SUPREME COURT OF THE STATE OF NEW YORK
NEW YORK COUNTY CRIMINAL TERM: PART-95

----------x

THE PEOPLE OF THE STATE OF NEW YORK	.	
	.	**Ind. No.: 3853/14**
	.	
-against-	.	
	.	**DECISION & ORDER**
ANTHONY J. THOMPSON,	.	
ERIC VAN NGUYEN,	.	
JAY FUNG,	.	
JOSEPH DERVALI,	.	
CHRISTOPHER BALSEIRO,	.	
HANNA SCHMIEDER,	.	
LUZ RODRIGUEZ,	.	
KENNETH OXSALIDA,	.	
	.	
Defendants.	.	
	.	

----------x

DANIEL P. CONVISER, J.:

New York County District Attorney Cyrus R. Vance, Jr. (Garrett A. Lynch, Brian A. Kudon and Sean Pippen, of counsel) for the People.

Thompson Hine (Miranda E. Fritz, of counsel) for Defendant Anthony Thompson.

The Defendants are charged with 85 counts of securities fraud, scheme to defraud, criminal possession of stolen property and grand larceny. The charges arise out of nine alleged fraudulent "pump and dump" penny stock promotion schemes. Defendant Anthony Thompson moves here to suppress approximately 100,000 of his emails recovered in the execution of two search warrants directed to his internet service providers in 2012.

For the reasons outlined *infra*, the Court holds that: (i) the People were not required to obtain an eavesdropping warrant to seize the emails; (ii) the warrants were supported by probable cause; (iii) the warrants, as interpreted by the People, were overbroad; (iv) the First Department's recent assertion in the case of *In re 381 Search Warrants Directed to Facebook, Inc.*, 132 AD3d

11 (1st Dept 2015), *lv granted,* 2015 NY SlipOp 93656 ("*Facebook"*) that the Fourth Amendment does not apply to seizures like those here because of the "third-party doctrine" means suppression is not an available remedy in this case; (v) the Defendant's suppression motion is therefore denied in all respects, and (vi) the People are hereby ordered to return and expunge seized communications they did not identify as responsive to the warrants prior to February 6, 2015 as outlined in section 10 of this Decision.

1. General Factual Background

The parties in this case are all alleged to have been participants in a series of penny stock pump and dump schemes. A penny stock is one which trades for less than $5 per share, is not listed on the NASDAQ and requires limited disclosure, making investments more risky and volatile. The alleged principal of the schemes was Kevin Sepe. Mr. Thompson is alleged to have been a key participant in the frauds through penny stock promotional internet newsletters he owned which fraudulently touted the stocks. It is alleged that Thompson was compensated with substantial shares of the companies which he sold during the promotions and was a key participant in the frauds. Kevin Sepe and the Defendants are alleged to have earned millions of dollars in profits from the stock sales.

It is alleged that the Defendants acquired companies with little or no assets and trading volume and promoted the stocks during discrete periods through multiple internet newsletters. They employed various fraudulent devices, such as hiding the fact that virtually all of the company stock was owned by Sepe and his nominees and that the stock tips outlined in multiple seemingly unconnected internet newsletters were in fact all coming from promotions generated by the defendants. The Defendants carefully coordinated their sales of the company's stock to coincide with the promotions. Share price and volume rose rapidly during the promotions and

the Defendants then sold their stock for significant profits. The promotional periods then ended and share prices and volume fell dramatically. Numerous individual investors lost sums ranging from several thousand to over forty thousand dollars. In multiple cases, individual investors lost virtually all of the money they paid for the stocks when share prices plummeted.

2. The Search Warrants and Search Warrant Affidavits

The warrants here authorized the seizure of communications from two of Thompson's email accounts, one at gmail and one at hotmail (the "gmail" and "hotmail" accounts). The gmail warrant was initially issued on December 21, 2011 by Criminal Court Judge James M. Burke. A revised warrant was issued by Criminal Court Judge Melissa Jackson on January 4, 2012[1]. The hotmail warrant was issued on June 21, 2012 by Judge Burke. Both of the warrants were supported by substantively identical affidavits from an investigator for the New York County district attorney's office alleging there was reasonable cause to believe the emails would provide evidence of a Scheme to Defraud in the First Degree (PL 190.65) and related crimes. The affidavits sought identifying information from the accounts, evidence of the commission of crimes, information concerning persons the Defendant communicated with and evidence of financial proceeds derived from the crimes.

The information supporting the affidavits came from an investigator for the United States Securities and Exchange Commission (the "SEC"), Timothy Nealon. Mr. Nealon had investigated a microcap or "penny stock" called Blast Applications ("BLAST"). BLAST was a company which claimed to develop applications for Iphone, Facebook and Twitter but whose monthly profits rarely exceeded a few hundred dollars. Nealon asserted that BLAST's stock history provided evidence its owners had engaged in a pump and dump scheme. In a pump and

1The revised warrant was issued because of a typographical error in the original. Both Judge Burke and Judge Jackson are now Acting Supreme Court Justices.

dump, share prices are inflated by having conspirators buy and sell stock on the same day to create the false impression the stock is being actively traded in the market and through website advertising campaigns which indicate, with no basis, that a stock is poised to significantly increase in value.

The affidavits asserted there were certain "red flags" indicating a pump and dump with respect to BLAST. These were consulting agreements where the company contracted with promoters who were then compensated with large shares of the company's stock, extensive promotion, the exercise of the right to obtain shares by consultants on the eve of a promotion, a large increase in stock volume and price over a short period and the liquidation of the shares by the consultants during the promotion.

BLAST issued 100 million shares in October of 2009. Multiple consultants were hired to promote the company including OTC solutions ("OTC") which was owned by Anthony Thompson. OTC was compensated with 18 million shares of BLAST stock. It was asserted that OTC and other promoters colluded to artificially inflate BLAST's share price. The affidavits included emails from Mr. Thompson to two other promoters including one in which Mr. Thompson apparently directed a second defendant to disclose that he would be compensated with 6 million shares rather than 18 million shares. The emails also indicated a plan to sell the shares at a specific time and split the proceeds.

Promotion of the stock began on November 18, 2009. The promotion claimed the stock could rise up to 500% in value. The affidavits alleged the promotion falsely stated the amount of compensation received by the promoters was 6 million rather than 18 million shares. Prior to the promotion, BLAST stock averaged .02 cents per share with a daily trading volume of less than 1000 shares. On the first day of the promotion, the share price jumped to .05 cents and trading

volume was over 45 million shares. On that same day, OTC sold 2.35 million shares and a second conspirator sold 3.4 million shares for a total profit of over $250,000. The following day, Mr. Thompson and a second alleged conspirator emailed to discuss how to coordinate their share liquidations. By the end of the month, OTC had sold all of its 18 million shares for a profit just over half a million dollars. As is typical in a pump and dump, the share price then fell dramatically. From November 30, 2009 until the end of the calendar year, the share price never rose above .015 cents per share and daily trading volume was a few hundred thousand shares.

The warrants authorized the seizure of communications from January 1, 2008 through the warrant dates. With respect to the gmail warrant, this included communications until January 4, 2012 (a period of four years). With respect to the hotmail warrant, this included communications until June 21, 2102 (a period of roughly 4 ½ years). The warrants authorized the email service providers to conduct the searches and provide the emails to law enforcement.

The People seized all of the communications in the subject email accounts within the 10 days authorized by the warrants. They then had the contents of the recovered emails assessed by a "privilege review team" to segregate any attorney-client communications from the assistant district attorneys working on the investigation. The People have provided copies of all of these email files to the Defendant (who, presumably, has them in any event). The People have also continued to retain all of the communications they seized. This includes emails the People believe are responsive to the warrants as well as communications the People concede they have never determined have any relevance in this case. The Defendant alleges that included in these emails are purely personal and intimate communications. The People estimate that the 100,000 emails they seized include approximately 670,000 electronic records totaling 1.65 million pages.[2]

In order to identify relevant communications following the privilege review, the People

2People's February 3, 2016 Letter Submission ("People's Letter Submission"), p. 13.

put the emails into a database and used search terms to look for potentially responsive material. The People described this process as "tagging" the relevant communications and say they last searched the database for responsive emails in September of 2014. The indictment was issued on August 15, 2014. The People concede that they are not permitted to keep the non-relevant communications indefinitely. They also assert, however, that there is no "bright line" defining how long they are entitled to retain them and take the position that they should be allowed to keep all of the seized communications (including material never determined to be responsive to the warrants) and continue to search the emails until the trial proceedings in this case are over. On January 26, 2016, this Court issued an interim order directing the People not to search for or use any materials in the database other than those they had already identified as being responsive to the warrants pending the instant Decision.

CONCLUSIONS OF LAW

The Defendant makes four claims here. First, he asserts the People were required to obtain eavesdropping warrants to seize Thompson's emails. Second, he argues the search warrant affidavits failed to demonstrate probable cause to believe a crime had been committed. Third, he claims the warrants were overbroad. Finally, he asserts the People failed to complete the execution of the warrants by isolating relevant emails and returning or expunging non-responsive material within a reasonable time. He asserts that each of these arguments warrants the suppression of all of the seized material.

3. The People Were Not Required to Obtain Eavesdropping Warrants

The Defendant first claims the warrants were defective because they did not comply with New York's eavesdropping statute, CPL 700.05. That statute contains requirements for "wiretapping", the "mechanical overhearing of conversation" or the "intercepting or accessing of

an electronic communication" as defined by the Penal Law CPL 700.05 (1). At least one trial court has recognized, however, that New York's eavesdropping statute is designed to cover communications in transit rather than stored emails like those here. *See Gurevich v. Gurevich,* 24 Misc3d 808 (Kings County Supreme Court 2009 [Sunshine, J.]).

This issue was also addressed by the First Department in *Facebook.* The holding in that case, that Facebook did not have the right to challenge search warrants issued for the seizure of customer communications before a search warrant execution, is not directly relevant here. The *Facebook* Court also expressed its views, however, on two issues which are applicable to the instant motion. First, the Court asserted that under the "third-party doctrine" email users who entrust the security of their on-line communications to third-parties like Facebook relinquish any Fourth Amendment protection for that information:

> The Fourth Amendment to the U.S. Constitution protects the people's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures". (citation omitted). However, when applied to information stored online, the Fourth Amendment's protections are potentially far weaker. In part, this is because computer records are stored in a technologically innovative form, raising the question whether they are sufficiently like other records to engender the "reasonable expectation of privacy" required for Fourth Amendment protection.
> Furthermore, users generally entrust the security of online information to a third party, an ISP. In many cases, Fourth Amendment doctrine has held that, in so doing, users relinquish any expectation of privacy (*see Smith v. Maryland,* 442 US 735, 99 SCt 2577, 61 LEd 220 [1979]). The Third-Party Doctrine holds that knowingly revealing information to a third part relinquishes Fourth Amendment protection in that information (*see* Orin S. Kerr, *The Case for the Third-Party Doctrine,* 107 Michigan L. Rev. 561 [2009]). While a search warrant and probable cause are required to search one's home, under the Third-Party Doctrine only a subpoena and prior notice (a much lower hurdle than probable cause) are needed to compel an ISP to disclose the contents of an email or of files stored on a server. 132 AD3d at 20-21.[3]

In analyzing Facebook's right to contest the issuance of the warrant for its subscriber

---

3In a footnote, the Court explained: "Unlike the tangible physical objects mentioned by the Fourth Amendment, computer records typically consist of ordered magnetic fields or electrical impulses." n. 6 (citations omitted).

communications in that case, the *Facebook* Court also looked the Federal Stored Communications Act, 18 USC § 2703 ("SCA") which governs the manner in which email communications may be seized under federal law. The Court noted that in order to obtain stored communications under the SCA, like those at issue here, the police must obtain a search warrant. 132 AD3d at 22, *citing* 18 USC § 2703 [a] & [b]. The Court held that the search warrants in the Facebook case were "analogous to SCA section 2703 (a) warrants" because they authorized the government through the issuance of a warrant to seize stored communications.[4] The Court concluded that the SCA provided "Fourth Amendment-like privacy protections for email and other digital communications stored on the Internet." 132 AD3d at 21.

New York courts have thus recognized both that New York's eavesdropping statute applies only to communications in transit and that the procedure the People followed here, obtaining a search warrant directed to an ISP to obtain customer communications, is the proper vehicle for obtaining such material. This Court thus finds that the basic procedure the People used here, to obtain a search warrant, was proper.

4. The Warrants Were Supported by Probable Cause

A search warrant application "must provide the magistrate with information sufficient to support a reasonable belief that evidence of illegal activity will be present at the specific time and place of the search". *People v. Edwards,* 69 NY2d 814, 816 (1987). A "presumption of validity" attaches to a warrant issued by an impartial magistrate who has already reviewed information supporting probable cause and found it sufficient. *People v. Castillo,* 80 NY2d 578,

---

4The SCA, as the *Facebook* Court noted, authorizes warrants to obtain communications like those at issue here "using State warrant procedures". 18 USCA § 2703 (b) (A). But a warrant is not required under the statute. A second method of obtaining stored communications more than 180 days old is through a administrative or court-ordered subpoena. Such subpoenas or court orders may only be issued upon notice to a subscriber or customer. 18 USCA § 2703 (b) (B).

585 (1992), *cert denied*, *Castillo v. New York*, 507 US 1033 (1993). Two judges in this case found, based on substantively identical affidavits, that the People provided probable cause to search the Defendant's emails. The evaluation of whether a warrant affidavit is supported by probable cause should be based on all the facts and circumstances viewed together, and the affidavit should not be read in a hypertechnical manner, but viewed in the light of everyday experiences. *People v. Gramson*, 50 AD3d 294 (1st Dept 2008), *lv denied*, 11 NY3d 832. In this Court's view, the warrants were supported by probable cause.

The Defendant argues that the facts in the affidavits indicated only that he engaged in normal and lawful promotional activity designed to generate interest and increase the price of a stock. This Court does not agree. The affidavits outlined not only the general parameters of a fraudulent pump and dump, but explained how the specific actions taken by the Defendant were typical of and could be construed as being designed to facilitate such a scheme.

They alleged that the Defendant directed a co-defendant, Eric Van Nguyen, to make one specific fraudulent representation: that he was being compensated with 6 million shares of BLAST stock for the promotion rather than 18 million shares, which the communications between Defendants Thompson and Nguyen appeared to indicate was the actual amount of compensation Nguyen received. The Defendant asserts that this communication was not in fact fraudulent because there were three companies engaged in the promotion and each received only 6 million shares, not 18 million.

As the Defendant also points out, the affidavits primarily relied upon the claim that the promotion of BLAST and the Defendant's profits from the BLAST sales bore all the tell-tale signs of a fraud. The affidavits did not recount how, if at all, any of the representations the Defendant made about the BLAST stock were fraudulent. Probable cause here also required the

two judges to draw the inferences the People urged them to draw. The two judges who issued the warrants, however, in the Court's view, were entitled to draw the reasonable inferences which the affidavits asked them to make with respect to how the details of the BLAST promotion were indicative of a pump and dump.

5. The Warrants, As Interpreted by the People, Were Overbroad

The Warrants' Literal Terms

The affidavits in support of the search warrants outlined alleged fraudulent conduct with respect to one penny stock: BLAST. But the warrants were much broader.[5] Their first operative section authorized the seizure of evidence regarding:

> commission of, participation in, knowledge of, or any other form of involvement in any of the crimes mentioned above and/or related crimes, including, but not limited to, involvement in a scheme to defraud and related crimes, which may be evidenced through . . . (hereinafter the "first paragraph")

Next, the warrants authorized information about the identity of crime "participants and/or accomplices in any of the crimes mentioned above and/or related crimes, including, but not limited to, involvement in a scheme to defraud . . ." (hereinafter the "second paragraph"). Finally, the warrants authorized the seizure of "evidence of proceeds from the commission, participation in or involvement in the above-described crimes, including but not limited to, stored electronic communications . . ." (hereinafter the "third paragraph").[6] Pursuant to this authority the People seized not only emails relevant to BLAST but seven other alleged penny stock pump and dump schemes which were then presented to the grand jury which issued the indictment.

5As noted *supra*, the warrant affidavits and warrants were substantively identical except that they related to different email accounts and were signed on different dates by different judges. The affidavits and warrants are referenced here in both a singular and plural tense as appropriate.

6Hotmail Warrant.

The Fourth Amendment, of course, requires that a warrant will not issue unless supported by an oath "particularly describing the place to be searched, and the persons or things to be seized". The question is whether the warrants met that requirement. There are first a number of issues regarding the warrants' language. The first warrant paragraphs began by accusing the Defendant of "involvement in any of the crimes mentioned above". The warrants, however, did not denominate any crimes in these "above" provisions. The warrant affidavits recounted alleged criminal conduct concerning BLAST and asserted that this information indicated the target accounts had been used "to coordinate and engage in a pump and dump fraud scheme".[7] The affidavits also alleged the warrant executions would uncover evidence of a "Scheme to Defraud in the First Degree, PL § 190.65, and other related crimes."[8] The Court will read the warrants as referencing the affidavits, which is what the People obviously intended .[9]

The provisos "related to", as they are written in the warrants, describe relations of a multiple order. In the first paragraph evidence of "related crimes" are authorized to be seized. The provision then goes on to note one such "related crime" would be a scheme to defraud. But then, additionally, the warrants authorize evidence to be seized if it is a related crime to a scheme to defraud (provided the scheme to defraud is a related crime to the crimes recounted in the affidavits). Returning to the affidavits, however, they also describe a "Scheme to Defraud in the First Degree, PL § 190.65, and other related crimes". Thus the warrants' first paragraph literally provides (reading backwards beginning with the first warrant paragraphs and proceeding to the

---

7Hotmail Warrant Affidavit, ¶ 8.

8*Id.,* ¶ 2.

9This is not a trivial point. A warrant may refer to an affidavit through "appropriate words of incorporation" but "[t]he Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents. . . . The Fourth Amendment requires that the *warrant* particularly describe the things to be seized, not the papers presented to the judicial officer . . . asked to issue the warrant." *Groh v. Ramirez,* 540 US 551, 557-558 (2004) (quotation omitted, second ellipsis in original, emphasis in original).

affidavits) authority to seize evidence of "involvement in a scheme to defraud and related crimes" if such crimes are "related crimes" to a "Scheme to Defraud in the First Degree, PL § 190.65, and other related crimes".

The second paragraph concerning the authority to seize identity information expands the "related crimes" authority to a fourth order. Here, the warrants first authorize the seizure of evidence of "any of the crimes mentioned above" which includes the immediately preceding recitations in the first paragraph and the affidavits. The second paragraph then goes on to authorize the seizure of identity evidence of "related crimes, including, but not limited to, involvement in a scheme to defraud". Read literally then (again, reading backwards this time from the second paragraph), such evidence may be seized if it is a "related crime" to "involvement in a scheme to defraud and related crimes" if those crimes are "related crimes" to a "Scheme to Defraud in the First Degree, PL § 190.65, and other related crimes". The third paragraph, dealing with evidence of proceeds of a crime, provides identical authority by referencing "involvement in the above-described crimes".

The term "related crimes" is not defined. The warrants can only be read, however, as providing that such "related crimes" would extend beyond a "scheme to defraud" since the warrants twice note that such related crimes include but are "not limited to" involvement in a scheme to defraud. The preceding quotations are not provided because the Court believes the People construed the warrants as authorizing them to search for evidence of crimes within four degrees of separation from the BLAST allegations. The Court understands the People read the warrants as simply authorizing the seizure of evidence they believed was related to the BLAST pump and dump. But the warrants obviously provided the People with some flexibility in that regard.

The "Overbreadth" Cases

A review of warrants New York appellate courts have found overbroad in other cases provides guidance with respect to the instant question.[10] In *People v. Brown,* 96 NY2d 80 (2001) the Court of Appeals found a search warrant which authorized the seizure of four specific items relevant to the Defendant's alleged theft of a tractor along with "any other property the possession of which would be considered contraband" to be overbroad with respect to that final clause. The Court noted that to meet the Fourth Amendment's particularity requirement the directive in a warrant "must be specific enough to leave no discretion to the executing officer". 96 NY2d at 84. (citation and internal quotation omitted). This "no discretion" requirement "has not always been applied literally" but is rather given a reasonable construction under the circumstances. *United States v. Galpin,* 720 F3d 436, 446 (2d Cir 2013) (quotation omitted). The *Brown* Court nevertheless found that the valid portion of the warrant describing the four specific items could be severed from the invalid part and upheld the seizure of guns found in plain view during the execution of the warrant's valid portion.

In *People v. Yusko,* 45 AD2d 1043 (2d Dept 1974) a warrant which authorized a search "for dangerous drugs including, but not limited to cocaine, heroin and marijuana as well as narcotics paraphernalia" was found overbroad because the warrant affidavit provided probable cause to believe only that a letter containing cocaine would be recovered. In *People v. Marshall,* 57 AD3d 1163 (3d Dept 2008) the Court held that a search warrant authorizing the seizure of

10The terms "particularity" and "overbreadth" in Fourth Amendment jurisprudence are not always used consistently. Some decisions have treated the concepts as analytically distinct with the particularity requirement referencing whether the executing officer can ascertain with reasonable certainty the items authorized to be seized while the overbreadth doctrine refers to whether there is sufficient probable cause to justify the scope of the search. *See United States v. Carpenter,* 2015 WL 9461496 (D. Connecticut 2015 [Chatigny, J.]) at 3-5. On the other hand, New York cases tend to use the word "overbroad" simply to describe a warrant which is not sufficiently particularized and thus merge the two analytical inquiries. That latter convention is used here.

"documents that prove possession, sale or conspiracy to possess, sell and distribute heroin" did not encompass recorded narcotics buy money recovered from the Defendant's home because currency was not specifically listed as an item the police were authorized to seize. In *People v. Couser,* 303 AD2d 981 (4th Dept 2003) the Court found overbroad a warrant authorizing the seizure of "papers of [defendant]" relating to a specific homicide. The Court found the police had probable cause to search for three specific items and that this right did not permit the inference that they had probable cause to search for others.

In *People v. Smith,* 138 AD2d 932 (4th Dept 1988) the Court found the description "soiled mens clothing" in a search warrant authorizing the seizure of evidence of what was apparently an arson resulting in attempted murder charges to be overbroad where the warrant did not identify the "type, color, size or ownership of the clothing". *See also, People v. Niemczycki,* 67 AD2d 442 (2d Dept 1979), *abrogated on other grounds*, *People v. Brown*, 96 NY2d 80 (2001) (warrant authorizing search for marijuana and "any other contraband which is unlawfully possessed" invalid as to the latter proviso).

In this Court's view, the "related crimes" authority provided by the warrants here came close to the "other unlawful contraband" warrants which have been rejected in narcotics cases. Had the warrants found overbroad in these "other" or "additional" contraband cases instead read "other *related* contraband" the results, in this Court's view, would have been no different. The authority here was certainly broader than warrants found overbroad because they authorized the search for multiple kinds of narcotics when there was probable cause to search for only one kind, the "soiled mens clothing" warrant or the "papers" of the defendant warrant related to an identified homicide which have been found invalid in other cases.

The Court has located a case which supports the People's position on the overbreadth

issue, *United States v. Juarez,* 2013 WL 357570 (EDNY 2013 [Mauskopf, J.]). In *Juarez* police seized the defendant's cell phone in an arrest for the crime of "unlawful surveillance" under New York law after he placed his cell phone camera under the skirts of women in Union Square Park and recorded them. The warrant to search the phone authorized the seizure of evidence of the unlawful surveillance crime "in the vicinity of 4th Avenue and 14th Street" in Manhattan and unspecified "related crimes and conspiracy to commit those crimes" which the Court found under the warrant had to occur "at a specific location in New York City". p 4. Child pornography was then discovered in the search of the phone.

The Court acknowledged that the "related crimes" authority was not "terribly precise" but said the specification of the underlying "unlawful surveillance" crime "cure[d] any ambiguity" with respect to the issue. p. 5. This Court does not agree with the *Juarez* Court's reasoning in that regard. But the particularity issue in *Juarez* was also fundamentally different than that here. *Juarez* concerned the question of whether a warrant which authorized a search for evidence of related crimes, which occurred at a "specific location" in connection with a discrete event was permissible. That is far different than the question of whether the authorization to search 100,000 emails transmitted over 4 ½ years for evidence of undefined crimes related to a months' long financial fraud satisfies the particularity requirement.

This is not a case where the People alleged in the affidavits that the BLAST pump and dump was indicative of a fraudulent pattern in which evidence of equivalent frauds would likely be uncovered. The affidavits uniformly asserted that a search of Thompson's emails were expected to uncover evidence of <u>one</u> pump and dump scheme.[11] This case is therefore distinguishable from those in which warrants have been held not to be overbroad because the

11*See, e.g.,* Warrant Affidavit, ¶ 7 ("I believe that individuals have used the target email account to coordinate and engage in a pump and dump fraud scheme").

evidence supporting the warrant issuance was indicative of a larger pattern of illegality. *See People v. Germaine,* 87 AD2d 848, 849 (2nd Dept 1982) (warrant which authorized search for multiple kinds of narcotics and paraphernalia justified since evidence indicated a "regular pattern of drug dealing" where the presence of "more than one single item of contraband could be anticipated").

The People argue that the assertion Thompson used his email "to coordinate and engage in a pump and dump fraud scheme" and that the search would provide "further evidence of criminal activity" alleged that evidence of additional pump and dumps would be discovered in Thompson's emails.[12] But the factual allegations in the affidavits were limited to BLAST. The vague language cited here cannot be read as asserting that the BLAST allegations provided evidence of other frauds. In fact, the Defendant asserts that although Kevin Sepe was at the hub of the non-BLAST pump and dumps alleged in the indictment, Sepe was not involved in the BLAST sales.

Of course, a larger pattern of illegality involving additional pump and dumps was what the People allege they discovered when they searched Thompson's emails. But the language of the warrants would have supported an argument that evidence of additional crimes would have been validly seized no matter what was found. That is the problem. Evidence of a tax fraud uncovered in the emails might arguably be related to the BLAST scheme. So would evidence of some other kind of financial impropriety. If Thompson had emailed a business associate in a pump and dump about child pornography or narcotics, that might arguably be an undefined "related crime" as well.

Indeed, any evidence of criminality discovered among the 1.65 million pages of Thompson's 100,000 emails would arguably be a "related crime" to the BLAST allegations by

12People's February 3, 2016 Letter Submission, p. 5, *quoting* Warrant Affidavits, ¶ 8.

definition, since it would concern the same person, Anthony Thompson, using the same email as the BLAST scheme. The People have proffered a number of definitions for the word "related" including "connected by reason of an established or discoverable relation".[13] That definition would cover any crime Thompson used his email account to commit.

The overbreadth question must also be understood in the context of the extended period the seizures covered. The affidavits alleged a scheme involving one company over a two month period, in October and November of 2009. They asserted Thompson's emails were likely to contain communications regarding the scheme during "this time period".[14] The affidavits provided no argument that emails outside this period might be relevant. The warrants authorized the seizure of all of Thompson's emails, however, over a period of 4 and 4 ½ years. This included communications 1 year and 9 months prior to the alleged crimes and more than 2 and 2 ½ years *after* the crimes were allegedly committed. Even if these date ranges in themselves were not overbroad, they certainly contributed to the overbreadth of the "related crimes" authority.

The warrants by limiting their terms only to unspecified connections involving unspecified crimes extending for years beyond any evidence of criminality allowed the People to search for evidence and then come back later when it was discovered and argue it was validly seized no matter what was found. As the Second Circuit argued in *United States v. Galpin, supra,* there must be a "heightened sensitivity to the particularity requirement in the context of digital searches" because the government, by necessity, must make at least a cursory examination of numerous non-responsive communications to discover the particular content authorized by a warrant. 720 F3d at 447. The warrants' directives in this case certainly did not "leave no discretion to the executing officer". *People v. Brown, supra.* A warrant must be "specific

13*Id.,* p. 4 *quoting* Merriam-Webster dictionary.
14Hotmail Affidavit, ¶ 6 (o).

enough" to ensure that "the Judge and not the officer fixes the scope of the search". *People v. Darling,* 95 NY2d 530, 537 (2000). That did not occur here.

Construing the Warrants as Authorizing Only a BLAST Seizure
Would Not Allow Evidence of Non-BLAST Communications to be Seized

There is an additional argument which can be made as to why the seizures here were valid and although it is not asserted by the People it is worth addressing. Even if the warrants were construed as authorizing a search only for evidence of the BLAST pump and dump, the People might have permissibly uncovered evidence of additional pump and dumps in plain view while searching for the BLAST material. This Court does not find any such "plain view" argument persuasive because the fraudulent nature of any email communications the People may have inadvertently found would not be readily apparent.

The Second Department confronted a similar argument in *People v. Haas,* 55 AD2d 683 (2d Dept 1976) where they found a warrant which authorized a search for marijuana did not authorize the seizure of "stolen goods" in plain view since those goods did not contain a "brand of illegality" and were thus not "contraband per se". The police, the Court noted, could only have determined the goods they found in plain view during the warrant execution were stolen if they carefully scrutinized them. That reasoning is obviously even more compelling here. Thompson's emails generally communicated his work touting stock and timing stock promotions and sales. There was nothing inherently unlawful about those emails. They only became evidence of illegality when they were combined with the extensive additional evidence the People presented to the grand jury.

Courts have rejected similar arguments in other cases. For example, in *United States v. Carey,* 172 F3d 1268 (10th Cir 1999) a detective executing a search warrant on a computer authorizing a search for illegal narcotics happened upon an image file which contained child

pornography and then proceeded to open other files which also contained such images. The Court suppressed all but the first image, ruling that the prosecutor should have sought an additional search warrant once the first pornographic image was discovered. Relying upon that holding, the trial court in *People v. Carratu,* 194 Misc2d 595 (Nassau County Supreme Court 2003) suppressed evidence from a computer file labeled "Fake I.D." which was opened as part of a computer search authorized for a suspected illegal cable television operation.

6. The "Third-Party Doctrine" as Applied in *Facebook*

In determining the remedy for the overbroad warrants in this case, however, the *Facebook* court's conclusion that the third-party doctrine negates any Fourth Amendment protection for subscriber communications seized from an ISP is controlling. The third-party doctrine is based on a long line of clear legal authority, most significantly the United States Supreme Court's decision in *United States v. Miller,* 425 US 435 (1976). The doctrine has also been subject to significant criticism, however. As Justice Sotomayor argued in her concurring opinion in *United States v. Jones,* 132 S.Ct. 945, 957 (2012) "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. (citations omitted). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[15]

At a time when many people routinely relay sensitive personal information by email, the assertion that no Fourth Amendment protections apply to such communications because email requires an email account, in this Court's view, is an archaic notion which negates the protection of the Fourth Amendment for many of our most private communications. This Court explored

15In *Jones,* the Supreme Court held that the government's installation of a GPS tracking device on a vehicle constituted a search under the Fourth Amendment.

the problems with the third-party doctrine as applied to personal banking records in its decision in *People v. Lomma,* 35 Misc3d 395 (New York County Supreme Court 2012). This Court, moreover, is only one of a multitude of commentators who have condemned the doctrine's expansive use. As the law review article cited by the *Facebook* court supporting the doctrine noted:

> The third-party doctrine is the Fourth Amendment rule scholars love to hate. It is the *Lochner*[16] of search and seizure law, widely criticized as profoundly misguided. Decisions applying the doctrine top the chart of the most-criticized fourth amendment cases. Wayne LaFave asserts in his influential treatise that the [United States Supreme] Court's decisions applying it are "dead wrong" and "make a mockery of the Fourth Amendment" . . . Over a dozen state Supreme Courts have rejected the doctrine under parallel provisions of their state constitutions. Orin S. Kerr, "The Case for the Third-Party Doctrine", 107 Mich L. Rev. 561 (2009), at 2, *cited in Facebook, supra,* 132 AD3d at 21 (citations and internal quotations omitted).

In this Court's view, the one case the *Facebook* court cited in support of its invocation of the third-party doctrine for digital content, *Smith v. Maryland,* 442 US 735 (1979), is also not persuasive. *Smith* held that the installation of a pen register at a telephone company's offices which recorded phone numbers the Defendant dialed did not constitute a Fourth Amendment search because persons do not have a reasonable expectation of privacy with respect to such phone numbers. Central to the Court's holding was that, unlike the overhearing of a phone call, "pen registers do not acquire the *contents* of communications." 442 US at 741 (emphasis in original). Of course, precisely the opposite is true for emails. Even the high court's seminal 1976 decision in *United States v. Miller, supra,* is of limited relevance to email content. *Miller* applied the third-party rule to a defendant's banking records, to which "the bank was itself a

---

16*Lochner v. New York,* 25 S. Ct. 539 (1905) was the namesake for the "Lochner era" in which the Supreme Court invalidated many state and federal regulations on working conditions. In *Lochner*, the Court held that a New York statute limiting the hours of bakery employees to 60 per week violated the "freedom to contract" guaranteed by the Fourteenth Amendment. The high court began to reject the use of substantive due-process to invalidate such regulations in the 1930's and *Lochner* is now seen as a product of a by-gone era.

party". 425 US at 441. The Court found these records were "not confidential communications but negotiable instruments to be used in commercial transactions". 425 US at 442.

The New York Court of Appeals in *People v. Weaver,* 12 NY3d 433 (2009) rejected the notion that the increased siting of personal information on the internet has been accompanied by any reduction in our reasonable expectations of privacy. In *Weaver* the Court held that New York's analogue to the Fourth Amendment generally requires a warrant before the police may attach a GPS device to a car, even though cars generally travel on public roads where their location is apparent to anyone:

> [T]he great popularity of GPS technology . . . may not be taken simply as a massive, undifferentiated concession of personal privacy to agents of the state. Indeed, contemporary technology projects our private activities into public space as never before . . . the advent of portable computing devices has resituated transactions of all kinds to relatively public spaces. It is fair to say, and we think consistent with prevalent social views, that this change in venue has not been accompanied by any dramatic diminution in the socially reasonable expectation that our communications and transactions will remain to a large extent private. 12 NY3d at 442-443.

Our constitution requires that when new technologies emerge which change our reasonable expectations of privacy, legal doctrines must change with them. What must remain immutable are not the physical objects whose treatment has historically been assessed to determine the proper scope of government intrusion. What must remain constant is the scope of our liberty.

Multiple federal appellate and trial courts have held that the third-party doctrine does not apply to email content held by ISP's. In *United States v. Warshak, rehearing and rehearing in banc denied,* 631 F3d 266, 288 (6th Cir 2010), the Sixth Circuit held that absent some unusual explicit agreement which abrogated an email user's privacy rights, "a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through a commercial ISP." (internal quotation and citations omitted). Commenting on

the "explosion of Internet-based communication" the Court explained:

> People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. . . Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. (631 F3d at 284). Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection. . . Email is the technological scion of tangible mail and it plays an indispensable part in the Information Age. . . If we accept that email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. *Id.* at 285-286.

The 9th Circuit reached a similar conclusion in *Quon v. Arch Wireless Operating Company,* 529 F3d 892, 904 (9th Cir 2008) holding that "users of text messaging services . . . have a reasonable expectation of privacy in their text messages stored on the service provider's network . . .". Federal trial courts have reached the same conclusion. *See In Re Applications for Search Warrants for Information Associated With Target Email Accounts/ Skype Accounts,* 2013 WL4647554 (D. Kansas 2013 [Waxse, Magistrate Judge]) at 4 ("an individual has a reasonable expectation of privacy in emails stored with, sent to, or received through an electronic communications service provider"); *United States v. Keith,* 980 F Supp2d 33, 39-40 (D. Mass 2013 [O'Toole, J.]) (email users have a reasonable expectation of privacy in the content of emails or their attached files); *United States v. DiTomasso*, 56 F Supp3d 584 (SDNY 2014 [Scheindlin, J.]) (email users generally have a reasonable expectation of privacy in email contents held by ISP's but child pornography defendant by agreeing to AOL's email monitoring policy did not have Fourth Amendment right to suppress seized emails).

As many of these cases have also held, the reasonable expectation of privacy email users have in the content of their communications is not applicable to subscriber identifying information which has been held not entitled to Fourth Amendment protection. *See United States*

v. Keith; United States v. DiTomasso, supra. Such subscriber information is analogous to the phone numbers the Supreme Court found were not subject to the Fourth Amendment in *Smith v. Maryland, supra*.

The Defendant argues, *inter alia*, that the *Facebook* Court's assertion that the Fourth Amendment is inapplicable to digital content held by ISP's is *dicta* and should not be followed here. This Court does not agree. The *Facebook* Court's assertions on the third-party issue were part of the reasoning process the Court used to determine that the SCA defined the available remedies for the seizure from Facebook and that this federal statute provided "Fourth Amendment-like privacy protections for email and other digital communications stored on the Internet." The Court's conclusions were not "superfluous". *Rose Park Place, Inc. v. State of New York,* 120 AD3d 8 (4th Dept 2014).

Dicta which is an "extraneous, gratuitous and casually expressed statement particularly in a case where the issue was neither argued nor factually relevant, can carry no controlling weight" for a lower court. *People v. Bourne*, 139 AD2d 210 (1st Dept 1988), *appeal denied*, 72 NY2d 955. The *Facebook* Court's statements concerning the third-party doctrine had none of those characteristics. Nor is the *Facebook* decision a decades old ruling, one by a closely divided court or by a tribunal this Court is not obliged to follow. It was a unanimous decision by a rare six justice panel, including the presiding justice, in a decision seven months ago by the appellate division with direct authority over this Court. The Defendant also points out that the postings at issue in *Facebook* were more widely available to the public than the private emails here. That is true. But it doesn't modify the plain language of the *Facebook* decision.

7. Suppression is Not an Available Remedy for a Violation of the SCA

The overbreadth cases outlined *supra* are based on the Fourth Amendment. The

Facebook Court determined the Fourth Amendment does not apply to search warrants for emails held by ISP's. What applies here, according to the *Facebook* Court, is the SCA. The SCA, however, does not authorize suppression for a violation of its provisions. It rather provides that the specific statutory remedies provided by the Act "are the only judicial remedies and sanctions for nonconstitutional violations of this chapter". 18 USCA § 2708. The remedy for a violation of the SCA is a civil action in which an aggrieved party can seek equitable and injunctive relief, damages and attorney's fees. 18 USCA § 2707. In accordance with the statute's unambiguous language, federal appeals courts have held that suppression is not an available remedy for an SCA violation. *See, e.g., United States v. Guerrero,* 768 F3d 351, 358 (5th Cir 2014), *cert denied,* 135 S.Ct. 1548 (2015); *United States v. Perrine,* 518 F3d 1196, 1201-1202 (10th Cir 2008); *United States v. Smith,* 155 F3d 1051, 1056 (9th Cir 1998), *cert denied*, *Smith v. United States*, 525 US 1071 (1999).

There is language in the *Facebook* decision which points in a different direction. The Court held that Facebook did not have a pre-warrant execution right to quash the warrants issued in that case because the SCA did not provide it. The Court pointed out that the remedy for search warrants which exceed the State's authority under the Fourth Amendment is a suppression motion and that "these protections eliminate any need for a suspected citizen to make a pre-execution motion to quash a search warrant." 132 AD3d at 17. At the same time, the Court held the Fourth Amendment did not apply to the Facebook content information at issue in that case or emails like those seized from the ISP's here. There is obviously a tension between these competing conclusions. But that does not justify the creation of a suppression remedy by this Court which does not exist under the SCA. The Criminal Procedure law authorizes the suppression of "tangible property" obtained through an unlawful search and seizure. CPL 710.20

(1). But this provision does not provide a substantive right to suppress evidence wholly outside the parameters of the constitution or any other law.[17] It is part of a procedural statute designed to effectuate other substantive rights.

Despite this Court's view, therefore, that the warrants in this case were overbroad under the Fourth Amendment, that conclusion does not warrant suppression. The combination of all of these rules moreover, may leave defendants like Thompson with no remedy in a trial court when warrants are overbroad. There is no constitutional remedy. There might also be no viable civil claim in a case like this. The SCA provides that it is a "complete defense to any civil or criminal action brought under this chapter or any other law" that a civil defendant, *inter alia*, relied in good faith upon a warrant or order issued by a court. 18 USCA § 2707 (e). The People could certainly claim that to the extent the warrants here were overbroad, they executed them in good faith based on their terms. As the People argue, under *Facebook*, "a federal statute, not the Fourth Amendment, provides whatever protections exist for email communications stored by third-party ISP's, and governs law enforcement's ability to obtain that information."[18]

8. The People Were Not Permitted To Retain All of Thompson's Emails

As noted above, the People here seized all of the Thompson emails which were transmitted during the warrant-authorized time periods and then searched them for responsive material. The Defendant does not argue that this initial "overseizure" was unlawful. Myriad federal authorities have held that because of the practical difficulties of isolating responsive

---

17*See* Practice Commentary to CPL Article 710, § 710.10, Peter Preiser, McKinney's 2016 (rulings provided pursuant to CPL suppression motions determine whether evidence obtained by the State was "in violation of the defendant's constitutional right or through violation of a statute designed to safeguard either that right or a closely allied value". . .)

18People's Letter Submission, p. 3. As the People also correctly point out, were suppression granted here based on the overbreadth of the warrants, it is possible that only a portion of the seized emails, rather than all of them, would be suppressed. *Id.* p. 6; *People v. Brown, supra.*

computer communications without an initial review, the basic initial procedure followed by the People in this case was proper. *See, e.g., United States v. Evers,* 669 F3d 645, 652 (6th Cir 2012) (authorizing the seizure and search of defendant's home computer and digital media equipment for subsequent off-premises search); *United States v. Lacy,* 119 F3d 742, 746 (9th Cir 1997), *cert denied, Lacy v. United States,* 523 US 1101 (1998) (similar).

But the People here are asserting a right to do far more than seize the Defendant's emails, search them for responsive communications and then expunge, return or destroy the non-responsive material. They assert that they are permitted under the warrants to retain all of the Defendant's emails so long as the instant proceeding is pending and continue to search them at their leisure or to the extent some new issue in this case might arise. The People concede that they would not be able to use the emails in a different case, although they propose no method by which such use might be regulated or foreclosed. Federal courts which have considered this issue have reached varying conclusions on it as described *infra*. In this Court's view, however, the notion that the People are entitled to retain 100,000 of the Defendant's emails and continue to search them for responsive material for a period which has now extended for more than four years is plainly unreasonable. Indeed, when the date ranges of the warrant seizures are added to the period the People have now retained Thompson's emails, the People currently possess Thompson emails they have never identified as relevant which date back more than 8 years.

The proper conduct of the government in executing "overseizure" warrants for digital communications was recently explored by the Second Circuit in *United States v. Ganias,* 755 F3d 125 (2d Cir 2014), *rehearing en banc granted*, 791 F3d 290 (2015). In *Ganias*, Army investigators executed a search warrant for the defendant\accountant's computer files in connection with a criminal investigation into fraud and theft by two of the Defendant's clients by

making a copy of all of the information in the Defendant's three computer hard drives. The files contained emails which were both responsive and not responsive to the warrant. The Army isolated the relevant files but then retained all of them. They subsequently developed information that the Defendant had improperly reported income to the IRS, which was not a subject of the initial search warrant application and expanded their investigation to include the tax issue. Almost 2 ½ years after the initial warrant execution, the government obtained a second search warrant to search the non-responsive files they still retained to obtain personal financial records for the tax investigation. The Defendant was then convicted of tax charges based in part on those records.

The Second Circuit reversed the conviction. The Court pointed out that the primary evil which motivated the adoption of the Fourth Amendment was the indiscriminate search and seizure by the British through "general warrants" not grounded upon a specific infraction by a particular person. 755 F.3d at 134 (citations omitted). The British had long used this practice to enter the home of political opponents and seize all of their papers, hoping to find evidence of criminality. "The Framers abhorred this practice, believing that papers are often the dearest property a man can have and that permitting the Government to sweep away all papers whatsoever, without any legal justification, would destroy all the comforts of society." *Id.* (internal quotations and citations omitted). The Court pointed out that the Fourth Amendment's particularity requirement restricts the government's ability to remove all of a person's papers for later review because it is generally unconstitutional to seize an item not described in a warrant, *citing Horton v. California,* 496 US 128 (1990).

Outlining the Fourth Amendment's application to computer files, the Court explained:

> Like 18th Century "papers," computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle, and they should be similarly

> guarded against unwarranted Government intrusion. If anything, even greater protection is warranted. Advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain. The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs. 755 F3d at 135 (internal quotations and citations omitted).

The Court acknowledged that the search of a Defendant's hard drives off-site after an initial warrant seizure was a reasonable procedure in most cases. It held, however, that the People could not retain every file obtained during such a seizure and use it for future investigations. The Court held the retention of the Defendant's files after the relevant materials on them had been initially segregated constituted a continuing seizure which deprived the Defendant of the exclusive use of his files. They therefore ordered the files suppressed.

The instant case is distinguishable from *Ganias* in two important respects. First, unlike *Ganias,* the People here do not argue that they would be entitled to retain the non-relevant emails indefinitely, as the government urged in *Ganias*, and use them in a future investigation. They argue only that they are permitted to retain the non-responsive emails for use in the instant case. On the other hand, the basic error the People made in *Ganias*, the reason the government's actions were unlawful, was because the government seized the defendant's non-responsive emails for an unreasonable period of time and therefore interfered with his possessory rights. The same improper seizure occurred here. The other significant difference, of course, is that the instant seizures, by virtue of the *Facebook* decision, do not implicate the Fourth Amendment.

Similar issues arose in *United States v. Metter*, 860 FSupp2d 205 (EDNY 2012 [Irizarry, J.]) a securities fraud overseizure case in which the Court suppressed computer files recovered from the Defendant's home and business as well as personal email messages which had been

obtained from his internet service providers.[19] Fifteen months after the initial seizure, the government had not yet completed its privilege review or determined whether any of the seized material fell outside the scope of the warrants. The Court concluded the government's 15 month delay in isolating responsive communications constituted a search and seizure in violation of the Fourth Amendment because of the unreasonable period of time the government had consumed searching the Defendant's files. The Court did not address the third-party doctrine, although part of the materials which were suppressed were email communications seized from ISP's. Thus, the Court apparently implicitly recognized that the third-party doctrine was not applicable to those seizures.

Courts have sanctioned searches of digital media for shorter periods, recognizing that a computer may not be practically examined during the time limit applicable to a warrant execution. Those decisions have implicitly recognized, however, the necessity for imposing some time limits on those searches. *See, e.g., United States v. Gorrell,* 360 F Supp 2d 48, n. 5. (D. DC 20004) (delay of ten months in obtaining data from seized computer and camera "lengthy" but does not warrant suppression); *United States v. Hernandez,* 183 F Supp 468 (D. Puerto Rico 2002) (6 week delay in searching computer discs reasonable).

In support of their position, the People cite three trial court decisions, primarily the decision of the Magistrate Judge in the case of *In Re A Warrant for Content and Other Information Associated with the Email Account xxxxxxxgmail.com Maintained at Premises Controlled by Google, Inc.*. 33 FSupp3d 386 (SDNY 2014 [Gorenstein, J.]) ("*Google"*). In *Google,* the Court declined to impose a time limit on the government's search of a subject's emails for responsive material at the time the search warrant was issued, holding that neither the Fourth Amendment nor any statute required search warrant protocols which proscribed the

19Defendant's counsel in the instant case also represented the Defendant in *Metter.*

government's conduct in executing an overseizure warrant in the first instance. The Court found, consistent with the People's position here, that:

> [T]he Government has a need to retain materials [obtained in an overseizure warrant] as an investigation unfolds for the purpose of retrieving material that is authorized by the warrant. For example, in a drug investigation, it might be obvious based on information from an informant or other source that emails referring to the purchase or importation of "dolls" refers to cocaine, but investigators might only learn as the investigation unfolds that a seemingly innocuous email referring to purchase "potatoes" also refers to a cocaine shipment. 33 FSupp3d at 398.

The Court noted that a suppression motion, an action for damages and other relief would be available if the government acted contrary to the Fourth Amendment. *Google*, however, considered the People's retention rights as of the date of a warrant issuance. It did not assess whether the seizure and retention of non-responsive emails for more than a four year period, as occurred here, would be reasonable. *See also, United States v. Carpenter, supra,* (government's retention of seized materials before trial reasonable); *United States v. Lee,* 2015 WL 5667102 (ND Georgia 2015 [Batten, J.]) (government's retention of seized files for more than three years reasonable).

The issues which arise in these cases are obviously varied and depend on what a warrant authorizes and the differing requirements of federal and state law. The basic threshold question regarding the government's retention rights in overseizure cases, however, in this Court's view is simple. When concededly non-responsive digital communications are obtained in an overseizure warrant to allow the government to conduct an effective search, can the non-responsive material be construed as being validly seized or is it only provided as an administrative convenience to allow the search for responsive material to occur?

If the answer is the former, then conclusions like those of the People here may follow. If the latter, non-responsive materials must be expunged or returned following the reasonable

period allotted for a search. In this Court's view, the answer is the latter for an obvious reason. When a search warrant is issued, the People cannot seize, under the warrant's authority, material which is not responsive to the warrant.

The People analogize their actions here to a case where they seize a gun under a search warrant, test the gun for fingerprints and then later, when new information suggests the possible presence of DNA on the gun, swab it for DNA. But that example is inapposite. The Defendant's non-responsive emails were never properly seized by the People. They were provided as an administrative convenience to allow an effective search. The proper analogy between the emails and the gun here are between the responsive emails and the gun. Once the People tagged emails as responsive during their initial search, they could subject those emails to additional analyses later if they chose to. They could not conduct a new database search to obtain new emails after the reasonable time allotted for the search to occur had expired.

To provide a more apt analogy, no one would suggest that a warrant to recover a gun in an apartment would allow the police to return to that same apartment 4 years later to search the apartment again under the same warrant upon learning that in addition to the gun, the police had also learned that bullets which could be used in the gun were in the apartment. An additional warrant would have to be issued. Of course, the privacy interests inherent in the search of a home are not equivalent to those in the search of an email account. But the basic principle is the same.

The People argue that the execution of the warrants was complete when the Defendant's email communications were provided by the ISP's, that is, shortly after January 4 and June 21, 2012. The warrants provided that they would be "deemed 'executed' when served upon the email provider".[20] Thus, the People argue, there is no issue with respect to whether the People

---

20Hotmail warrant, final sentence.

timely executed the warrants. But that argument, in this Court's view, is also plainly wrong. The "deemed executed" provision was intended to clarify that the requirement that the warrants be executed within 10 days (as provided by the warrants and the Criminal Procedure Law[21]) would be met upon service to the ISP's. It was not intended to authorize the People to retain non-responsive digital communications for a multi-year period.

The best analogy here is to a warrant authorizing the search of voluminous paper files and records. When a warrant is issued which authorizes a search of paper records, the government is entitled to search the files and seize responsive material. They are not permitted to search the files, seize responsive material and then retain files they have never identified as relevant for multiple years, because, at some later time, they might want to search the files again. A search warrant which authorizes a search of voluminous digital records is no different. As Defendant's counsel during an argument pointed out, overseizure is "a courtesy that was developed for law enforcement".[22] It is not a license for the government to retain tens of thousands of a defendant's non-relevant personal communications to review and study at their leisure for years on end.

The People argue that the intrusion which would be attendant to their continued retention of Thompson's files would be "minimal" because Thompson has copies of all of these materials. That is true with respect to the Defendant's access to his emails. But the Fourth Amendment protects our reasonable expectations of privacy. That is what would be lost by the People's continued retention of Thompson's personal, irrelevant files. The argument that the continued intrusion here would be minimal would apply equally to the seizure of the entirety of any person's digital communications by the government from an ISP for any reason – or no reason at

---

21CPL 690.30 (1).

22December 15, 2015 argument p. 25.

all.

The People raise a practical issue. They argue that requiring them to return the original communications seized from the ISP's might impair the authenticity of these materials and support an argument that they would be inadmissible at a trial. According to the People, "[t]his is because the 'hash values,' which are strings of characters described as 'digital fingerprints', are assigned to the digital records produced by the ISP's, and they are the best method of verifying that the data in the People's possession is identical to the data produced and is unaltered".[23]

While this is a legitimate point, the notion that it would support a viable argument that responsive communications would be inadmissible is both implausible and easily addressed. It is implausible because a court ordering a prosecutor to return seized communications would not then use the People's compliance with the Court's own order to find the People's retained evidence inadmissible. It is easily resolved by a suggestion the People make here (assuming the Court orders the return of any of the Defendant's emails). The solution is to provide the original of the seized communications to the Court, for the Court to retain as a sealed record. That way, if any questions about the authenticity of the emails arise in the future, the Court can authorize the use of the original seizure to resolve them.[24]

9. Blanket Suppression is Not Warranted

In this Court's view, therefore, the warrant executions were unlawful in two respects. First, the warrants were overbroad. Second, the People improperly retained the Defendant's non-responsive emails for an unreasonable time after their initial search was conducted. As this Court outlined *supra*, suppression is not an available remedy for the overbreadth issue. The

23People's Letter submission, p. 14-15.

24The *Ganias* court found the same argument unpersuasive for similar reasons. *See Ganias,* 755 F3d at 139.

third-party doctrine also forecloses any argument that all of the emails obtained by the People should be suppressed because the People improperly retained them. The argument for such "blanket suppression" is also based on the Fourth Amendment.

Even if the Fourth Amendment applied here, however, blanket suppression would not be appropriate. In order for such suppression to be granted, government agents must "flagrantly disregard" the terms of a warrant by effecting a "widespread seizure of items that were not within the scope of the warrant" and "not act in good faith". *United States v. Shi Yan Liu,* 239 F.3d 138, 140 (2d Cir 2000), *cert denied*, *Jie Hu v. United States*, 534 US 816 (2001). Those standards did not come close to being met here.

First, and unlike what occurred in *Metter*, the People have not failed to timely comply with any instruction given by this or the two different courts which issued the warrants. Second, the Court believes that the People sincerely believe in their legal arguments and are thus not acting in bad faith. Third, as the case law outlined *supra* indicates, there are at least three federal trial courts which have appeared to agree with the People's basic position here. Finally, while the overseizure issue has been the subject of multiple federal decisions, it is apparently a matter of first impression under New York law. The People here have not acted in "flagrant disregard" of any judicial mandate.

10. The People Must Return Thompson's Non-Responsive Communications

The Court does believe it appropriate, however, to order the People to return and expunge any material they seized from Thompson's accounts which they did not identify during their initial reviews as being responsive to the warrants. That order is not one granting suppression. It is an order which enforces the plain terms of the warrants and the Criminal Procedure Law.

Optimally, in this Court's view, when the People submit an overseizure warrant of this

magnitude involving 100,000 emails and 1.65 million pages they should present a search warrant protocol to the court, which outlines the search procedures the People intend to use and sets a reasonable time limit on their retention and search of the target's accounts. *See e.g., In the Matter of the Search of Cellular Telephones,* 2014 WL 7793690 (D. Kansas, 2014 [Waxse, Magistrate Judge]) (discussing the benefits of such search protocols). New York law does not require or even explicitly authorize such protocols. But they might help avoid the kind of practical problems which have arisen here. The goal, obviously, should be to establish clear rules in the first place, rather than rely on the costly remedy of suppression to sanction the People when they venture beyond an unsettled boundary. The best way to accomplish that would be legislation.

Here, had the People been granted the authority to take a box of the Defendant's files and search them for responsive papers, they would not be permitted to retain the non-responsive files when the search ended. If the People sought to do so, the Court would certainly be authorized to order the People to return the non-responsive property to its owner. That is what the Court is doing here.

With respect to responsive property seized during a search from a person "a police officer must write and subscribe a receipt itemizing the property taken and containing the name of the court by which the warrant was issued. If property is taken from a person, such receipt must be given to such person." CPL 690.50 (4). No different rule should apply here. Here, of course, the property was seized from ISP's and there is an argument that any receipt should be provided to the ISP's rather than the Defendant. *See People v. Lomma, supra,* (decision by this Court; 35 Misc3d at 403-404, discussing a bank customer's lack of standing to contest the seizure of his own banking records). It is obvious, however, that the ISP's likely do not care which emails the

People tagged as responsive and that Thompson has a vital interest in the question. The People have also already provided notice to Thompson of the emails they intend to use at the trial and thus have already provided a partial or full record of the emails they have determined are responsive. Under these circumstances, in this Court's view, it is reasonable that the receipts for the seized property the People have identified as responsive should be provided to Thompson. The People point out that under *Facebook*, the SCA is controlling here. But the SCA, as noted *supra,* explicitly contemplates that where a warrant is issued in a state court, it is subject to "State warrant procedures".[25]

There remain two questions: (i) how to fix criteria which separate communications lawfully seized by the People from those they had no right to retain, and (ii) how to establish precisely what, in practical terms, the People should be required to do. The Court has both discussed these issues on the record with the parties and considered their written submissions. There are no obvious answers. As the People correctly point out, "there are no commonly accepted procedures or protocols governing the length of the review, the manner of the review, or the length of the retention of email communications obtained pursuant to a warrant issued under the SCA."[26] Nor do any such procedures or protocols exist under New York State law.

With respect to the first question, a reasonable time cut-off which separates the period the People should have been given to search for responsive communications from the time communications not yet found to be responsive should have been returned would seem to the Court, although in one respect inherently arbitrary, to be the best way to draw a line which is both fair and not subject to conflicting interpretations. Creating criteria other than such a time certain cut-off (for example, a directive that the People return any communications they did not

---

2518 USCA § 2703 (a).

26People's Letter Submission, p. 7 (citation omitted).

initially tag as responsive) would seem both susceptible of differing interpretations and potentially prejudicial to the People. Drawing a line which would set a retroactive trap for the People and compromise the extraordinary volume of work they have done based on requirements no court has ever asked them to comply with before would also be manifestly unfair.

The Defendant argues that if blanket suppression is not ordered, the cut-off date should be in February of 2015. He asserts the People produced copies of all of the emails they intended to use at trial on February 6, 2015. The People assert, meanwhile, that their searches of the database concluded six months prior to that date, in September of 2014. The People have thus not even looked through the database for the past 1 ½ years. The Court hereby sets February 6, 2015 as the demarcation between emails the People will be permitted to retain, assuming they were specifically tagged or identified by the People prior to that date as being responsive to the warrants (hereinafter the "previously tagged responsive communications") and communications they have no right to retain. Emails not so previously and specifically identified shall be returned and expunged as described *infra.*

This date, in the Court's view, has a number of advantages. It follows by roughly six months the last date the People indicate they searched the database, thus allowing them to retain and use every communication they have ever tagged as being responsive. Since this date is also more than six months after the indictment, it will not impair the grand jury presentment. It allows the People to have retained and searched the seized communications for more than 2 ½ and 3 years (with respect to the two warrants), certainly a reasonable period. On the other hand, it provides the relief the Defendant is seeking (absent blanket suppression) on a date which will help create a clear record of the tagged communications because it was the date of the People's document production. It is important to recognize that the People not only had unfettered access

to all of Thompson's emails prior to this date. They also used them in support of a grand jury presentment of extraordinary depth, running to more than 2600 transcript pages and thousands of pages of exhibits. The People have thus apparently already applied great diligence to identify which of Thompson's 100,000 emails are responsive to the warrants .[27]

Turning to the second point, the People are hereby ordered to return to Mr. Thompson, as soon as reasonably practicable, copies of all the materials seized from the subject email accounts other than the previously tagged responsive communications. Those submissions may be made in digital form. The People shall also not retain any material previously seized pursuant to the subject warrants in any form other than the previously tagged responsive communications and shall expunge copies of any such returned material they possess. The People shall provide the Defendant with a listing of all of the previously tagged responsive communications, or, if the People choose, copies of the previously tagged responsive communications. In order to ensure that no unjustified authenticity issues arise from a return or destruction of the original seizure, the People may provide those originals to the Court to retain as a sealed record. *See* CPL 690.55.

By the phrase "as soon as reasonably practicable" the Court does not intend that attorneys or support staff from the district attorney's office pull "all nighters" or make herculean efforts to implement these directives in the shortest possible time. The Court recognizes that the People have legitimate concerns about how this order should be implemented. Since the Court previously issued an Interim Order directing the People to cease searching the Thompson database, moreover, the Court does not believe a brief delay in implementing this order will be prejudicial to the Defendant.

The Defendant finally asks that if the People gave third parties any of the materials the

---

27The Court is currently considering Defendants' motions to dismiss the indictment and for related relief. These comments are not intended to indicate any views on those motions.

Court is now ordering the People to return and expunge, the People obtain those materials from those third parties and destroy them. The Court directs the parties to confer about that issue and if it remains disputed contact the Court. The Court understands the Defendant's concerns but, assuming the People did provide any of these materials to third parties, it is not clear the People or the Court would be empowered to "claw them back", particularly if they were provided to a federal agency like the SEC.

The Court does not believe it is appropriate, initially, to micro manage the implementation of this order. Rather, the Court directs the parties to confer and attempt to agree on a procedure and time line for implementing it. In the event the parties are unable to do so they may contact the Court to arrange for a conference.

11. Conclusion

The issues here are both unique to this case and implicate the broader question of the degree to which reasonable expectations of privacy apply to electronic communications. This Court's analysis is informed by a number of precepts. It is unreasonable to condition the use of electronic media like email on the abdication of our Fourth Amendment rights. The fact that ISP's use digital communications for some purposes does mean we must surrender any constitutional claim that such content should ordinarily remain private. "Privacy is not a discrete commodity, possessed absolutely or not at all." *United States v. Jones, supra,* 132 S.Ct. at 957 [Sotomayor, J., concurring] (quotation omitted).

While the search of 100,000 emails is not the same as the search of a home, the particularity requirements of the Fourth Amendment, as the *Galpin* court argued, are even more necessary for digital communications. Computer records for most of us are the modern day equivalent of the "papers" whose indiscriminate search the founders so deeply abhorred. When

the government executes a search, it has no more right to retain non-responsive digital communications than a person's private paper files.

Much has been written through the ages about why privacy is such an enduring value. The right to be left alone, to possess an inviolate zone of not just privacy but secrecy in some aspects of our lives, particularly from the coercive power of the state, is not less precious today than it was 100 years ago. It is instead much more urgent because of the extraordinary ease with which modern technology in an instant can pierce the most private confines of our lives.

"In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical." *United States v. Jones, supra,* 132 S. Ct. at 963 [Alito, J., concurring]. Seizing the entirety of a person's written communications over a 4 ½ year period 100 years ago would require far more than the service of warrants on two companies. More to the point, 100 years ago, a person like Anthony Thompson would have likely conducted much of his business verbally and face-to-face, in forums where the government would be unable to retroactively capture his private communications no matter how much effort they expended. The fact that criminality can now be much more easily detected, of course, has made all of us immeasurably safer. But it has also exposed us to invasive scrutiny the founders could never have imagined. Drawing the proper boundaries between these competing imperatives in a rapidly changing information economy will require us to look to our fundamental values, rather than outdated legal rules, as our ultimate touchstone.

February 17, 2016

Daniel Conviser, A.J.S.C.