the seizure of the challenged evidence, we conclude that the district court properly denied Whitehorn's motion to suppress the evidence first detected by the bomb sweep.

Id. at 1231. By contrast, in *United States v. Cabassa*, 62 F.3d 470 (2d Cir. 1995), the circuit court rejected the doctrine in a case in which the application process had begun, but no warrant had been issued:

> In cases in which a claim of inevitable discovery is based on expected issuance of a warrant, the extent to which the warrant process has been completed at the time those seeking the warrant learn of the search is of great importance. First, the extent of completion relates directly to the question of whether a warrant would in fact have issued; ultimate discovery would obviously be more likely if a warrant is actually obtained. Second, it informs the determination of whether the same evidence would have been discovered pursuant to the warrant. If the process of obtaining a search warrant has barely begun, for example, the inevitability of discovery is lessened by the probability, under all the circumstances of the case, that the evidence in question would no longer have been at the location of the illegal search when the warrant actually issued.

Id. at 473.

The specific concerns raised in *Cabassa* are not present here. There is little doubt that the government could now obtain a warrant authorizing a search that would yield the November 23rd Email, and that the email would still be found still present on Google's server. Nevertheless, the government's timing still presents a problem: Having seen the November 23rd Email, the

government is now in a position to obtain a warrant with perfect particularity. There is, in other words, no way to purge the taint of its unconstitutionally overbroad search.

Even if I were to restrict the government to the facts set forth in the Affidavit, a more fundamental problem would remain. The "inevitable discovery" doctrine is essentially a rule of harmless error. *See Nix*, 467 U.S. at 443 n.3 ("The ultimate or inevitable discovery exception to the exclusionary rule is closely related in purpose to the harmless-error rule[.]"). No court has ever endorsed the view that it would allow the government to retroactively *cure* a Fourth Amendment violation, and it is easy to see why. The violation is not the discovery of incriminating evidence, but the invasion of the searchee's privacy. Since such a violation is inherently irremediable, the exclusionary rule exists to deter violations in the first instance. *See Elkins v. United States*, 364 U.S. 206, 217 (1960) ("The [exclusionary] rule is calculated to prevent, not to repair. Its purpose is to deter -- to compel respect for the constitutional guaranty in the only effectively available way -- by removing the incentive to disregard it."). It is one thing to say that there is no need to deter by suppressing evidence that would have been discovered regardless of unconstitutional conduct; it is quite another to allow the government a second chance to fix a problem that never should have arisen.

V

In concluding, I note that my observation in *Cohan* -- that, in light of *Groh*, a facially invalid warrant cannot be salvaged unless a particularized affidavit is attached to the warrant and incorporated into the warrant by reference -- was technically *dicta* since I found that the warrant there was sufficiently particular. *See* 628 F. Supp. 2d at 362. Nonetheless, I thought that this *dicta* was appropriate to alert the government that if it did not heed *Groh's* holding in the future, it would risk the suppression of evidence that it wished to introduce at trial.

I have been the assigned judge on this case since its inception over a year ago. *Cohan* was issued this past June, two weeks before the Warrant was sought. The government was, therefore, on explicit notice that my understanding of the Supreme Court's holding in *Groh* would undoubtedly oblige me strike down a facially invalid warrant in the absence of incorporation and attachment of the supporting affidavit.

CONCLUSION

Tannin's motion to suppress is granted. The government is barred from introducing the November 23rd Email into evidence in its case-in-chief.[10]

SO ORDERED.

FREDERIC BLOCK
Senior United States District Judge

Brooklyn, New York
October 26, 2009

[10]The exclusionary rule does not bar the prosecution from using illegally obtained evidence to impeach the defendant's own testimony. *See James v. Illinois*, 493 U.S. 307, 308-09 (1990).