UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. DZHOKHAR TSARNAEV	No. 13-CR-10200-GAO

MOTION TO SUPPRESS FRUITS OF SEARCHES: ELECTRONICALLY STORED INFORMATION, INCLUDING EMAIL COMMUNICATIONS AND DATA CONTAINED IN THE SONY VAIO LAPTOP COMPUTER

Defendant, by and through counsel, moves that this Court suppress from evidence at trial any substantive communications, or any fruits of such evidence, that were unlawfully seized by the government pursuant to search warrants directed to Yahoo! and Google for email communications and associated data. Defendant further moves that the Court suppress from evidence at trial electronic files and data seized and searched pursuant to a warrant authorizing the search of his Sony Vaio laptop computer. As grounds for this motion, undersigned counsel state that the searches violated Mr. Tsarnaev's rights under the Fourth Amendment to the United States Constitution because:

1) the April 19, 2013, warrant to seize and search Mr. Tsarnaev's j.tsarnaev@yahoo.com email account failed to establish probable cause and the subsequent use of the fruits of that illegal search to obtain the July 3, 2013 search warrant to seize and search his two Gmail accounts was impermissible;

2) the failure of all three warrants to provide for a procedure, specifically the use of a filter team, to distinguish between or otherwise segregate responsive communications or computer data from irrelevant communications and data effectively authorized general searches prohibited by the Fourth Amendment; and

3) the government's inspection of *all* of the email communications from email providers Yahoo and Google and *all* of the data contained in the Sony Vaio laptop computer, regardless of whether each piece of data related to the criminal violations set forth in the authorizing warrants, exceeded the scope of the warrants.

FACTS

A. THE YAHOO EMAIL ACCOUNT

On April 15, 2013, two bombs exploded at the Boston Marathon, killing three spectators and injuring many others. The suspects remained unidentified until the evening of April 18. A later carjacking ended with Tamerlan Tsarnaev's death in a shootout with law enforcement agents in Watertown. Tamerlan's younger brother, Dzhokhar, fled the scene of the gun battle and there ensued a manhunt that lasted 17 hours.

On April 19, Tamerlan was identified through fingerprints. While law enforcement agents searched for Dzhokhar, federal agents applied for and received a search warrant to seize and search content and data associated with both Tamerlan's and

Dzhokhar's Yahoo email accounts.[1] The search warrant for the two email accounts issued at 3:12 p.m. on April 19, and is filed under seal as Exhibit A; the search warrant affidavit in support is filed under seal as Exhibit B. The facts presented to support probable cause as to the email accounts were exceedingly scanty. Under the heading "Probable Cause to Believe that the Accounts Contain Evidence, Fruits, and Instrumentalities," the warrant affidavit stated:

> I also have probable cause to believe that the Subject Accounts and the data associated with those accounts contain evidence, fruits, and instrumentalities of the crimes identified above. I base this conclusion in part on my training and experience. I know that many people regularly use e-mail to provide contact information to others, as well as to discuss future plans and to make logistical arrangements. I also know, based on my training and experience, that many criminals use e-mail to plan and discuss their criminal schemes.
>
> Furthermore, the characteristics of both Tamerin [sic] and Dzhokhar Tsarnaev make it likely that the Subject Accounts contain evidence, fruits, and instrumentalities of the crimes identified above. It appears that both Tamerin and Dzhokhar used social media. It appears that Tamerin had a YouTube page containing several videos. It appears that Dzokhar [sic] has a Facebook page. Given their ages (19 for Dzokhar and 26 for Tamerin), their use of social media, and the fact that they provided Yahoo! E-mail addresses to the Department of Education and Bunker Hill Community College, there is probable cause to believe that they used these e-mail accounts regularly, and that evidence of the crimes described in this affidavit would be found in them.

[1] The FBI on April 19 simultaneously obtained search warrants for the Tsarnaev family home at 410 Norfolk Street, Cambridge and two cars associated with the Tsarnaev family. The 410 Norfolk Street search is the subject of a separate challenge. *See* D.E. 297

Exhibit B at p. 11 ¶ 37-38. The warrant affidavit also disclosed that law enforcement agents had already seized the data sought by the search warrant before they applied for the warrant. Exhibit B at p. 2 ¶ 6.[2]

The search warrant referenced Attachment A, which authorized the "search" of Yahoo for the "seizure" of account content and associated data for the two email accounts. Exhibit A at pp. 1-3. Attachment A, in turn, referenced Attachment B, which listed the procedure for the disclosure by Yahoo along with a list of the types and kinds of data that were to be culled by law enforcement forensic search of the Yahoo disclosure. *Id.*

Attachment B directed a two-part process for the retrieval, seizure, and search of the requested material. First, Yahoo would provide law enforcement with a duplicate of all of the specified content and associated data listed in its possession. Exhibit A at p. 4-6. Once provided to agents, the content and data would be forensically searched for broad categories of information. Exhibit A at pp. 6-7. Despite the sparse probable cause provided in the affidavit, the list of sought items was sweeping. Under the general

[2] The search warrant affiant invoked 18 U.S.C. 2702(b)(8) of the Stored Communications Act (SCA) as an explanation of why the government already was in possession of the content and associated data for the two accounts, and went on to aver that the content of the disclosure had not yet been reviewed by him. Exhibit B at p. 2 ¶ 6. Section 2702(b)(8) permits a provider such as Yahoo to disclose stored communications to a governmental entity if it believes in good faith that an emergency involving danger of death or serious physical injury to any person requires that disclosure without delay. Section 2702(b)(8) , however, limits the communications that can be disclosed to those "relating to the emergency" at issue. As discussed herein, the communications actually disclosed were far broader than the emergency at issue on April 19, 2013.

heading of evidence, fruits, or instrumentalities of violations of 18 U.S.C. Sections 2332a(a)(2)(d), 844(i), 1951, 924(c) and 371, the list included:

1. All communications between or among Tamerian [sic] Tsarnaev and Dzhokhar Tsarnaev;

2. All communications pertaining to the Boston Marathon, explosives, bombs, the making of improvised explosive devices, firearms, and potential people and places against which to use firearms, explosives or other destructive devices.;

3. The identity of the person or persons who have owned or operated the J.tsarnaev@yahoo.com and Tamerlan~tsarnaev@yahoo.com e-mail accounts or any associated e-mail accounts;

4. The data described in paragraphs II(A)(3)-(5), above [*i.e.*, the contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content, calendar data, and lists of friends, buddies, contacts, or other subscribers].

6. [sic] The existence and identity of any co-conspirators;

7. The travel or whereabouts of the person or persons who have owned or operated the J.tsarnaev@yahoo.com and Tamerlan_tsarnaev@yahoo.com e-mail accounts or any associated e-mail accounts;

8. The identity, location, and ownership of any computers used to access these e-mail accounts;

9. Other e-mail or Internet accounts providing Internet access or remote data storage or e-commerce accounts;

10. The existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and

11. The existence or location of paper print-outs of any data from any of the above.

Exhibit A at pp. 6-7. Clause four, referring to the "data described in paragraphs II(A)(3)-(5), above," so broadened the data that a searcher was permitted to seize as to render the other limiting categories meaningless. Those clauses brought within the warrant's ambit:

> 3. *The contents of all electronic data files*, whether word-processing, spreadsheet, image, video, or any other content;
>
> 4. The contents of all calendar data;
>
> 5. Lists of friends, buddies, contacts, or other subscribers.

Exhibit B at pp. 7-8 (emphasis supplied). Because all emails, text, and instant messages *are* electronic data files, the reference authorizing the search and seizure of all electronic data files – without limitation to any category tied to the violations - permitted an unrestrained foray into the contents of everything seized by the government from Yahoo. In short, the April 19 warrant authorized law enforcement to seize all of the data from the accounts and search it without any limitation.

Notably, neither the warrant nor the referenced schedule established a method – for example, a filter team – to distinguish between email communications that fit within the listed categories and the irrelevant communications that did not. Nor did the warrant provide a temporal limitation tailored to the offenses set forth in the warrant application; instead, it directed that all content and data, regardless of how ancient, be seized and turned over to the government. In response to the warrant, Yahoo produced in excess of 6,000 emails and associated attachments.

B. THE SONY VAIO LAPTOP COMUTER

As the investigation unfolded, the government continued to seek and obtain search warrants (as well as grand jury and administrative subpoenas) for a variety of items , including digital items belonging to the Tsarnaevs and online service providers. On April 23, 2013, law enforcement agents sought a search warrant to search Mr. Tsarnaev's Sony Vaio laptop computer. The search warrant is filed under seal as Exhibit C; the affidavit in support of the application for the search warrant is filed under seal as Exhibit D. The facts included in support[3] of the search were, like those in the April 19 application, exceptionally sparse:

> From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e-mail, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.
>
> From my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B in computer hardware, computer software, computer-related documentation, and storage media. Some storage media, such as thumb drives, can be smaller than a stick of gum and can therefore be stored almost anywhere.
>
> In this case, I have probable cause to believe that the Target Computer belongs to Dzhokhar, one of the Boston Marathon bombers. The Target Computer was taken

[3] The affidavit suggests abandonment of the Sony Vaio laptop because FBI agents seized the computer from one of his friends by consent of the friend on April 19; the friend had collected it from Mr. Tsarnaev's dorm room the day before. Exhibit D at pp. 12-13, ¶¶ 38-41. However, there is no indication in the affidavit that Mr. Tsarnaev gave or otherwise voluntarily relinquished the computer to his friend. *Cf. United States v. James*, 353 F.3d 606, 616 (8th Cir. 2003) (giving computer disks to someone else to store did not constitute abandonment of them).

> from Dzhokar's [sic] dormitory room by Individual A and later seized by the FBI during a consent search of the apartment at 69A Carriage Road in New Bedford, Massachusetts.

Exhibit E at p. 14 ¶ ¶ 43-44. Although located in a different part of the affidavit, the affiant also disclosed that he had learned that Tamerlan and Dzhokhar purchased materials online which they used to manufacture the explosives used in the Marathon bombings. Exhibit E at p. 12 ¶ 36.

Like the April 19 warrant for the Yahoo email accounts, the search warrant for the Sony Vaio referenced Attachment A, which identified and generally authorized the forensic search of the Sony Vaio. Exhibit C at pp. 1-3. The search warrant also specifically referenced Attachment B, which listed the types of data that were to be culled from the forensic search of the computer. Exhibit C at pp. 1, 4-6 .

Despite the trifling and tenuous connection of the computer to the offenses alleged in the affidavit – that Dzhokhar and Tamerlan had purchased materials online to make the explosives – the list of items that were to be searched for was sweeping. Under the general heading of evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2232(a) (Using and Conspiring to Use A Weapon of Mass Destruction), 844(i) (Malicious Destruction of Property by Means of an Explosive Device Resulting in Death), 2119 (Carjacking), 1951 (Interference with Commerce by Violence), 924(c) (Use of a Firearm During a Crime of Violence) and 371 (Conspiracy to Commit Offenses), Sections 2332a, 844(i), 1951, 924(c) and 371, the list included:

1. Records, items, or other information, related to violations of the aforementioned statutes, including but not limited to, bomb making material and equipment, ammunition, weapons, explosive material, and components of bomb delivery devices;

2. Records or other information related to the ordering, purchasing, manufacturing, storage, and transportation of explosives;

3. Records or other information related to the ordering, purchasing, manufacturing, storage, and transportation of firearms;

4. Records or other information related to the ordering and purchasing of pressure cooker devices, BBs, nails, and other small metallic objects;

5. Records or information related to the Boston Marathon;

6. Records or information related to any plans to initiate or carry out any other attacks inside or outside the United States, or any records or information related to any past attacks;

7. Records or information related to the state of mind and/or motive of Tamerlan and Dzhokhar to undertake the Boston Marathon bombings;

8. Records or other information related to the identity of Tamerlan and Dzhokhar;

9. Records or other information related to the identity of any individuals who were in contact with, or were associates of Tamerlan and Dzhokhar;

10. Records or information, related to any organization, entity, or individual in any way affiliated with Tamerlan and Dzhokhar, that might have been involved in planning, encouraging, promoting the actions described herein;

11. Records or other information, related to Tamerlan's and/or Dzhokhar's schedule of travel or travel documents;

12. Records or information related to any bank records, checks, credit card bills, account information, and other financial records.

Exhibit C at pp. 4-7. The list went on to authorize the search of the actual computer equipment, such as hardware, software, and documentation. *Id.* ¶13. The scope of the warrant was broader than the April 19 search warrant; instead of being limited to items "including" the identified categories, it contained the more expansive phrase "including, *but not limited to*" the identified categories. Exhibit C at p. 4 (emphasis supplied). As with the April 19 Yahoo warrant, neither the warrant itself nor the referenced attachments established a method to distinguish between files that fit within the particularized categories and files that did not. Nor did the warrant provide a temporal limitation tailored to the offenses set forth in the warrant application; instead, it directed that all content and data, regardless of how ancient, be seized and turned over to the government.

C. THE GMAIL ACCOUNTS

On July 3, 2013, after the grand jury had returned its indictment against Mr. Tsarnaev, the government sought search warrants for multiple providers, including Google, Facebook, YouTube, Twitter, Instagram, and Skype.[4] In regard to Google, agents

[4]Of the several platforms and providers subjected to search by the government – Yahoo, Google, Facebook, YouTube, Twitter, Instagram and Skype – this Motion only addresses suppression of the email content and data provided by Google and Yahoo. The amount of data provided in discovery is vast, and the breathtaking amount of data provided by the platforms in combination with the to-date unlimited scope of the government's case in chief makes it difficult to conclude with certainty that all evidence possibly subject to suppression has been considered. The defense attempts to cabin the universe of possible evidence at trial, and so attain certainty in regard to suppressible evidence, have been rebuffed. By letter dated December 9, 2013, the defense requested of the government notice the defense, pursuant to Fed. R. Crim. P. 12(b)(4) of its "intent to use (in its evidence-in-chief at trial) any evidence that the defendant may be entitled to discover under Rule 16." The government responded by letter on February 7, 2014: "The government has not yet identified all of the evidence that it intends to introduce in its case-in-chief, and it is too early for the government to rule anything out[.] Accordingly, at least for the time being, please treat everything that we have produced to you in discovery as something we may offer in our case-in-chief."

sought (among other things) more email communications and associated data from additional accounts, tsar1jahar@gmail.com and jahar1tsar@gmail.com, registered to Mr. Tsarnaev. The search warrant is filed under seal as Exhibit E; the search warrant affidavit is filed under seal as Exhibit F. The July 3 search warrant affidavit provided somewhat more support as to the purported probable cause than did the April 19 and 23 affidavits. Significantly, however the July 3 affidavit was strengthened in part by the review of the j.tsarnaev.com search results which, among other things, resulted in the conclusion that "Dzhokhar was an avid user of e-mail and social media, and used these methods to communicate with his brother Tamerlan, as well as others." The information requested was somewhat more particularized but the substantive breadth essentially tracked the same categories spelled out in the April 19 warrant. Like the April 19 warrant, it had no time limit.[5] And like the first search warrant, it contained no methodology or process to segregate irrelevant and thus protected emails. Google responded to the warrant by providing in excess of 160 emails.

The emails seized from Dzhokhar's Yahoo and Gmail email accounts, culled by forensic agents, and available to the government for use in trial of this matter, include (by way of representative sample) emails regarding clothing purchases for his mother, car parts purchases, Domino's Pizza order confirmations, Netflix requests, and his participation in the Model UN and Best Buddies programs while in high school. The Sony Vaio contained, among other things, high school and college homework

[5] Indeed, the lack of temporal limitation resulted in the seizure of many emails received in the gmail accounts *after* Mr. Tsarnaev's arrest.

assignments, pool lifeguard schedules, and personal pictures of family and friends taken over a period of several years, most taken well before the events at issue.

ARGUMENT

I. THE APRIL 19, 2013 SEARCH WARRANT APPLICATION FAILED TO ESTABLISH PROBABLE CAUSE TO SEIZE AND SEARCH THE J.TSARNAEV@YAHOO.COM EMAIL ACCOUNT, AND THE APRIL 23, 2013 SEARCH WARRANT APPLICATION FAILED TO ESTABLISH PROBABLE CAUSE TO SEARCH THE SONY VAIO LAPTOP ONCE ILLEGALLY OBTAINED INFORMATION IN THE UNDERLYING AFFIDAVIT IS EXCISED.

"'A warrant application must demonstrate probable cause to believe that (1) a crime had been committed – the "commission" element, and (2) enumerated evidence of the offense will be found at the place to be searched – the so-called "nexus" element.'" *United States v. Ribeiro*, 397 F.3d 43, 48 (1st Cir. 2005) (*quoting United States v. Feliz*, 182 F.2d 82, 86 (1st Cir. 1999)). With regard to the nexus requirement, a judge or magistrate must find that the information contained within the four corners of the search warrant affidavit establishes a fair probability that evidence of a crime will be found in the place to be searched. *Id.* at 86-87; *United States v. Rodrigue*, 560 F.3d 29, 33 (1st Cir. 2009). Examination of the affidavit in support of the April 19 application for the first warrant demonstrates the absence of a nexus specific to the violations being investigated. The seizure of the j.tsarnaev@yahoo.com email account, therefore, violated the Fourth Amendment.

The asseverations in the April 19 affidavit as to why evidence, fruits, and instrumentalities were likely to be found in Mr. Tsarnaev's email content were as general as they were bare. Boiled to its essence, the "nexus" to the email account existed,

according to the agent, because (1) "many criminals use e-mail," and (2) the Tsarnaev brothers, at ages 19 and 26, likely would have used social media and communicated with the outside world by email. Exhibit B at p. 11, ¶ 37-38. Glaringly absent was any hint that Mr. Tsarnaev or his brother had used email during the relevant time period at all, let alone that its use was in connection with the criminal violations that guided the search authorization. The "characteristics" cited as important to the nexus apply, of course, to an overwhelming percentage of the world population; application to Mr. Tsarnaev's age cohort specifically would mean that the government could establish probable cause to seize email content 100% of the time.

In regard to the April 23, 2013 warrant to search Mr. Tsarnaev's Sony Vaio, the sole link that provides a nexus between the violations and the purported need to search the laptop is the agent's asseveration that he had learned that Tamerlan and Dzhokhar purchased materials online which they used to manufacture the explosives used in the Marathon bombings. Exhibit D at pp. 11-12 ¶ 36. He almost certainly learned this information from the statements made by Mr. Tsarnaev at Beth Israel Deaconess Medical Center on April 20 through 22. The defense has sought to suppress those statements, arguing that they were involuntary and obtained in violation of *Miranda v. Arizona*. *See* D.E. 295. Should those statements be ruled inadmissible, probable cause for issuance of the April 23, 2013 warrant must be considered with the offending facts excised. *United States v. Dessesaure*, 429 F.3d 359, 367 (1st Cir. 2005). *United States v. Patane*, 542 U.S. 630, 640 (U.S. 2004) ("We have repeatedly explained 'that those subjected to coercive police interrogations have an automatic protection from the use of their involuntary

statements (or evidence derived from their statements) in any subsequent criminal trial.'") (citations omitted). Once excised, there is no basis in the search warrant application whatsoever to conclude that the Sony Vaio contained evidence, fruits, or instrumentalities of the violations alleged.

"Bare suspicion" that criminal evidence will be found in the place to be searched is insufficient for probable cause. *See Brinegar v. United States*, 338 U.S. 160, 175 (1949). The Fourth Amendment demands more: the critical element in a reasonable search is whether there is reasonable cause to believe that the specific incriminating evidence exists at the place to be searched. *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978). Because the Yahoo warrant affidavit failed to demonstrate probable cause to believe that any---let alone specific --- incriminating evidence would be located in Mr. Tsarnaev's email, the fruits of the Yahoo email content and associated data searches must be suppressed. Similarly, as the affidavit for Mr. Tsarnaev's Sony Vaio laptop failed to establish probable cause absent the unconstitutionally obtained information, the results of any search of the laptop must also be suppressed.

Given the complete lack of probable cause, there can be no claim of good faith reliance on the issuance of the warrant. *See United States v. Leon* 468 U.S. 897, 923 (1984)("Nor would an officer manifest objective good faith in relying on a warrant based on an affidavit 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable'").

II. THE WARRANTS' LACK OF PARTICULARITY AS TO THE THINGS TO BE SEARCHED FOR, AND THEIR FAILURE TO PROVIDE MEANINGFUL GUIDANCE TO SEARCHERS FOR DISTINGUISHING EMAIL CONTENT AND COMPUTER DATA THAT FELL OUTSIDE THE WARRANTS, EFFECTIVELY AUTHORIZED GENERAL SEARCHES.

General warrants are prohibited by the Fourth Amendment. *Andresen v. Maryland*, 427 U.S. 463, 480 (1976). General warrants are impermissible because they permit "a general, exploratory rummaging in a person's belongings[.]" *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). To avoid this problem, the Fourth Amendment requires "a 'particular description' of the things to be seized." *Id.* "As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Stanford v. Texas*, 379 U.S. 476, 485 (1965), *quoting Marron v. United States*, 275 U.S. 192, 196 (1927). "The *Marron* standard finds its derivation in Colonial America's aversion to writs of assistance and general warrants which placed broad discretionary authority with British custom officials to search anywhere for smuggled goods and seize anything they pleased." *United States v. Klein*, 565 F.2d 183, 186 (1st Cir. Mass. 1977). The First Circuit has explained,

> The particularity requirement demands that a valid warrant: (1) must supply enough information to guide and control the executing agent's judgment in selecting where to search and what to seize, and (2) cannot be too broad in the sense that it includes items that should not be seized.

United States v. Kuc, 737 F.3d 129, 133 (1st Cir. 2013).

Here, on April 19, 2013 the Magistrate Judge issued a limitless search warrant for J.tasnaev@yahoo.com and Tamerlan_tsarnaev.com, an expansive search warrant permitting a forensic search of Mr. Tsarnaev's entire Sony Vaio laptop computer on April

23, and, on July 3, 2013, a broad warrant for information associated with the email accounts tsar1Jahar@gmail.com and Jahar1tsar@gmail.com. The lack of particularity as to what was to be seized, or of guidance on how non-seizable data was to be protected, in essence authorized unconstitutional general searches. The fruits of the searches must therefore be suppressed.

A. The Warrant Terms Failed to Provide a Meaningful Limit on Searcher Discretion.

The particularity requirement is crucially important where, as here, the government seeks to search digital evidence. *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (stating that the ability of a computer to store "a huge array" of information "makes the particularity requirement that much more important"). In the context of email and other electronically stored communications, the particularity requirement necessitates that a stored communication seizure be designed to target e-mails or files that could reasonably be believed to have some connection to the alleged crime under investigation. *United States v. Warshak*, 490 F.3d 455, 476 n.8 (6th Cir. 2007). While it may sometimes be difficult for the government to identify the exact communications sought, it cannot have carte blanche to seize whatever it chooses: only evidence of the criminal activity under investigation may be seized. *See Kuc*, 737 F.3d at 133. The guiding principle in the email context, as in all searches, is that the government should seize only those e-mails and files related to the crime under investigation. *Id.* (*citing United States v. Whitten*, 706 F.2d 1000, 1009 (9th Cir. 1983)).

The seizure of all electronically stored evidence associated with an individual's email accounts or his computer allows precisely the kind of general rummaging through a

person's e-mail account that the Fourth Amendment proscribes. *See Cassady v. Goering*, 567 F.3d 628, 635 (10th Cir. 2009) (unconfined scope of warrant authorized the seizure of all possible evidence of any crime in any jurisdiction). This general rummaging permits a search into all corners of an individual's life. For this reason, warrants must contain "sufficiently particularized language" that demonstrates "a nexus" with the crime to be investigated and courts have invalidated warrants as overly broad for failing to do so. *United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009) ("[i]If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment's particularity requirement") (collecting cases); *United States v. Hall*, 142 F.3d 988, 996-97 (7th Cir. 1998) ("The search warrants were written with sufficient particularity because the items listed on the warrants were qualified by phrases that emphasized that the items sought were those related to child pornography."). Thus, warrants for stored e-mails and other stored communication files should provide details as to the particular offense that has been committed, is being committed, or is about to be committed, to which the sought-after communications relate. *See, e.g.*, *United States v. Rosa*, 626 F.3d 56, 62 (2nd Cir. 2010) ("The warrant was defective in failing to link the items to be searched and seized to the suspected criminal activity ... and thereby lacked meaningful parameters on an otherwise limitless search of Rosa's electronic media."); *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) ("The government could have made the warrant more particular. Most obviously, the warrant could have specified the suspected criminal conduct."); *United States v. Biasucci*, 786 F.2d 504, 510 (2nd Cir. 1986) ("The Constitution requires particularization in the warrant,

i.e., the warrant must describe ... the crime that has been, is being, or is about to be committed.") Here, all three warrants failed to provide the requisite particularity.

With respect to the April 19 warrant for the brothers' email accounts, the list of violations refers only to general statutes and does not provide a particular date, place, or occurrence when these violations took place, with a single exception: in the provision authorizing the seizure of "[a]ll communications pertaining to the Boston Marathon, explosives, bombs [.]" Exhibit A at p. 6 ¶ 2. That isolated mention cannot be interpreted as applying to all of the other provisions. Indeed, the fact that the other provisions do not mention the Marathon bombings or any other specific crime, coupled with the fact that one of the provisions refers to past or future attacks, suggests the opposite: that the other types of property or information listed may not relate to any violations of the listed statutes.

Although more of its provisions are tied to the Boston Marathon Bombing, the July 3 warrant for Mr. Tsarnaev's Gmail accounts suffers from the same deficiency. For example, the July 3 search warrant provides that the searcher may seize "[i]nformation related to the identity of any individuals who were in contact with, or were associates of Dzhokhar and Tamerlan[.]" Exhibit E at p. 5 ¶ II(i). Where the subject of the search is email accounts, the provision is tautological: all of the content is necessarily "related to the identity of any individuals who were in contact with, or were associates" of Mr. Tsarnaev. This untethered and unlimited provision effectively swallows the other search warrant provisions that limit the universe of seizeable items to the Boston Marathon and the violations set forth in the warrant.

The fact that the events are described in detail in the application and affidavit for the warrant does not save the generality of the description of the violations. None of the warrants issued by the Magistrate Judge incorporated the affidavits underlying the warrants. *United States v. Tiem Trinh*, 665 F.3d 1, 15 (1st Cir. Mass. 2011) (affidavit may be referred to for purposes of providing particularity only where it is incorporated into the search warrant by reference); *United States v. Roche*, 614 F.2d 6, 8 (1st Cir. 1980). Without resort to the affidavit, the warrant itself fails to provide any meaningful guidance to satisfy the particularity requirement:

> (T)he requirement that the warrant itself particularly describe the material to be seized is not only to circumscribe the discretion of the executing officers but also to inform the person subject to the search and seizure what the officers are entitled to take. . . .
>
> Moreover, self-restraint on the part of the instant executing officers does not erase the fact that under the broadly worded warrant appellees were subject to a greater exercise of power than that which may have actually transpired and for which probable cause had been established.

In re Application of Lafayette Academy, 610 F.2d 1, 5 (1st Cir. 1979).

When read together, the categories specified in each of the search warrants, generally similar throughout all three warrants, fail to provide sufficient limitations on what the agents could search for and seize. The "state of mind and/or motive" category, for example, is present in all three search warrants and could have been construed to allow the agents to examine or seize every email and every file in the Sony Vaio in the hope that it might shed light on the religious, political, or other beliefs of the Tsarnaev brothers, regardless of the actual subject matter and temporal relationship to the Boston Marathon Bombings. No temporal limitation of any kind is provided to cabin the

forensic searcher's discretion. *Cf. Lafayette Academy*, 610 F.2d at 5 n.4 (even a list of documents relating to a particular crime may be overly broad, as "efforts may also be required to narrow the documents by category, time periods and the like").

Similar deficiencies doom the provision permitting a search for evidence relating to "the identity of Tamerlan and Dzhokhar." Where every email and every file to be searched is personal and identifies Mr. Tsarnaev, the provision permits carte blanche seizure of *all* data. Thus, each of the warrants was, for all practical purposes, a general warrant that permitted an unfettered search for constitutionally protected information. The warrants were invalid and the evidence must be suppressed.

B. The Warrant Failed to Provide a Method, Such as a Filter Team, for Avoiding or Minimizing Sweeping Unauthorized Emails and Computer Data Into the Search

Even if the search warrants had established probable cause and the attachments had provided a measure of particularity, the failure to include a method for avoiding wholesale rummaging through the email content and computer files after seizing them ran afoul of the Fourth Amendment. The federal rules provide for a two-step procedure in regard to electronically stored information:

> A warrant [for property] may authorize the seizure of electronic storage media or the seizure and copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant.

Fed. R. Crim. P. 41(e)(2)(B). The rule thus contemplates the initial seizure of all e-mails contained in an individual's account and all data on a computer, more information than strictly necessary to further an investigation tied to the violations and categories specified in the warrant.

Courts have recognized that the second phase of the two-step procedure, where the government uses forensic investigators to cull the email and computer data to further their investigation, is fraught with risks and may require a neutral and detached procedure to avoid or at least minimize the unreasonable intrusion into Fourth Amendment protected areas. *United States v. Carey*, 172 F.3d 1268, 1275 & n.7 (10th Cir. 1999) (recommending a "special approach" to avoid discovering evidence outside the scope of the warrant in computer searches); *see also United States v. Hunter*, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) ("To withstand an overbreadth challenge, the search warrant itself, or materials incorporated by reference, must have specified the purpose for which the computers were seized and delineated the limits of their subsequent search."). Here, searching through *all* of Mr. Tsarnaev's email and computer data with only the modest guidance of the amorphous categories will necessarily sweep into the search email and computer files beyond their limited scope. In these circumstances, the warrant's failure to provide a filter team or some other method to enforce the particularity requirement by preventing or minimizing unauthorized intrusion in the Mr. Tsarnaev's constitutionally protected information renders the warrant invalid. *In re Applications for Search Warrants for Information Associated with Target Email Address*, 2012 WL 4383917 at *8 (D. Kan. 2012) (denying search warrant applications for email content where proposed warrants did not identify any sorting or filtering procedures to identify which emails were not relevant and did not fall within the scope of the government's probable cause statement).

Given this context, the warrant should have provided for examination of the email accounts and computer data, and segregation of the files particularly described in the warrant. *See* Nichole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E–Mail Surveillance*, 90 Neb. L. Rev. 971, 1014 -1016 (2012). Segregation should have been ordered to be executed by a filter-team consisting of agents or specially-trained computer personnel who are not involved in the investigation. *United States v. Comprehensive Drug Testing, Inc. (CDT II)*, 621 F.3d 1162, 1168 (9th Cir. 2010) ("the representation in the warrant that computer personnel would be used to examine and segregate the data was obviously designed to reassure the issuing magistrate that the government wouldn't sweep up large quantities of data in the hope of dredging up information it could not otherwise lawfully seize."). The warrant could have further ordered that the filter-team would be prohibited from communicating to the investigating agents any information gleaned from e-mails and files not described in the warrant. *See CDT II*, 621 F.3d at 1168-69. Once the e-mails for which the government has established probable cause have been isolated from other e-mails stored in an account, the investigating agents should be permitted to examine only the sought-after e-mails. *See id.*; *United States v. Tamura*, 694 F.2d 591, 595-96 (9th Cir. 1982) ("In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site . . .[t]he essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate."). *See also Dalia v. United States*, 441 U.S. 238, 246-248 (1979) (discussing the role of detached judicial officers in ensuring searches executed reasonably post search).

A filter procedure is a common-sense solution to the problem of necessarily over-seizing evidence, offering the government a safe harbor to have all of the evidence at its disposal while simultaneously protecting privacy and property rights in stored e-mail communications. *CDT II*, 621 F.3d at 1178, 1180 (Kozinski, C.J., concurring). *Accord, United States v. Payton*, 573 F.3d 859, 864 (9th Cir. 2009) (the nature of computers makes their searches so intrusive that judges issuing warrants may place conditions on the manner and extent of such searches, to protect privacy and other important constitutional interests).

Filter teams have been recognized by the Department of Justice to be a workable method of insuring that privileged electronic data not properly part of an investigation is segregated from investigating agents:

> When agents seize a computer that contains legally privileged files, a trustworthy third party must examine the computer to determine which files contain privileged material. After reviewing the files, the third party will offer those files that are not privileged to the prosecution team. Preferred practices for determining who will comb through the files vary widely among different courts. In general, however, there are three options. First, the court itself may review the files in camera. Second, the presiding judge may appoint a neutral third party known as a "special master" to the task of reviewing the files. Third, a team of prosecutors or agents who are not working on the case may form a "filter team" or "taint team" to help execute the search and review the files afterwards. The filter team sets up a so-called "ethical wall" between the evidence and the prosecution team, permitting only unprivileged files to pass over the wall.

Department of Justice Attorney Manual § 9-7.100 *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 110-11 (2009). The manual goes on to caution that "[a]gents contemplating a search that may result in the seizure of legally privileged computer files should devise a post-seizure strategy for screening out

the privileged files and *should describe that strategy in the affidavit*. *Id. (emphasis supplied)*. While defendant here does not claim that the data are privileged, there is no reason why a similar approach could not be used in a sweeping digital search.

In sum, the potential risk that agents would peruse private files that do not arguably fall under any legitimate portion of the search warrant is great in the case of electronically stored information where files are often intermingled. Due to the intrusiveness of searching and seizing the contents of stored e-mails and computer files, magistrate judges should place restrictions on the execution of warrants to ensure adherence to the Fourth Amendment. *Payton*, 573 F.3d at 864. In the absence of a neutral predetermination of the scope and breadth of stored e-mail and computer searches and seizures, "individuals [are] secure from Fourth Amendment violations 'only in the discretion of the police.'" *Katz v. United States*, 389 U.S. 347, 358-59 (*quoting Beck v. Ohio*, 379 U.S. 89, 97 (1964)). The failure of the warrant to include a method for that predetermination requires suppression of the fruits of the search.

III. THE TWO SEARCHES OF EMAIL CONTENT AND THE SEARCH OF THE SONY VAIO NECESSARILY EXCEEDED THE SCOPE OF THE SEARCH AUTHORIZED BY THE WARRANT, AND THE COURT MUST HOLD AN EVIDENTIARY HEARING TO DETERMINE WHETHER EMAILS AND COMPUTER DATA WERE IMPERMISSIBLY OBTAINED.

In considering whether a search of electronically stored information violated Fourth Amendment principles, "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Dalia*, 441 U.S. at 258; *United States v. Ramirez*, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis ... governs the method of execution of the

warrant."); *Hill*, 459 F.3d at 978 ("reasonableness of the officer's acts both in executing the warrant and in performing a subsequent search of seized materials remains subject to judicial review"). A search conducted in an unreasonable manner can be remedied after the fact, including through the sanction of evidence suppression. *Hudson v. Michigan*, 547 U.S. 586, 591 (2006).

Warrants for the contents of email accounts raise unique issues because the information is held by third party providers. As in the case of a computer seized by the government, a search warrant issued to a third-party provider – in this case, Yahoo and Google -- will result in disclosure of *all* information in its possession, regardless of whether the information fits within the particularized categories. Courts have recognized the difficulty of limiting electronic searches in the digital age. The Ninth Circuit has explained the problem:

> [The] 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 . . . . 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.
>
> Once a file is examined, however, the government may claim . . . that its contents are in plain view and, if incriminating, the government can keep it. Authorization to search some computer files therefore automatically becomes authorization to search all files in the same subdirectory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media.

United States v. Comprehensive Drug Testing, Inc., (CDT II), 621 F.3d 1162, 1176 (9th Cir. 2009) (en banc); *see also Carey*, 172 F.3d at 1275; Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 565-69 (2005). The Ninth Circuit called for judicial oversight to ensure that "[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *CDT II*, 621 F.3d at 1177.

Even if the affidavits in support of the warrants established probable cause to seize the entirety of Mr. Tsarnaev's email accounts and his computer (the did not, *see argument I above*), searches through *all* of the emails provided to the government by Yahoo and Google and *all* digital files on the Sony Vaio were outside the scope of a search properly limited to the search for evidence in the warrant's described categories.

The defense cannot presently determine whether the scope and methodology of the searches here resulted in unconstitutional searches and seizures of electronic data from the email accounts, computer data, or indeed any digital media. This is so because all information about the contours of the searches, as well as the possible trial evidence that resulted from the searches, is entirely within the control of the government, which continues to resist disclosure despite requests from the defense for disclosure. In regard to the search of Mr. Tsarnaev's Sony Vaio, for example, the defense by letter and motion has requested the Forensic Toolkit ("FTK") report of the examination of the computer; the government rejected the defense's letter request. The government has conceded that the FTK reports will necessarily delineate the contours of the searches that were, and perhaps continue to be, conducted on the seized items of digital evidence.

> Most of the FTK reports in this case were prepared at the prosecutors' request to explore and evaluate the usefulness of particular items of digital evidence in proving the defendant's guilt. Some were prepared to explore and evaluate possible criminal activity by others, or to search the digital evidence for possible leads.

D.E. 243 (Government's Opposition to Defendant's Motion to Compel) at 13. Clearly, the FTK reports, in conjunction with searchers' testimony at an evidentiary hearing, are crucial pieces of evidence as to whether the forensic searches exceeded the scope of the particularized categories authorized by the warrant.

Similarly, the defense by letter dated December 9, 2013, asked the government for notice under Fed. R. Crim. P. 12(b) (4) of its intent to use any evidence that the defendant may be entitled to discover under Rule 16. The need for this information is particularly acute with regard to the computer and email searches. The government has provided mirror images of the data seized, but the defense is left at a loss to know which of the terabytes of data will be offered at trial. Such notice would streamline the suppression proceedings and delineate the scope and parameters of the search conducted of both the Sony Vaio and of Mr. Tsarnaev's Yahoo and Gmail accounts. The government, however, responded by letter on February 7, 2014 that it

> has not yet identified all of the evidence that it intends to introduce in its case-in-chief, and it is too early for the government to rule anything out[.] Accordingly, at least for the time being, please treat everything that we have produced to you in discovery as something we may offer in our case-in-chief.

Given the breadth of the search warrants' categories, the government's disappointing response necessarily requires an evidentiary inquiry. The inquiry must determine whether the seemingly unrestricted forensic search of the entirety of Mr.

Tsarnaev's emails and computer violated his Fourth Amendment rights.[6] *See United States v. Fuccillo*, 808 F.2d 173, 177-178 (1st Cir. 1987) (search may be unreasonable in its execution as well as its scope). Email content that falls outside of the warrant must be suppressed regardless of the plain view doctrine. *See* Kerr, *supra*, 119 Harv. L. Rev. at 565-69; *CDT I*, 579 F.3d at 997–99 ("the government should, in future warrant applications, forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data. If the government doesn't consent to such a waiver, the magistrate judge should order that the seizable and non-seizable data be separated by an independent third party under the supervision of the court, or deny the warrant altogether."); *CDT II*, 621 F.3d at 1178 ("The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect."). *But see United States v. Crespo-Rios*, 645 F.3d 37, 43 (1st Cir. 2011) (computer search for "'chats' and other evidence of enticement" cannot be limited to "certain folders or types of files for keywords" because files may be mislabeled to hide their contents and a broader search is therefore appropriate). Similarly, emails falling outside of the particularized categories must be suppressed without resort to the good-faith exception of *United States v. Leon*,

[6] Of course, identification of data that were seized but will not be offered into evidence is not the end of the matter; that data may well have led the government to other evidence that it does intend to introduce, evidence that should be suppressed if it is the fruit of an unconstitutionally overbroad search of the digital evidence.

468 U.S. 897; *Fuccillo*, 808 F.2d at 177-178 (manner of execution rendered good-faith exception inapplicable).

In sum, the Fourth Amendment guards against unreasonable searches and seizures. The search warrants could not constitutionally permit a limitless search of all email and computer files, regardless of their content and whether they were connected to the specified violations. Where the extent of the forensic searches of Mr. Tsarnaev's email accounts and laptop are unclear, but where it appears that an unguided and unrestricted general rummaging occurred, the Court should conduct an evidentiary hearing to determine whether there were Fourth Amendment violations in the execution of the searches.

CONCLUSION

For the foregoing reasons, this Court must suppress from evidence at trial any substantive communications, or any fruits of such evidence, that were unlawfully seized by the government pursuant to search warrants directed to Yahoo! and Google for email communications and associated data, and similarly must suppress from evidence any electronic files and data unlawfully seized pursuant to a warrant authorizing the search of his Sony Vaio laptop computer.

Respectfully submitted,

DZHOKHAR TSARNAEV
By his attorneys

/s/ Timothy Watkins

Judy Clarke, Esq.
California Bar: 76071
CLARKE & RICE, APC
1010 Second Avenue, Suite 1800
San Diego, CA 92101
(619) 308-8484
JUDYCLARKE@JCSRLAW.NET

David I. Bruck, Esq. (SC Bar # 967)
220 Sydney Lewis Hall
Lexington, VA 24450
(540) 460-8188

Miriam Conrad, Esq. (BBO # 550223)
Timothy Watkins, Esq. (BBO # 567992)
William Fick, Esq. (BBO # 650562)
FEDERAL PUBLIC DEFENDER OFFICE
51 Sleeper Street, 5th Floor
(617) 223-8061
MIRIAM_CONRAD@FD.ORG
TIMOTHY_WATKINS@FD.ORG
WILLIAM_FICK@FD.ORG

Certificate of Service

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on May 12, 2014

/s/ Timothy Watkins