MATTHEW SCHINDLER, OSB# 96419
501 Fourth Street #324
Lake Oswego, OR 97034
Phone: (503) 699-7333
FAX: (503) 345-9372
e-mail: mattschindler@comcast.net

ATTORNEY FOR DEFENDANT GREGORY WALSH

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

UNITED STATES OF AMERICA,
Plaintiff,

Case No. 3:13-CR-00332-02-SI

MOTION TO SUPPRESS EVIDENCE

vs.

GREGORY WALSH,
Defendant(s).

Defendant, Gregory Walsh, through his attorney, Matthew Schindler moves the Court for an order suppressing all evidence obtained through the execution of a search warrant that, without limitation or relationship to probable cause, authorized the seizure and search of the entire contents of his personal email account. The search warrant fails to meet minimum Constitutional standards because it is overbroad and lacks particularity. The search of Mr. Walsh's email account was unreasonable and violates the Fourth Amendment and therefore all evidence derived from that search must be suppressed.

1. Procedural Background:

On January 15, 2014 the government indicted Gregory Walsh and his brother, Geoff Walsh, with a variety of fraud offenses. On July 22, 2015 Geoff Walsh pleaded guilty to a superseding information charging him with conspiracy to provide false statements to a financial institution. Greg Walsh was initially represented by attorney Robert Calo. Mr. Calo took a position overseas and withdrew from representation. Attorney Lawrence Matasar took over for Mr. Calo and represented Mr. Walsh until he could no longer afford him. Neither filed anything substantive on Mr. Walsh's behalf. Counsel was appointed to represent Mr. Walsh under the CJA on June 18, 2015.

There have been a number of discovery issues that the parties have worked through to this point. The delays in litigating this case result from discovery issues never addressed by prior counsel. The defense believes that most, if not all, of the outstanding discovery issues have been resolved. Trial in this matter is currently set for May 2, 2016.

2. Factual Background:

a. The fraud:

This case emanates from Mr. Walsh's position as a financial advisor for Morgan Stanley. The government's allegations are that beginning in March 2011, Mr. Walsh engaged in fraudulent conduct which induced the one of Mr. Walsh's clients to provide money to his brother, Geoff. With the loan SP funded, Geoff Walsh engaged in a series of financial transactions and real estate deals with about

which he made certain representations. In the end, he did not fulfill those promises. SP was Greg Walsh's single biggest client at Morgan Stanley. Other than the wages and commissions he received from working at Morgan Stanley, Greg Walsh did not benefit in any way from his brother's activities.

While he was working with SP, Mr. Walsh used an email account provided by Morgan Stanley. That account is not the subject of this suppression motion. He also relied on a personal email account he obtained through Cox Communications to communicate with SP. It is the second of these accounts, the Cox Communications email account, which is addressed by this motion.

The precise dimensions of the fraud are not germane except that the government knew that the only alleged victim that Greg Walsh was involved with was SP and the government knew the specific timeframe in which the relevant transactions took place.

b. The Search Warrant:

The affidavit of FBI Special Agent Matthew Swansinger in support of the search warrant was provided by the government in discovery and is attached as Exhibit 1. The component of it that Mr. Walsh challenges is called Attachment B which as attached separately as Exhibit 2.

The process of seizing Mr. Walsh's email account began several weeks before the service of the warrant which occurred on October 25, 2013. On October 3, 2013, FBI Agent Matthew Swansinger faxed a letter to Cox communications requesting that Mr. Walsh's email account be preserved. A copy of that facsimile is

attached as Exhibit 3. There are no limitations on the scope of the materials related to the email account that the government requested Cox Communications preserve pending additional "legal process."

Attachment B also does not provide any limitation on the materials to be disclosed to the government. There is no temporal limitation and there is no restriction connected to the underlying probable cause.

In regards to Mr. Walsh's personal email account, Cox Communications was required to disclose to the government:

- The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- All records or other information regarding the identification of the account, to include full customer or subscriber name, customer or subscriber physical address, local and long distance connection records, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, 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);

- The types of service utilized;
- All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- All records pertaining to communications between the Email Service Provider and any person regarding the Email Account, including contacts with support services and records of actions taken.
- All content, records and information associated with the Email Account preserved by the Email Service Provider pursuant to a preservation request made by FBI Special Agent Matthew Swansinger on October 3, 2013.

Exhibit 2 at 1-2.

There does not appear to be any dispute about the fact that this required disclosure to the government of everything associated with Mr. Walsh's personal email account – every picture, every attachment, every contact, and the contents of every single email.

Attachment B describes a bifurcated procedure where all account information will be "disclosed" to the government and then later specific information within that account will be "seized" after the government has reviewed it without limitation. The precise scope of what this authorized the government to

"seize" is extremely difficult to understand because the language of the attachment is unclear.

Mr. Walsh acknowledges that the attachment does provide a laundry list of possibly relevant locations, email addresses, phone numbers, and names as an apparent limitation on the scope of the information to be seized. *See Exhibit 2 at* 2-4. The "seizure" is limited to information falling after the date January 1, 2010. *Exhibit 2* at 2. Mr. Walsh does not dispute that the government had limited probable cause to search for emails to the extent it related to SP and the beginning date of the indictment. *See In re Search of Google Email Accounts identified in Attachment A*, 92 F. Supp. 3d 944, 953 (D. Alaska 2015) However, the attachment authorizes the seizure of all information preserved by the email service provider relative to the letter from SA Swansinger demanding preservation. *See Exhibit 2* at 4. It does not limit the search to emails that relate to the investigation. It authorizes the review of all emails even if they have nothing to do with SP.

The defense requested the government provide any type of guidance and/or minimization instructions that the USAO provided to law enforcement as a guide to lawfully executing this warrant. The government represented that no such information or guidance exists. The lack of guidance means Mr. Walsh has no way of knowing how many of his private emails were reviewed in order to determine what was going to be reviewed. We also have no way of knowing what the guidelines were for reviewing those emails. Unlike a wiretap, no minimization or other instructions were provided by the government to the FBI. There are no

contemporaneous reports indicating what emails were reviewed or the process that was employed. There is no way of knowing if the list of items connected to probable cause in Attachment B actually limited the government's review in any way. *See Exhibit 2* at 2-4.

It is also important for the purposes of this motion that Mr. Walsh is not attacking the constitutionality of the taint team process laid out in the warrant. At this point, he has no reason to believe the government seized any emails from his personal account that implicate attorney client privilege. It is important, however, that based on the warrant, the taint team does not appear to have redacted emails that might have been covered by any other privilege such as the marital communications privilege or doctor-patient privilege. There are no written reports that have been provided to the defense explaining how the taint team functioned in this particular case.

The sum total of the information available regarding the execution of this warrant is found in the search warrant return which is attached as Exhibit 4. It is a one paragraph narrative of how the taint team operated:

> "FBI Special Agent Brian Kelly conducted the search as the taint agent and provided the case agents with a redacted report.[1] The redactions were made with the intent of protecting the attorney-client privilege between target and retained attorneys. The redactions were made after consulting with the taint AUSA. FBI Special Agent Kelly has retained an unredacted copy of the search results should be needed at a further date."

[1] There is no report. The defense requested it.

Exhibit 4.

LEGAL ARGUMENT

1. Mr. Walsh has a reasonable expectation of privacy in his personal email account.

The Fourth Amendment of the United States Constitution guarantees the right of citizens against unreasonable searches and seizures:

> 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.

The Fourth Amendment does not provide a list of exceptions. Nothing in its text suggests the government may engage in far-reaching fishing expeditions into a person's private correspondence untethered from probable cause. The fundamental purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Camara v. Mun. Court of City & Cnty. of San Francisco*, 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967).

Unbelievably, it does not appear that the issue of Mr. Walsh's expectation of privacy in his personal email account has been settled by the Supreme Court. However, based on the Supreme Court's pronouncements regarding privacy over the last 50 years and the Sixth Circuit's analysis of the issue *Warshak*, it seems very

likely that it would endorse an individual's reasonable expectation of privacy in their personal email account even if provided by a third-party.

The Supreme Court has held that there is a reasonable expectation of privacy in other forms of communication that are very similar to email, such as telephone and mail. In *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), the Court found that telephone users were "surely entitled to assume that the words ... utter[ed] into the mouthpiece w[ould] not be broadcast to the world," leading to a holding that has brought telephone conversations fully under the shelter of the Fourth Amendment. *Id.* at 352. In *United States v. Jacobsen*, 466 U.S. 109, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984), the Court found that "[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy," based on the premise that a search arises any time the government "infringes upon 'an expectation of privacy that society is prepared to consider reasonable.'"

In *City of Ontario, California v. Quon,* ___ U.S. ____, ____, 130 S.Ct. 2619, 2630, 177 L.Ed.2d 216 (2010) the Supreme Court addressed the reasonableness of a government employer's search of text messages sent and received on an employee's pager. While it did not directly decide the issue, the Court assumed *arguendo* that the employee had a reasonable expectation of privacy in text messages sent and received on the government employer-owned pager. *Id.* at 2630.

That a third party intermediary was involved like the phone company, or here, an Internet Service Provider, does not appear to be material to the analysis.

The Sixth Circuit in *United States v. Warshak*, 631 F.3d 266, 282–88 (6th Cir.2010), has extended Fourth Amendment protection to emails stored with third-party electronic communication service providers. The court held that the reasonable expectation of privacy for communication via telephone and postal mail, recognized by the Supreme Court respectively in *Katz* and *Jacobsen*, extends to emails stored with third parties, bringing stored emails within the protection of the Fourth Amendment. *Id*. at 285–87 (citing *Katz*, 389 U.S. at 352, and *Jacobsen*, 466 U.S. at 113).

In analyzing the issue and reaching its decision, the *Warshak* court reasoned that emails are analogous to phone calls and letters, and an internet service provider is the functional equivalent of a telephone company or the post office, thereby entitling email communications to the same strong Fourth Amendment protections traditionally afforded to telephone and letter communications. "Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection." *Id*. at 285–86. Based on this analysis, the Sixth Circuit held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial [internet service provider].'" *Id*. at 288.

Congress passed the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 et seq., which underlies this search warrant application, in 1986 as part of the Electronic Communications Privacy Act ("ECPA"). "The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the

Fourth Amendment does not address." *Quon v. Arch Wireless Operating Co., Inc*., 529 F.3d 892, 900 (9th Cir.2008). First, the statute limits the government's right to compel providers to disclose information in their possession about their customers and subscribers. 18 U.S.C. § 2703. Second, the statute limits the right of an Internet Service Provider ("ISP") to disclose information about customers and subscribers to the government voluntarily. 18 U.S.C. § 2702.

The ECPA was enacted against a backdrop of Fourth Amendment protections and privacy concerns.

> "With the advent of computerized record keeping systems Americans have the ability to lock away a great deal of personal and business information ... [T]he law must advance with technology to ensure the continued vitality of the fourth amendment.... Congress must act to protect the privacy of our citizens ... The Committee believes that [this Act] represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies."
>
> S.Rep. No. 99–541, at 3557–59 (1986), 1986 U.S.C.C.A.N. 3555, 3559.

This passage indicates that Congress' primary intent in passing the ECPA was to protect the privacy interests of American citizens. *Suzlon Energy Ltd. v. Microsoft Corp*., 671 F.3d 726, 729-30 (9th Cir. 2011).

Given this backdrop, it is difficult to imagine the USAO for this district arguing against a legitimate expectation of privacy in one's personal email account. If Mr. Walsh has such a reasonable expectation of privacy, then the Fourth Amendment applies to the government search of his email account. *Katz v. United*

States, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). The application of the Fourth Amendment requires the government to obtain a warrant that described particularly what was to be searched and limited the breadth of that search to the probable cause underlying it.

2. Section II of Attachment B of the warrant is overbroad.

a. The initial search by the government of Mr. Walsh's personal email account violates the Fourth Amendment.

The manifest purpose of the Fourth Amendment particularity requirement is to prevent general searches. *Maryland v. Garrison,* 480 U.S. 79, 84, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987). By limiting the authorization to search the specific areas and things for which there is probable cause to search, the particularity requirement ensures that the search will be carefully tailored to its justifications, and will not become a wide-ranging, exploratory search prohibited by the Fourth Amendment. *Id.* Thus, the scope of a lawful search is:

> defined by the object of the search and the places in which there is probable cause to believe that it may be found. Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase.
>
> *Id.* at 84–85.

"The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is

left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196, 48 S. Ct. 74, 76, 72 L. Ed. 231 (1927).

The rise of personal computing and networking has heightened the risk of overbroad warrants and at the same time the federal courts seem more and more willing to defer to the government's claims about what it "needs." The courts assume that when the government seeks to search electronic data for evidence of a crimes on a personal computer, how data is stored and how it can be hidden or disguised requires that the government look at all of the files. The Ninth Circuit endorsed this fiction in Comprehensive Drug Testing:

> This pressing need of law enforcement for broad authorization to examine electronic records ... creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant. The problem can be stated very simply: There is no way to be sure exactly what an electronic file contains without somehow examining its contents—either by opening it and looking, using specialized forensic software, keyword searching or some other such technique. But electronic files are generally found on media that also contain thousands or millions of other files among which the sought-after data may be stored or concealed. By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there.
>
> *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir.2010) (en banc) (per curiam).

Comprehensive Drug Testing gives short shrift to the fact that the Fourth Amendment was specifically intended to restrain the government. Nevertheless, the court starts with a flawed assumption that because the government has probable

cause to believe a crime has been committed, and electronic data is involved, the government should be allowed to look at the largest possible spectrum of data before deciding what it wants. This attitude has fostered an environment of *de jure* general warrants for electronic data. *See e.g. In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc*., 33 F. Supp. 3d 386, 395 (S.D.N.Y. 2014), as amended (Aug. 7, 2014).

On one hand the courts caution against general warrants, and yet the same courts assume that what amounts to a general warrant is appropriate in the context of electronic data. *Id*. Since the government is not sure where evidence might be within the electronic data it should be allowed to look at all of it. Many cases assume that the gross over-seizure of private information is a "necessity" and an inherent part of the electronic search process." *Comprehensive Drug Testing, Inc., 621 F.3d at 1176.* "Over-seizing" is an accepted reality in electronic searching because "[t]here is no way to be sure exactly what an electronic file contains without somehow examining its contents." *United States v. Flores,* 802 F.3d 1028, 1044-45 (9th Cir. 2015); *In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc*., 33 F. Supp. 3d 386, 395 (S.D.N.Y. 2014), as amended (Aug. 7, 2014).

Mr. Walsh does not concede that these courts' logic is consistent with the Fourth Amendment. Given the sophisticated software search capabilities that now exist, we no longer need to accept over-seizure by the government as a necessity.

Given the current state of technology, it should never be acceptable under the Fourth Amendment for the government to ever look at every email in Mr. Walsh's personal email account to determine whether or not a few are relevant to its case.

The constitutional flaw in this over-seizing is that it necessarily produces over-searching. While Mr. Walsh acknowledges that the government had some limited right to search for information relating to SP in his email account, that authority was fundamentally limited. *See In re Search of Google Email Accounts identified in Attachment A*, 92 F. Supp. 3d 944, 951 (D. Alaska 2015). In this case, the wording of the warrant certainly authorized an FBI special agent to look at every single one of Mr. Walsh's emails. By definition, that is overbroad. The permissive attitude of the courts has fostered warrants, such as the one at issue here, which do not sufficiently prevent the government from conducting a fishing expedition.

Some courts apologize for the government's blatant violation of privacy in this context by glossing over the intrusiveness of the initial search - the one characterized as a "necessity". In this case, the warrant authorized an FBI agent to look through thousands of Mr. Walsh's personal emails after the removal of only those that implicated attorney-client privilege. The important violation of Mr. Walsh's rights occurs not at some distant point in the future when the government happens to choose one or two emails from thousands it has looked at and then uses those to prosecute him. *See e.g. United States v. Flores*, 802 F.3d 1028, 1045 (9th Cir. 2015). The violation of his privacy occurs the moment someone from the government starts sifting through his personal, private correspondence. It does not

take a great deal of imagination to consider how much information is exposed to the government in this context for no reason. Why should the government be allowed to look at privileged communications between Mr. Walsh and his wife regarding their children or communications between Mr. Walsh and his doctor regarding treatment over the course of four years in order to execute a search warrant for a financial fraud involving a single victim?

It is the responsibility of the judiciary to demand that the standards applied to these kinds of searches evolve with technology otherwise the Fourth Amendment is meaningless. "The facts of this case well-illustrate the troubling implications to Fourth Amendment jurisprudence of allowing the government to seize and inspect a person's entire email account." *In re Search of Google Email Accounts identified in Attachment A*, 92 F. Supp. 3d 944, 953 (D. Alaska 2015). It is essential that the courts be vigilant in assuring that the scope of the search is narrowly tailored to probable cause.

b. The language of the warrant unlawfully allows the Government to seize and search Mr. Walsh's entire email account from January 1, 2010 forward.

The Ninth Circuit has developed the following three-factor test to determine whether a warrant is sufficiently precise:

> (1) whether probable cause exists to seize all items of a particular type described in the warrant, (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not, and (3) whether the government

> was able to describe the items more particularly in light of the information available to it at the time the warrant was issued.
>
> *United States v. Vasquez*, 654 F.3d 880, 884 (9th Cir.2011); *United States v. Storm*, No. 3:11-CR-00373-SI, 2012 WL 3643845, at *9 (D. Or. Aug. 23, 2012) aff'd, 612 F. App'x 445 (9th Cir. 2015).

The warrant in this case fall short in all three respects. The way the warrant is drafted indicates that the government will take the position that when it received all of Mr. Walsh's personal emails from Cox communications and then reviewed it was not a seizure. Mr. Walsh disagrees. When those emails were no longer within his control, or the control of Cox communications, and the government had the ability to look at every single one of them that has to be a seizure under the Fourth Amendment. Agent Swansinger's affidavit does not set forth probable cause to seize every one of Mr. Walsh's emails. The warrant the fails the first part of the *Vasquez* test.

Section 2 of Attachment B sets forth the information to be seized by the government. *See Exhibit 2* at 2 – 4. The government obviously understood that this warrant would expose thousands of emails completely unrelated to either its investigation or any crime. It attempted, we believe, to limit the information seized under Attachment B consistent with the Fourth Amendment.

For example, a date limitation, January 1, 2010, is included. *See Exhibit* 2 at 2. There are categories that relate to relevant parties, email addresses, phone numbers, and entities. *See Exhibit 2* at 2 – 4. Those categories are important because they connect this warrant to probable cause, otherwise this truly is an exploratory

search which violates the Fourth Amendment. *Maryland v. Garrison*, 480 U.S. 79, 84, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987); *Payton v. New York*, 445 U.S. 573, 584 n. 21, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980) (retracing the roots of the particularity requirement to the colonialists' objections to the writs of assistance).

The problem, however, is that this warrant was drafted in such a way so that these relevant categories do not in fact limit what law enforcement can seize. Paragraph E of Attachment B authorizes the seizure of: "all content, records and information associated with the email account preserved by Email Service Provider pursuant to a preservation request made by FBI Agent Matthew Swansinger on October 3, 2013." *Exhibit 2* at 4. The October 3 preservation letter is incredibly broad, reaching the entire contents of Mr. Walsh's personal email account and without date limitation or relationship to probable cause. *See Exhibit 3*. Paragraph E effectively eliminates the other limitations contained in Attachment B and means that this warrant fails to satisfy the second and the third part of the *Vasquez* test. When read in conjunction with Attachment B it is clear that the government was authorized to seize the entire contents of Mr. Walsh's personal email account from January 1, 2010 forward. That cannot be consistent with the Fourth Amendment.

Another problem with Attachment B is that beyond the date, it does not impose any limits on the case agent's review of the entire email file except that the information be connected to federal fraud or money laundering offenses. The warrant authorizes the government to seize: "all information described above in section I that constitutes evidence of violations of title 18 USC § 1343, Wire Fraud,

and Title 18 United States Code, Section 1957, Engaging In Monetary Transactions And Property Derived From Specified Unlawful Activity, for the time period of January 1, 2010, to the present, including:…" *See Exhibit 2* at 2.

The warrant then provides a series of categories that appear to be an attempt to relate the seizure in some way to the underlying probable cause. The problem, however, is the word "including" at the end of paragraph one of Section II. *See Exhibit 2* at 2. "Including" is not a word of limitation. That term means that the search had no limitations at all except the date of January 1, 2010 and some connection will to fraud or money laundering. The first paragraph of Section II of the warrant should have ended with the words "limited to" otherwise the terms that follow are mere suggestions regarding the scope of the search.

The government has made no showing here that Mr. Walsh's business was so thoroughly permeated with fraud that it was entitled to seize his entire email account. Because the warrant was facially overbroad, authorizing the government to seize and search the entirety of Mr. Walsh's personal email account data for a nearly four year period, all evidence resulting from that search must be suppressed.

c. The scope of the warrant is not justified by the underlying probable cause.

Despite the fact that the federal courts have created numerous exceptions in the area of electronic data privacy that cannot be found in the text of the Fourth Amendment, some courts still demand that the scope of probable cause define the scope of the search. *In re Search of Google Email Accounts identified in Attachment*

A, 92 F. Supp. 3d 944, 953 (D. Alaska 2015); *In re Applications for Search Warrants for Info. Associated with Target Email Address*, No. 12-MJ-8119-DJW, 2012 WL 4383917, at *10 (D. Kan. Sept. 21, 2012). There must be some threshold showing before the government may "seize the haystack to look for the needle." *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006). If the government intends to seize and search everything, then the affidavit in support of the search warrant must explain why. *United States v. Tamura*, 694 F.2d 591, 595 - 596 (9th Cir.1982); *Hill*, 459 F.3d at 976.

This is where this warrant fails. The January 1, 2010 temporal limitation in Attachment B bears no relationship to probable cause. The very first day Agent Swansinger can connect an email from Mr. Walsh's personal account to investment activity involving SP and Geoff Walsh is March 9, 2011. This corresponds to the beginning date listed in the indictment. *See Exhibit 1* at 25. There is no explanation in the affidavit for why it would be appropriate for him to reach back more than a year into Mr. Walsh's personal email account.

The affidavit refers to several other instances where Mr. Walsh's personal email account was used to correspond with his brother or with SP. For example, the affidavit states that the government's investigation revealed that beginning March 1, 2013 Greg Walsh used his email account at walshg@cox.net to communicate with SP. *See Exhibit 1* at 11. The affidavit cites a total of three additional emails from Mr. Walsh's personal account that had been provided to the FBI which it believed were relevant to the investigation. *See Exhibit 1* at 12-13. Agent

Swansinger's affidavit goes on to detail other investments involving SP, Greg Walsh, and Geoff Walsh. *See Exhibit 1* at 17, 20. In total the affidavit refers to five emails sent from Mr. Walsh's personal email account between March 9, 2011 and June 28, 2013.

The affidavit fails to explain why it was necessary to seize thousands of emails predating any evidence of fraud. Even assuming for the sake of argument that the government was entitled to the entire contents of his email account, which Mr. Walsh disputes, the beginning date for the warrant should have been January 1, 2011 allowing the government a generous amount of time to seek out pre-conspiracy communications. This warrant gave the government the right to access thousands of emails for which it had no probable cause. It had no reason to believe that on January 1, 2010 any criminal activity had taken place. To the extent this date was included as a limitation, it was a limitation unconnected to probable cause and rendered the warrant overbroad.

d. The procedure for executing this warrant renders it unconstitutional.

Mr. Walsh acknowledges that the current state of the law is such that the fact that the government provided no instructions and offered no real limits to its officers executing this warrant does not itself make it unconstitutional. *United States v. Storm*, No. 3:11-CR-00373-SI, 2012 WL 3643845, at *10 (D. Or. Aug. 23, 2012) aff'd, 612 F. App'x 445 (9th Cir. 2015). Nevertheless, it is clear that the government

should have done much, much more here to protect Mr. Walsh's expectation of privacy in his personal email account.

Despite its flaws, Attachment B does contain a number of relevant search terms that could have limited the agents but because of the government's unartful drafting did not restrain them in any meaningful way. What those terms to make clear, however, is that the government could have described with a great deal more precision what it intended to seize in a way that would have complied with the third part of the *Vasquez* test.

While the search procedure section of the warrant indicates that a taint team will be involved, that process had nothing to do with either eliminating irrelevant emails or protecting privileged materials other than attorney-client privileged documents. The search process outlined here did nothing to protect Mr. Walsh's underlying interest in the privacy of his emails.

There should have been a process in place that separated the investigating agents from Mr. Walsh's email account during the initial review phase and that initial phase should have culled far more than simply attorney-client privileged emails. The balancing of Mr. Walsh's privacy interest in his private email correspondence and the government's limited interest in a small number of emails should have been weighted much more in Mr. Walsh's favor. Agent Swansinger should never have had access to the entire contents of that email account. The government should have limited the review to the items listed in paragraphs A through D of Section II of Attachment B.

In addition, that initial review should have been done by a third party not the government Mr. Walsh believes the. The nature of the review that actually took place is also constitutionally significant. The defense is not entirely sure how the review was undertaken because no contemporaneous reports were produced. There is no log. Nothing in discovery has been produced which indicates how agent Swansinger accomplished the initial review of the email file.

Mr. Walsh argues that there is a constitutional difference between a nongovernment third-party contractor using keyword search terms to identify relevant emails and an FBI agent individually opening and looking at each email. The current state of technology allowed the government to obtain an email container file. That container file could have been searched very thoroughly without looking individually at any emails. Instead this warrant does not identify any sorting or filtering procedures for electronic communications and information that are not relevant and do not fall within the scope of the government's probable cause statement. *See e.g. In re Applications for Search Warrants for Info. Associated with Target Email Address*, No. 12-MJ-8119-DJW, 2012 WL 4383917, at *8 (D. Kan. Sept. 21, 2012); *In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, No. 13-MJ-8163-JPO, 2013 WL 4647554, at *9 (D. Kan. Aug. 27, 2013).

This procedure would have tailored the items seized to the probable cause. The government frequently uses third-party contractors to handle electronic discovery issues. Better yet, the government could have simply had Cox

communications only produce for it emails which contain search terms from paragraphs A through D of Section II of Attachment B. The government has made no showing that this would've placed too great a burden on Cox communications.

The level of intrusion involved could have been ameliorated with a search protocol that relied on targeted searches rather than a blanket sweep unconnected to probable cause. Because the government understood very precisely the potential dimensions of this fraud, there was no need for it to review the entirety of Mr. Walsh's personal email account. The government has thus failed to comply with the third component of the *Vasquez* test requiring a more particular search when the government possesses more specific information.

It is further problematic that the government did not provide FBI agent Swansinger more specific instructions about the execution of this warrant. In wiretap cases, the government always provides minimization instructions to law enforcement so that calls unrelated to the investigation are not recorded at all. The exact same kind of procedures should have been employed here. "[T]he warrants must contain some limits on the government's search of the electronic communications and information obtained from the electronic communications service provider. To comport with the Fourth Amendment, the warrants must contain sufficient limits or boundaries so that the government-authorized agent reviewing the communications can ascertain which email communications and information the agent is authorized to review." *In re Applications for Search*

Warrants for Info. Associated with Target Email Accounts/Skype Accounts, No. 13-MJ-8163-JPO, 2013 WL 4647554, at *9 (D. Kan. Aug. 27, 2013)

3. Conclusion:

The set of circumstances under which a court should ever approve a multi-year seizure and search of a personal email account is extremely limited. This is an extraordinarily broad invasion of an individual's legitimate expectation of privacy in their personal email correspondence. The limited probable cause that existed to search Mr. Walsh's personal email account was exceeded by the search that this warrant authorized. Thousands of emails were unnecessarily exposed to FBI review. The affidavit in support of the search warrant fails to justify the breath of this search and therefore it fails to comply with the Fourth Amendment. All evidence obtained as a result of the search warrant should be suppressed.

Respectfully submitted on January 25, 2016.

Matthew Schindler, OSB #96419
Attorney for Gregory Walsh