IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA, v. JARED WHEAT, JOHN BRANDON SCHOPP, and HI-TECH PHARMACEUTICALS, INC., Defendants.	No. 1:17-CR-0229-AT-CMS

JARED WHEAT AND HI-TECH PHARMACEUTICALS, INC.'S MOTION TO SUPPRESS EVIDENCE SEIZED PURSUANT TO THE SEARCH WARRANTS FOR EMAILS AND ELECTRONICALLY STORED INFORMATION AND MEMORANDUM OF LAW IN SUPPORT

COME NOW, Defendants Jared Wheat and Hi-Tech Pharmaceuticals, Inc. ("Hi-Tech"), by and through their undersigned counsel, and, pursuant to Fed. R. Crim. P. 41(h), file this Motion to Suppress Emails and Electronically Stored Information obtained as the result of two unlawful seizures and searches. In support of this motion, Defendants respectfully show this Court as follows:

I. INTRODUCTION

In 2013 and 2014, the Government obtained two search warrants for virtually every piece of information contained in or related to an AOL email account of Jared Wheat, the President and CEO of Hi-Tech, and a Yahoo email account of Choat Soviravong, a graphic design employee of Hi-Tech. The seizures pursuant to those two search warrants were recently revealed to Defendants in conjunction with their indictment in this case. The warrants were authorized on the basis of affidavits that failed to establish probable cause for the crimes alleged and relied on stale information. The resulting search warrants failed to state sufficiently particular categories of documents upon which the executing agents could rely and utterly failed to protect the Defendants' Sixth Amendment right to counsel. This litany of failures resulted in the Government seizing and reviewing tens of thousands of emails with little, if any, regard for the Defendants' right to privacy or right to the attorney-client privilege. The warrants are fundamentally insufficient to justify seizure and unfettered search of the email accounts of Hi-Tech personnel. Accordingly, Defendants respectfully request that the Court invalidate the warrants and suppress all evidence obtained in the searches. Furthermore, based on the violations of Mr. Wheat's attorney-client privilege, as set forth below, Defendants

respectfully submit that this Court should order a hearing into the Government's taint/privilege review process.

II. STATEMENT OF FACTS

A. Hi-Tech's Business

Hi-Tech is a manufacturer, distributor, wholesaler, and retailer of dietary supplement products. Hi-Tech manufactures and sells products under the Hi-Tech brand and several related brands. In total, Hi-Tech manufactures and sells approximately 215 different products under its brand or related brands. Thousands of retailers sell Hi-Tech Products, including major retail outlets such as GNC, Vitamin Shoppe, Kroger, Meijer Drugs, and Seven Eleven. *See* Doc. 36-5, Declaration of Michelle Harris, at ¶¶ 4-8. Hi-Tech also sells its products directly to consumers through various retail websites, with approximately 195 different products available through these websites. *Id*. at ¶ 6. Hi-Tech's business is subject to extensive regulation by the Food and Drug Administration ("FDA"). Declaration of Art Leach, attached to this motion as EXHIBIT A at ¶ 3.

B. Hi-Tech's History of Litigation With the Government

Since 2004, Hi-Tech and its President and CEO, Jared Wheat, have been involved in high profile, ongoing cases with the federal government in the U.S. District Court for the Northern District of Georgia related to Hi-Tech's

manufacturing and sale of certain dietary supplement products. *See, e.g., Federal Trade Commission v. National Urological Group, Inc., et al.*, 1:04-cv-3294 (N.D. Ga.) (related to labeling of certain weight loss supplements). Most pertinently, the FDA commenced a seizure action against Hi-Tech on November 5, 2013, seizing products and ingredients containing 1,3-dimethylamylamine HCL ("DMAA") at Hi-Tech's facilities. *See United States v. Undetermined quantities of... 1,3 dimethylamylamine*, No. 1:13-cv-3675 (N.D. Ga.). Contemporaneous with the FDA's seizure of Hi-Tech's products, Hi-Tech filed a complaint in the District Court for the District of Columbia that alleged the FDA had engaged in a campaign of intimidation against the dietary supplement industry. *See Hi-Tech Pharmaceuticals, Inc. v. Hamburg*, 1:13-cv-1747 (D.D.C.). None of these matters were sealed or otherwise unavailable to the Government.

C. The Instant Matter

On September 28, 2017, a federal grand jury in the Northern District of Georgia returned a First Superseding Indictment (hereinafter "indictment") against Hi-Tech, Jared Wheat, and John Brandon Schopp. Doc. 7. The eighteen-count indictment includes charges of conspiracy, wire fraud, money laundering, introduction of misbranded drugs, and manufacture and distribution of a controlled substance. *Id.* The indictment was unsealed on October 4, 2017. Doc. 15. The

Government revealed twelve days later, on October 16, 2017, that two search warrants had been issued and executed on email accounts of Hi-Tech personnel. EXHIBIT A at ¶ 8. The first was a May 17, 2013 warrant executed on AOL, LLC ("AOL") for the email account of Mr. Wheat (the "AOL warrant"). *Id.* at ¶ 5. The second was an October 23, 2014 warrant executed on Yahoo, Inc. ("Yahoo") for the email account of Choat Soviravong, a graphic designer employed by Hi-Tech (the "Yahoo warrant"). *Id.* at ¶ 6. Mr. Soviravong is not a defendant in the instant matter. Doc. 7 at 1.

1. The AOL Warrant

The first of the two warrants, the AOL warrant for the search of Mr. Wheat's email account, was authorized May 17, 2013. The search warrant, together with the application and affidavit of FDA-OIG Special Agent Brian Kriplean, is attached to this motion as EXHIBIT B.

The Kriplean affidavit sets forth the timeline of the FDA's investigation of Hi-Tech and its interest in the contents of Mr. Wheat's AOL account. The AOL warrant sought "any emails, records, files, logs, or information" available to AOL related to Mr. Wheat's email account, including: (i) the contents of all emails stored in the account; (ii) all records or other information regarding the identification of the account, including "full name, physical address, telephone

numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number)"; (iii) all records or information stored by the person using the account; and (iv) "all records pertaining to communications between AOL, LLC and any person regarding the account." EXHIBIT B, Attachment B at ¶¶ I. a-d. The Government further sought to seize all information "that constitutes fruits, evidence, and instrumentalities of false statements, mail fraud, wire fraud, and conspiracy to commit" any crime, including "[r]epresentations regarding audit reports, certifications (including GMP certifications), and any other representations concerning Hi-Tech's compliance with FDA rules and regulations"; and "[r]ecords relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts." *Id*. at ¶¶ II. a-b.

Agent Kriplean's affidavit supporting the application for the AOL warrant is based on information received from Sergio Oliveira, the former Director of Sales for Hi-Tech. According to the affidavit, Agent Kriplean met with Mr. Oliveira on

January 30, 2013. Three months later, in April 2013, Mr. Oliveira provided the agent with emails dated 2010 to 2012 purportedly related to alleged criminal activity by Hi-Tech. EXHIBIT B at ¶ 6. Agent Kriplean based his documentation of probable cause of the crimes on a handful of emails from the AOL account dated January 13, 2011, August 15, 2011, September 22, 2011, and October 14, 2011, and a press release document dated December 10, 2010. *Id.* at ¶¶ 7-15. Mr. Oliveria's account does not allege that the AOL email account was used to commit the crimes alleged in the indictment, nor does it state that Mr. Oliveira told the agent that the account was being used to commit the specific federal crimes alleged in the affidavit. *Id*. at ¶ 4. Nevertheless, the AOL warrant was authorized on May 17, 2013.

2. The Yahoo Warrant

The second search warrant was authorized seventeen months later, on October 24, 2013, and was for the Yahoo email account of Hi-Tech employee Choat Soviravong. A copy of the warrant, together with the application and affidavit of Special Agent Jacqueline Reynolds of the Internal Revenue Service Criminal Investigation Division, is attached to this motion as EXHIBIT C. The affidavit represented that there was probable cause to believe that the Yahoo email account contained evidence of mail fraud, wire fraud, false statements, and

conspiracy. *Id.* at ¶ 4. The Reynolds affidavit refers to the AOL warrant to support its assertion of probable cause to search the Yahoo email account. *Id*. at ¶ 7. In support of a finding of probable cause, the affidavit briefly recited the contents of three emails not detailed in the AOL warrant: emails dated March 3, 2011, March 15, 2011, and March 28, 2011. *Id*. at ¶¶ 8-10.

There is no statement in the affidavit that the Yahoo email account was used to commit the federal offenses specified in the Yahoo warrant. According to her affidavit, Agent Reynolds interviewed Mr. Soviravong, the owner of the Yahoo account, in June 2014. Not only did Mr. Soviravong deny committing the crimes alleged in the Yahoo warrant, he confirmed that his use of the Yahoo email account was limited to his legal business activities as an employee of Hi-Tech. *Id.* at ¶ 14. Moreover, the only paragraphs of the affidavit that alleged specific criminal activity related to two allegedly falsified GMP certificates. They do not link the alleged criminal activity back to the Yahoo email account. *Id*. at ¶¶ 10-12. The Government nonetheless sought the same information requested by the AOL warrant, including audit reports, GMP certificates, and any communications, representations, or documents concerning Hi-Tech's compliance with FDA rules and regulations. *Id.* at Attachment B, ¶¶ II. a-b.

Based on those two search warrants, upon Defendants' information and belief, the Government seized the *entire contents* of the AOL and Yahoo accounts identified in the warrants.

On October 26, 2017, the Government delivered its criminal discovery to Defendants, including the materials it had retrieved from AOL and Yahoo pursuant to the Warrants. EXHIBIT A at ¶ 8. Counsel for Hi-Tech discovered at that time that the Government had received, and apparently reviewed, thousands of emails and documents that were subject to the attorney-client communication privilege and attorney work product privilege. *Id*. at ¶ 9. Such documents include communications with Hi-Tech's counsel, attorney work product, and law firm invoices. *Id*. Much of this material was plainly marked "Attorney-Client Privileged." *Id*. at ¶ 10. The Government has noted in passing that it intends to use a "taint team" to review the seized materials for privileged documents and communications, but has not provided Hi-Tech with a corresponding protocol nor, upon information and belief, submitted such a protocol for approval to the Court. *Id*. at ¶ 11. Needless to say, such protocols are of little value if the material has been reviewed and utilized by the agents who have had the material for years.

III. ARGUMENT

A. The AOL and Yahoo Search Warrants Were Not Supported by Probable Cause and All Evidence Obtained Thereby Should Be Suppressed.

1. Fourth Amendment Requirements

The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, *but upon probable cause*, supported by Oath or affirmation, *and particularly describing the place to be searched, and the persons or things to be seized*." U.S. Const. Amend. IV (emphasis added); *see also United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013). The purpose of the Fourth Amendment warrant clause is to ensure that "those searches deemed necessary should be as limited as possible." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

"[T]he specific evil" in this case "is the 'general warrant' abhorred by the colonists, and the problem is not the intrusion *per se*, but of a general, exploratory rummaging in a person's belongings." *Id.*; *see also United States v. Blake*, 868 F.3d 960, 973 (11th Cir. 2017); *Galpin*, 720 F.3d at 446 ("'[T]he central concern underlying the Fourth Amendment [is] the concern about giving police officers unbridled discretion to rummage at will among a person's private effects.'") (citing

Arizona v. Gant, 556 U.S. 332, 345 (2009)). The Constitution limits law enforcement's rights to search only "the specific areas and things for which there is probable cause to search," which requires that "that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

The Government's warrants to perform unrestricted searches of the AOL and Yahoo accounts of Hi-Tech personnel were stale, overbroad, and insufficiently particularized. Moreover, they did not provide the required nexus between the stated facts and the alleged violations of federal law. Accordingly, the Warrants violated the Fourth Amendment, and the evidence seized pursuant to both warrants should be suppressed.

2. The Information Underlying the Warrants Was Stale.

In determining whether probable cause exists, the magistrate judge is required to assess whether the information set out in the application appears to be current, *i.e.*, true at the time of the application, or whether it instead has become stale. *United States v. Harris*, 20 F.3d 445, 450 (11th Cir. 1994) ("For probable cause to exist, however, the information supporting of the government's application for a search warrant must be timely, for probable cause must exist

when the magistrate judge issues the search warrant."); *accord United States v. Reyes*, 922 F. Supp. 818, 826 (E.D.N.Y. 1996) (same). To establish probable cause, the Government must show that it is "likely that the items being sought are in that place when the warrant issues." *Harris*, 20 F.3d at 450. "Warrant applications based upon stale information fail to create a probable cause that similar or other improper conduct is continuing." *Id*.; *see also United States v. Bascaro*, 742 F.2d 1335, 1345 (11th Cir. 1984); *United States v. Latimore*, 2014 U.S. Dist. LEXIS 91777, at *90 (N.D. Ga. May 29, 2014) ("[I]t is manifest that the proof must be of facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time.") (citing *Sgro v. United States*, 287 U.S. 206, 210 (1932)).

"There is no mathematical measure for when freshness fades away and staleness sets in." *United States v. Lopez*, 649 F.3d 1222, 1246 (11th Cir. 2011). While there is no bright line rule for staleness, the facts in an affidavit supporting a search warrant must be sufficiently close in time to the issuance of the warrant and execution of the subsequent search so that probable cause can be said to exist as of the time of the search and not simply as of some time in the past. *United States v. Wagner*, 989 F.2d 69, 75 (2d. Cir. 1990) (finding evidence that a defendant was a member of a drug conspiracy was stale when warrant certified a single drug

purchase six weeks prior to the search); *United States v. Harmon*, 2006 U.S. Dist. LEXIS 95196, at *40-41 (E.D. Tenn. Apr. 12, 2006) (finding search warrant partially invalid because it was based on activities that occurred nearly three years prior to the warrant's issuance); *Reyes*, 922 F. Supp. at 826 (information supporting a finding of probable cause should be no older than one year); *United States v. Murray*, 2014 U.S. Dist. LEXIS 77341, at *17 (N.D. Ga. Apr. 14, 2014) (affidavit in support of search warrant detailing investigation a year prior to search warrant's issuance would render warrant stale).

Staleness pervades both of the warrant applications at issue here. Not one factual statement ties the AOL or Yahoo accounts to an allegation of a crime that is "so closely related" to the time of the warrant issuance that a finding of probable cause is justified. *Latimore*, 2014 U.S. Dist. LEXIS 91777 at *90. The most recent information specifically tied to the AOL account is dated October 2011, *eighteen months* prior to the issuance of the AOL warrant. EXHIBIT B at ¶ 10. Notwithstanding the fact that Mr. Oliveira apparently provided Hi-Tech emails to the FDA that were dated during 2012, Agent Kriplean's affidavit did not cite to a single specific instance of an email linked to the AOL account in that year. *Id.* at ¶¶ 6-15. The affidavit for the Yahoo warrant, which piggybacks its probable cause finding on the AOL warrant, is equally based on stale information that cannot

support seizure or search of the email accounts. Indeed, the staleness of the Yahoo warrant is even more egregious than that of its counterpart; the emails cited to support a finding of probable cause in the Yahoo warrant are temporally separated from the date the warrant was issued by *three years*. EXHIBIT C at ¶ 8-10. An eighteen-month window between the last instance of an alleged crime and the issuance of the warrant renders the warrant stale – a three-year window is indisputably stale.

Importantly, the affidavits do not allege that the crimes here are pervasive, long-running, or protracted. *United States v. Bascaro*, 742 F.2d 1335, 1346 (11th Cir. 1984) (the "protracted and continuous activity" that is "inherent in large-scale drug trafficking operations" may warrant a more liberal interpretation of the staleness rule). Nor do they provide any corroborating evidence to update or refresh the information in the affidavits. The Government did not state any proof that the alleged crime was still ongoing at the time they executed the warrants, nor that the emails would even still exist at the time of execution. EXHIBIT B at ¶¶ 5-15; EXHIBIT C at ¶¶ 5-14. The connection between the facts alleged – a handful of emails dated during 2011 – and the execution of the warrants in May 2013 and October 2014 is simply too attenuated to support probable cause.

To be sufficiently fresh, the affidavits should have recited some information that tied the alleged crimes to the warrants "at the time of the search." *Harris*, 20 F.3d at 450. The affidavits fail as to this, and therefore the search warrants based upon them are invalid. Accordingly, all evidence derived therefrom should be suppressed.

3. The Warrants Are Unconstitutionally Overbroad.

"[A] warrant is overbroad if its 'description of the objects to be seized . . . is broader than can be justified by the probable cause upon which the warrant is based.'" *United States v. Lustyik*, 57 F. Supp. 3d 213, 228 (S.D.N.Y. 2014) (quoting *Galpin*, 720 F.3d at 446). Warrants must "specify the items to be seized by their relation to designated crimes." *United States v. Wey*, 2017 U.S. Dist. LEXIS 91138 at *60-61 (S.D.N.Y. June 13, 2017) (citing *United States v. Buck*, 813 F.2d 588, 590-92 (2d Cir. 1987) (warrant authorizing seizure of "any papers, things or property of any kind relating to [the] previously described crime" was overbroad)).

Nor does a conclusory reference to a broad set of federal statutes create a narrowness sufficient to ward off concerns of overbreadth. *United States v. Leary*, 846 F.2d 592, 601 (10th Cir. 1988). Courts have held that "even warrants that identify catchall statutory provisions, like the mail fraud or conspiracy statutes,

may fail to comply" with the particularization requirement. *Galpin*, 720 F.3d at 445 n. 5; *see, e.g.*, *Leary*, 846 F.2d at 594 (warrant authorizing search of export company's business records for violation of the "Arms Export Control Act, 22 U.S.C. § 2778, and the Export Administration Act of 1979, 50 U.S.C. App. § 2410," held overbroad)); *Voss v. Bergsgaard*, 774 F.2d 402 (10th Cir.1985) (warrant specifying 18 U.S.C. § 371 held overbroad and warrants invalidated); *United States v. Roche*, 614 F.2d 6, 8 (1st Cir.1980) (a limitation of a search to evidence relating to 18 U.S.C. § 1341, the general mail fraud statute, provides "no limitation at all").

A facially deficient warrant may not be cured by information laid out in the accompanying application. *See Groh v. Ramirez*, 540 U.S. 551, 557 (2004) ("[t]he fact that the application adequately described the things to be seized does not save the warrant from its facial invalidity" because the Fourth Amendment "by its terms requires particularity in the warrant"). Despite the allegations of specific statutory violations set forth in the affidavits, the AOL and Yahoo warrants are facially overbroad.

Here, the affidavits and the ensuing warrants provide almost no limitation on the crimes at issue. Both the AOL and the Yahoo warrant applications name only various catch-all federal crimes: "Title 18, United States Code, Sections 1341 (*mail*

fraud), 1343 (*wire fraud*), 1001 (false statements), and 371 (conspiracy)." EXHIBIT B at ¶ 4; EXHIBIT C at ¶ 4. The seizure of an *email account* for evidence of mail fraud could, arguably, encompass every single item and piece of electronic information contained in or related to that account. Based on the crimes stated on the face of the warrants, the agent executing the warrants would not have any basis for eliminating any document related to the AOL or Yahoo email accounts. The warrants are, accordingly, facially overbroad and invalid.

Further, a warrant that identifies "generic" or "catch-all" categories of items subject to seizure without any linkage to the suspected criminal activities may be invalidated for overbreadth. *Wey*, 2017 U.S. Dist. LEXIS 91138 at *72-73 (S.D.N.Y. June 13, 2017). The type of property that is "generally in lawful use in substantial quantities" requires "greater care in its description" in a warrant. *Id*. at *73. Specifically, where warrants authorize "virtually a wholesale search and seizure of the business records of the" business, the warrants are "constitutionally infirm" and must be invalidated. *Klitzman, Klitzman & Gallagher v. Krut*, 744 F.2d 955, 960 (3d Cir. 1984) (invalidating warrants executed on a law firm that "allowed the seizure of all" business records "without regard to whether the materials had any connection to particular alleged crimes").

Attachment B as to both warrant applications states the documents and information to be seized include "…any other communications, representations, or documents concerning Hi-Tech's compliance with FDA rules and regulations." EXHIBIT B at ¶¶ I. a-d & II. a-b; EXHIBIT C at ¶¶ I. a-d & II. a-b. This overbroad catch-all tacked onto the end of the applications opens the door for the Government to seize nearly all records of Hi-Tech's business, regardless of whether they are related to the criminal activity alleged in the warrants. The statements of probable cause set out in the affidavits relate specifically to GMP certification and GMP audits, *but not* broader issues related to FDA regulation or enforcement. There is absolutely no nexus between the purportedly illegal activity alleged in the affidavits and this nearly-unlimited category of documents. Moreover, it is the entire business of Hi-Tech, a dietary supplement manufacturer that markets over 200 products at thousands of locations, to ensure that it is continually "complian[t] with FDA rules and regulations."

In theory, the result of the execution of the warrants with this overbroad, catch-all category of documents is that agents, in searching for any communications, representations, or documents concerning "Hi-Tech's compliance with FDA rules and regulations" could conceivably seize any and all emails in the AOL and Yahoo accounts. In practice, that is exactly what happened. Such

overbreadth permitted the federal agents to rummage through all of Hi-Tech's day-to-day operations in the possession of AOL and Yahoo and, upon information and belief, the Government seized the entirety of Mr. Wheat's AOL account – his working email for the entire Hi-Tech business, including voluminous attorney-client privileged materials. EXHIBIT A at ¶ 7.

4. The Warrants Fail to Describe Materials to Be Seized With Particularity.

The AOL and Yahoo warrants wholly fail to describe with particularity the items to be seized. Instead, the warrants seek every conceivable record that could exist in the email accounts, with nearly no limitation by, *e.g.*, subject matter, type of activity, date range or otherwise. EXHIBIT B at ¶¶ I. a-d; EXHIBIT C at ¶¶ I. a-d. The executing agents were thus impermissibly left entirely to their own discretion to determine what to seize. Unsurprisingly under such conditions, they apparently seized virtually everything in the AOL and Yahoo accounts related to — and not related to – Hi-Tech. These warrants cannot be described as anything but impermissible "all documents" warrants, and the Government's searches thus violated the Defendants' fundamental rights.

a. Fourth Amendment Test for Particularity

The manifest purpose of the Fourth Amendment particularity requirement is to prevent the Framers' chief evil: general searches. A general search "le[aves] to

the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched . . . [and] provide[s] no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular [place].” *Steagald v. United States*, 451 U.S. 204, 220 (1981) (citing *Stanford v. Texas*, 379 U.S. 476, 481-85 (1965)). The main purpose of the particularity requirement is to ensure that the search will be carefully tailored to its justifications and that it will not take on the “character of the wide-ranging exploratory searches the Framers intended to prohibit.” *Nathan v. Lawton*, 1989 U.S. Dist. LEXIS 1398, at *21 (S.D. Ga. Jan. 18, 1989) (citing *Maryland v. Garrison*, 480 U.S. at 87)).

The test for particularity is a practical one: “[a] description is sufficiently particular when it enables the searcher to reasonably ascertain and identify the things authorized to be seized.” *United States v. Leary*, 846 F.2d 592, 600 (10th Cir. 1988) (quoting *United States v. Wuagneux*, 683 F.2d 1343, 1348 (11th Cir.1982)). A search conducted pursuant to a warrant that fails to conform to the particularity requirement will be held unconstitutional. *Nathan v. Lawton*, 1989 U.S. Dist. LEXIS 1398, at *21 (citing *Massachusetts v. Sheppard*, 468 U.S. 981, 988 n.5 (1984)); *see also United States v. Fuccillo*, 808 F.2d 173, 176 (1st Cir. 2015) (“warrants are conclusively invalidated by their substantial failure to specify

as nearly as possible the distinguishing characteristics of the goods to be seized").

b. Failure to State Time Frames of Criminal Activity With Particularity

A failure to state a temporal limitation on the documents to be seized can create a constitutional deficiency in the warrant. Here, despite the underlying affidavit citing to emails from specific dates, there was no temporal limit set forth in the warrants. If, as here, the underlying affidavit provides specific dates of the alleged criminal activity, a warrant may still be invalidated if the *warrant itself* does not "limit the items subject to seizure by reference to any relevant time frame or dates of interest." *Wey* at *77; *see also, e.g.*, *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (warrant "not sufficiently particular" in part because the "government did not limit the scope of the seizure to a time frame within which the suspected criminal activity took place"); *United States v. Abrams*, 615 F.2d 541, 545 (1st Cir. 1980) (deeming warrant insufficiently particularized and noting, among other things, that "[a] time frame should also have been incorporated into the warrant"). Failure to limit the search warrant temporally leaves the warrant open to challenge. *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017) ("[W]arrants should have requested data only from the period of time during which Moore was suspected of taking part in the prostitution conspiracy…. That procedure would have undermined any claim that the Facebook warrants were the

internet-era version of a 'general warrant.'")

c. Particularity in the Context of Electronic Data

The principles set forth above are equally applicable to search warrants for the seizure of electronic data. *See, e.g., In re Search of premises known as: Three Hotmail Email accounts*, 2016 U.S. Dist. LEXIS 40545 (D. Kan. Mar. 28, 2016) (denying application for search warrants for email accounts and all associated [electronically stored information] due to failure to state particularity); *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017) (lack of temporal limitation on search warrants for Facebook accounts created "unnecessar[y]" intrusion); *Wey*, 2017 U.S. Dist. LEXIS 91138 (invalidating warrants for email accounts when the warrants lacked any temporal limitation on the emails to be seized). The Government's lack of particularity in a search of electronic media can grant the searcher a virtually unlimited look into every aspect of an individual's life. *Riley v. California*, 573 U.S.__, 134 S. Ct. 2473, 2489 (2014) ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions . . . ."); *see also In re Search of premises known as: Three Hotmail Email accounts*, 2016 U.S. Dist. LEXIS 40545 at *22-23 ("[I]ndividuals have a right to privacy with respect to email"… accordingly, the Court "continues to disagree with cases that find [temporally unlimited warrants]

were not overly broad in their authorization for the Email Provider to disclose—without limitation or any concern for the privacy rights of the account holder or any person communicating with that account—all ESI in or associated with the target email account."). Indeed, the Eleventh Circuit has recently noted that it is "troubling" when searches of email accounts "d[o] not limit the emails sought to emails sent or received within the time of [the suspect's] suspected participation in the [crime]." *Blake*, 868 F.3d at 973 n.7. Heightened sensitivity to the particularity requirement in the context of electronic searches is therefore required. *Galpin*, 720 F.3d at 447 (quoting *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam)) ("There is, thus, 'a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.'").

Here, the warrants fail to specify sufficiently the records to be identified and seized, both in terms of the subject matter or any temporal limitation on the records sought. Although the warrants ostensibly limit the documents to be seized by providing suggested categories of documents and information, the warrants are not truly limited in scope. Instead, the broad categorical language authorized agents to seize nearly all of Hi-Tech's records *and Mr. Wheat and Mr. Soviravong's personal correspondence and documents* in possession of AOL or Yahoo.

Based on our preliminary review of the Rule 16 discovery provided by the Government, there is no indication that the Government limited its seizure or search in any respect, including by subject matter, type of activity, date range, or otherwise. EXHIBIT B, Attachment B at ¶¶ I. a-d; EXHIBIT C, Attachment B at ¶¶ I. a-d. The lack of particularity in the warrants effectively opened the gate for the Government to acquire unlimited access to the day-to-day operations of Hi-Tech in the possession of AOL and Yahoo. Upon information and belief, the Government seized the entirety of Mr. Wheat's AOL account – his working email for the entire Hi-Tech business. *Id.* at ¶ 27. Similarly, the Government requested the entire Yahoo account of Mr. Soviravong, which was used, in part, "to conduct business activities for Hi-Tech." EXHIBIT C at ¶ 26. The warrants, driven by the Government's over-reaching, became impermissible "general warrants." The remedy is suppression of all fruits of the overbroad and insufficiently particularized warrants.

5. The Warrants Do Not State a Sufficient Nexus Between the Underlying Factual Information and the Alleged Crimes.

A finding of probable cause must be based upon facts sufficient to create a nexus between the information in the warrant and the alleged federal crime. *See United States v. Blocker*, 2016 U.S. Dist. LEXIS 77280 at *15-16 (N.D. Ga. Feb. 29, 2016) (citing *United States v. Miller*, 24 F.3d 1357, 1360 (11th Cir. 1994))

("The federal search warrant affidavit must set forth facts upon which the issuing judge can find probable cause that a federal crime is involved."); *see also United States v. Brouillette*, 478 F.2d 1171 (5th Cir. 1973) (finding that failure to provide facts showing why a federal statute was violated rendered warrant invalid). Facts must be on the record before the magistrate judge and may not be inferred. *See Thomas v. United States*, 376 F.2d 564 (5th Cir. 1967) (warrant for gun deemed invalid when no information in warrant that gun was illegally possessed under federal law). Lacking this nexus, a warrant is deficient and the fruits of the search should be suppressed. *Id*.

The affidavit underlying the Yahoo warrant fails to state a sufficient nexus between the facts alleged and any federal crime. Paragraphs 5 through 25 of the Yahoo affidavit are set out as support for probable cause for seizing and searching the Yahoo account. EXHIBIT C at ¶¶ 5-25. Two paragraphs generally introduce Hi-Tech and its business. *Id.* at 5-6. One paragraph relates the prior warrant for the AOL account. *Id*. at ¶ 7. The next five paragraphs describe emails seized in the AOL warrant which describe the Government's assertion of criminal activity related to three allegedly falsified GMP certificates, but, significantly, do not link the allegedly criminal behavior back to the Yahoo email account. *Id*. at ¶¶ 8-12. The remaining two paragraphs, which do, at least, reference the Yahoo account, do

not even allege that any federal crime occurred related to the Yahoo account – only that the Yahoo account corresponded with the AOL account about GMP audits. *Id.* at ¶¶ 13-14. The affidavit even goes on to confirm, based on an interview with the owner of the Yahoo account, that the account was used for the day-to-day business of the operations of Hi-Tech, but that the account owner denied any involvement with preparation of GMP certificates or audit reports *Id*. at ¶ 14. The remaining paragraphs deal with the logistics of email accounts and the provider's retention of records. *Id.* at ¶¶ 15-25.

The required nexus between facts stated in a warrant and the alleged crime must be present in order for a warrant to be valid. *Miller*, 24 F.3d at 1359. Not a single fact stated in the Yahoo affidavit tends to show that this Yahoo email account was used to commit a federal crime. Accordingly, the Yahoo warrant should be invalidated and the fruits of the search should be suppressed.

B. The Government's Execution of the Search Warrants Was Reckless and Resulted in the Review of Privileged Information by the Investigatory Teams

The Government, despite the publicly available knowledge that Hi-Tech and its sole owner, Jared Wheat, were involved in ongoing, high profile litigation with federal government agencies at the time of issuance of both warrants, entirely failed to create a mechanism that would protect and preserve the attorney-client

privilege and attorney work product privilege during its search of the AOL and Yahoo email accounts. This reckless disregard for the privileges led the Government to obtain and review voluminous privileged documents and communications. Accordingly, the fruits of the searches should be suppressed and Defendants request a hearing on the Government's taint/privilege review process.[1]

1. The Government Egregiously and Unjustifiably Invaded the Attorney-Client Privilege.

The attorney-client privilege is the "oldest of the privileges for confidential communications known to the common law." *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981). Documents reflecting attorney-client communications are entitled to special protection under the Fourth Amendment because of the "intrinsic high expectation of privacy" such documents enjoy. *United States v. Skeddle*, 989 F. Supp. 890, 894 (N.D. Ohio 1997) (quoting *OKC Corp. v. Williams*, 461 F. Supp. 540, 542 (N.D. Tex. 1978)). Documents within the scope of the attorney-client privilege are "zealously protected." 8 C. Wright & A. Miller, *Federal Practice and Procedure* § 2017 (1970); *see Chore-Time Equipment, Inc. v. Big Dutchman, Inc.*, 255 F. Supp. 1020, 1021 (W.D. Mich. 1966) ("It generally is acknowledged that

[1] Defendants reserve the right to move to disqualify the Government's trial team if information is developed that they reviewed Defendants' privileged materials.

the attorney-client privilege is so sacred and so compellingly important that the courts must, within their limits, guard it jealously.").

A "purposeful intrusion" into the attorney-client relationship creates a presumption that there has been a "prejudicial effect on the reliability" of the litigation process. *Shillinger v. Haworth*, 70 F.3d 1132, 1142 (10th Cir. 1995); *see also United States v. Orman*, 417 F. Supp. 1126, 1133 (D. Colo. 1976) (holding that when a party accesses attorney-client protected documents, a "strong presumption" exists that the review of the protected information "causes incurable prejudice"). Such a presumption is justified because "no other standard can adequately deter this sort of misconduct," and "prejudice in these circumstances is so likely that case-by-case inquiry into prejudice is not worth the cost." *Shillinger* at 1142. In fact, a defendant "need not prove that the prosecution actually used the information obtained" in order to establish a constitutional violation. *Briggs v. Goodwin*, 698 F.2d 486, 494 (D.C. Cir. 1983), *vacated on other grounds*, 712 F.2d 1444 (D.C. Cir. 1983).

After its seizure of virtually every electronic document in Jared Wheat's AOL email account, the Government apparently took the opportunity to have an unmonitored rummage through the tens of thousands of emails seized, without any

regard for the privileged nature of the documents.[2] This demonstrates reckless disregard for, if not a blatant violation of, the Sixth Amendment.

At the time of the seizures, there could have been no doubt in the minds of the Government agents that the accounts – unrestricted by search terms or other limiters – would contain privileged communications. Hi-Tech has been involved in several high-profile, ongoing lawsuits with the Government since 2004. In particular, a 2013 seizure action initiated by the FDA dealt with strikingly similar documents and information sought by the Government in the instant matter. *See United States v. Undetermined quantities of... 1,3 DMAA*, Civil Action No. 1:13-cv-3675 (N.D. Ga.) (combined Administrative Procedure Act and seizure action related to the FDA's detention of DMAA products at Hi-Tech facilities). The Government cannot reasonably claim that it was unaware of the parallel civil

[2] "In order to avoid impinging on valid attorney-client relationships, prosecutors are expected to take the least intrusive approach consistent with vigorous and effective law enforcement" when potentially privileged evidence is sought. United States Attorney's Manual, § 9-13.420 (noting that this policy applies to "searches of business organizations where such searches involve materials in the possession of individuals serving in the capacity of legal advisor to the organization"). It is clear that, four years after the issuance of the AOL warrant and three years after the Yahoo warrant, the "least intrusive approach" has not been implemented by the Government.

proceedings being litigated in the same district as the warrants were issued,[3] nor plead ignorance that that the seized email accounts likely had a litany of attorney-client privileged emails.

The Government's blatant intrusion into privileged material here is not a hypothetical or abstract concern on the part of Hi-Tech. The Government has noted in passing that it *intends* to use a "taint team" to review the seized materials for privileged documents and communications, but has not provided Hi-Tech with a corresponding protocol nor, to Defendants' knowledge, submitted such a protocol for approval to the Court. EXHIBIT A at ¶ 11. Moreover, the Government's Rule 16 discovery production in this matter contains voluminous privileged attorney-client documents, including email communications with counsel, legal memoranda, and legal bills. *Id*. at ¶ 10. It is clear that the Government took the opportunity to "purposeful[ly] intru[de]" on Hi-Tech and Mr. Wheat's attorney-client

[3] Any claim to the contrary is not only absurd but contrary to established Department of Justice procedure. The United States Attorney's Manual prescribes that, during parallel proceedings, "criminal prosecutors and civil trial counsel should timely communicate, coordinate, and cooperate with one another and agency attorneys to the fullest extent appropriate to the case and permissible by law." U.S. Attorneys' Manual, Organization and Functions Manual, § 27 - Coordination of Parallel Criminal, Civil, Regulatory, and Administrative Proceedings.

relationships. The only reasonable conclusion is that the Government acted with open disregard for the "sacred" privilege.

2. The Appropriate Remedy for the Unconstitutional Intrusion Is to Invalidate the Search Warrants.

The appropriate remedy for such a wanton, pervasive intrusion into the privilege by the Government is invalidation of the warrants. *Klitzman,* 744 F.2d at 960-62 (seizure of privileged documents caused irreparable harm to defendants and warrants ordered invalidated as a result). Egregious behavior on the part of the Government without consequence erodes the public trust in the judicial system:

> When a public official behaves with such casual disregard for his constitutional obligations and the rights of the accused, it erodes the public's trust in our justice system, and chips away at the foundational premises of the rule of law. When such transgressions are acknowledged yet forgiven by the courts, we endorse and invite their repetition.

United States v. Olsen, 737 F.3d 625, 632 (9th Cir. 2013) (Kozinski, C.J., dissenting from denial of rehearing *en banc*).

Intentional intrusion into the attorney-client relationship by the prosecution is "especially troubling." *United States v. Pedersen,* 2014 U.S. Dist. LEXIS 106227 at *82 (D. Ore. Aug. 4, 2014) (where prosecutors and members of the government filter team intentionally intercepted defendant's legal mail and other legal communications, judge found several deficiencies in prosecutors' actions and

protocols). Such a *laissez-faire* approach to protect Defendants' Sixth Amendment Rights should not benefit the Government.

3. Defendants Request a Hearing on the Government's Taint/Privilege Review Process.

Due to the "sacred" nature of the privilege, and the severe consequences that result if the privilege is intentionally breached, the Department of Justice recommends that, when agents seize electronic information or storage that contains legally privileged files, "a trustworthy third party must examine the [storage] to determine which files contain privileged material." *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Office of Legal Education Executive Office for United States Attorneys, p. 109 ("Electronic Crimes Manual")[4].Based on the thousands of documents released to Defendants as part of the Government's Rule 16 discovery materials, it is clear that this recommendation has not been followed.

The Government has noted in passing that it intends to use a "taint team" to review the seized materials for privileged documents and communications. EXHIBIT A at ¶ 11. Use of a taint team is not without its issues; courts have

[4] Available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

expressed concerns about the use of "taint teams" to review seized materials. *See, e.g., United States v. Neill*, 952 F. Supp.834 (D.D.C. 1997). A Government taint team's review of potentially privileged documents is, still, an intentional intrusion into the privilege. *Neill*, 952 F. Supp. at 840 (appeal from evidentiary hearing holding that the government "intentionally invaded the attorney-client privilege" when it reviewed materials it knew were protected but set up a "taint team" to review them). There is a presumption that privileged information will be passed to the prosecution team. *Id.* at 841. The Government bears the burden to rebut the presumption that tainted material was disclosed. *Id.*

The Government has provided no further details to Hi-Tech about the composition of taint team or its review to date – neither the makeup of the team[5] nor the process for ensuring that the Defendants' "sacred" privilege is maintained. EXHIBIT A at ¶ 11. The best course of action to protect the privilege is to allow the defense team an opportunity to object before the Government reviews *any* material obtained via the warrants. Accordingly, Defendants request that the Court

[5] Courts have held that it is inappropriate to assign the task of reviewing and segregating potentially privileged information to non-attorney government personnel. *See In re Fattah*, 802 F.3d 516, 530 (3d Cir. 2015) ("Because of the legal nature of the privilege issues involved, we agree that the first level of privilege review should be conducted by an independent DOJ attorney acceptable to the District Court," not a non-attorney agent).

hold a hearing on the Government's taint/privilege review process to ensure that proper procedures were, and continue to be, utilized to segregate and return privileged information, and confirm that no privileged documents have slipped through the cracks to the prosecution team.

CONCLUSION

The AOL and Yahoo warrants must be invalidated because they violate Mr. Wheat and Hi-Tech's constitutional rights.

WHEREFORE, Defendants respectfully pray that this Court enter an Order invalidating both the AOL and the Yahoo search warrants, suppressing the fruits of the searches and seizures conducted pursuant to those warrants, and for such other and further relief as this Court may deem just and proper.

This 10th day of November 2017.

Respectfully submitted,

/s/ Bruce H. Morris
Bruce H. Morris
Georgia Bar No. 523575
Finestone Morris & White
340 Peachtree Road NE
2540 Tower Place
Atlanta, Georgia 30326
404-262-2500
BMorris@FMattorneys.com
Counsel for Defendant
Jared Wheat

/s/ Arthur W. Leach
Arthur W. Leach
Georgia Bar No. 442025
The Law Office of Arthur W. Leach
5780 Windward Parkway, Suite 225
Alpharetta, Georgia 30005
404-786-6443
Art@ArthurWLeach.com
Counsel for Defendant
Hi-Tech Pharmaceuticals, Inc.

/s/ James K. Jenkins
James K. Jenkins
Georgia Bar No. 390650
Maloy Jenkins Parker
1506 Brandt Court
Boulder, Colorado 80303
303-443-9048
jenkins@mjplawyers.com
Counsel for Defendant
Jared Wheat

/s/ Jack Wenik
Jack Wenik
Epstein Becker & Green, P.C.
One Gateway Center, 13th Floor
Newark, New Jersey 07102
973-639-5221
jwenik@ebglaw.com
Admitted Pro Hac Vice
Counsel for Defendant
Hi-Tech Pharmaceuticals, Inc.

CERTIFICATE OF SERVICE

I hereby certify that I have this day filed the foregoing "Defendants Jared Wheat and Hi-Tech Pharmaceuticals, Inc.'s Motion to Suppress Evidence Seized Pursuant to the Search Warrants for Emails and Electronically Stored Information and Memorandum in Support" through this District's ECF system, which will automatically serve all counsel of record.

This 10th day of November 2017.

/s/ Arthur W. Leach
Arthur W. Leach
Counsel for Defendant
Hi-Tech Pharmaceuticals, Inc.