UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
[REDACTED]@MAC.COM
THAT IS STORED AT PREMISES
CONTROLLED BY APPLE, INC.

Magistrate Case. No. 14-228 (JMF)

SECOND MEMORANDUM OPINION AND ORDER

Pending before the Court is a Renewed Application for a search and seizure warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure and 18 U.S.C. § 2703(a), (b) and (c) to disclose certain records and contents of electronic communications relating to an Apple e-mail address.[1] See Affidavit in Support of an Application for a Search Warrant [#5-1] (sealed) at 1 (hereinafter Affidavit). In a previous Memorandum Opinion and Order,[2] this Court denied the government's original application for a search and seizure warrant for the same e-mail address without prejudice both because it failed to clearly specify which e-mails it sought to seize and because it sought authorization to seize e-mails for which it had not established probable cause to seize. In re Search of Apple E-mail, 2014 WL 945563, at *3, *5. The government's Renewed Application does not address these concerns and ignores the substance of this Court's previous rulings. The government persists in its attempt to seize an *entire* e-mail account and search through all of it. For the reasons stated below, the government's Renewed Application for a search and seizure warrant will, therefore, be denied.

[1] All references to the United States Code are to the electronic versions that appear in Westlaw or Lexis.
[2] See In the Matter of the Search of Information Associated with [redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc., Mag. Case No. 14-228, 2014 WL 945563 (D.D.C. Mar. 7, 2014) (hereinafter In re Search of Apple E-mail).

I. Background

This is the government's second attempt to obtain a search and seizure warrant for a specific Apple e-mail address as part of its investigation of a possible violation of 41 U.S.C. § 8702 (Solicitation and Receipt of Kickbacks) and 18 U.S.C. § 371 (Conspiracy) involving a defense contractor. Affidavit at 10. For purposes of this opinion, the details of the investigation—which remain under seal on the Court's docket—are irrelevant.[3]

In response to this Court's previous opinion in In re Search of Apple E-mail, the government has deviated from the standard format used to search e-mail accounts that is found in the Department of Justice's manual Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Department of Justice Criminal Division Computer Crimes and Intellectual Property Section, 255-262.[4] See In re Search of Apple E-mail, 2014 WL 945563, at *7 ("To be clear: the government must stop blindly relying on the language provided by the Department of Justice's Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations manual. By doing so, it is only submitting unconstitutional warrant applications."). In an "Attachment A," titled "Place to Be Searched," the government specifies the location of Apple, Inc. and indicates that the "warrant applies to information associated with the e-mail account [redacted]@mac.com dating from [January], 2014, to the present."[5] Affidavit at 12. An "Attachment B," titled "Particular things to be seized by the government," is as follows:

[3] This opinion addresses an investigatory tool related to an ongoing investigation, and the underlying documents must remain sealed for the time being. However, this opinion is intended to be—and shall be—made public, as it discusses the investigation in a sufficiently vague manner such as to avoid compromising the ongoing criminal investigation.

[4] A*vailable at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (last visited Mar. 29, 2014).

[5] The government's original application sought e-mails and records from December, 2013, until the present. See In re Search of Apple E-mail, 2014 WL 945563, at *1.

ATTACHMENT B

Particular things to be seized by the government

All emails, including email content, attachments, source and destination addresses, and time and date information, that constitute evidence and instrumentalities of violations of 41 U.S.C. § 8702 (Solicitation and Receipt of Kickbacks) and 18 U.S.C. § 371 (Conspiracy), dated between [January], 2014, to the present, including emails referring or relating to a government investigation involving any or all of the following: [Redacted list of names of companies and individuals in the form of "John Smith, John Smith, Inc., any current or former John Smith employees, etc."].

Id. at 13.

Finally, the government has included an "Attachment C," titled "Procedures to facilitate execution of the warrant":

ATTACHMENT C

Procedures to facilitate execution of the warrant

I. Information to be disclosed by Apple (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) [in January], 2014, the Provider is required to disclose the following information to the government for the account listed in Attachment A: all emails, including attachments, associated with the account, dating from [January], 2014, to the present, and 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.

Apple shall deliver the information set forth above via United States mail, courier, or email to: [The Department of Justice].

II. Government procedures for warrant execution

The United States government will conduct a search of the emails produced by the Provider and determine which are within the scope of the information to be seized specified in Attachment B. Those that are within the scope of Attachment B may be copied and retained by the United States.

Law enforcement personnel will then seal any information from Apple that does not fall within the scope of Attachment B and will not further review the information absent an order of the Court.

Affidavit at 14-15. Thus, the government requests that Apple provide all e-mails from a certain date in January, 2014, so that the government may search them for evidence of specific crimes and keep any non-relevant e-mails under seal until further order of a court.

II. Analysis

This is the third Memorandum Opinion from this Court regarding overbroad search and seizure warrants for data held by a third party provider of an electronic communications service. In September, the Court substantially modified a search warrant for the Facebook account of Navy Yard shooter Aaron Alexis to narrow its scope and prevent the government from retaining information that was irrelevant to its investigation. See In the Matter of the Search of Information Associated with the Facebook Account Identified by the Username Aaron. Alexis That Is Stored at Premises Controlled by Facebook, Inc., 2013 WL 7856600, at *8 (D.D.C. Nov. 26, 2013) (Facciola, M.J.) (hereinafter Facebook Opinion). In that Opinion, the Court implored the government to "seriously consider how to minimize the amount of information that its search warrant applications seek to be disclosed" because, as it stood, the government was requesting authorization to seize data for which it had not established probable cause. Id. at *8. In so doing, this Court recommended, *inter alia*, "[a]sking the electronic communications service provider to provide specific limited information such as emails or faxes containing certain key words or emails sent to/from certain recipients." Id. (citing In re Applications for Search Warrants for Case Nos. 12–MJ–8119–DJW and Information Associated with 12–MJ–9191–DJW Target Email Address, Nos. 12–MJ–8119, 12–MJ–8191, 2012 WL 4383917, at *10 (D.Ks. 2012) (hereinafter In re Search of Target Email Address)); see also Facebook Opinion at 2013 WL 7856600, at *8 (listing five measures the government could take to bring its warrant applications

in line with the requirements of the Fourth Amendment). Unfortunately, over the following four months, the government did not take any steps to modify their search warrant applications.

This Court's previous Memorandum Opinion in this matter was driven by two principal concerns.[6] First, the government's original application sought to seize an entire e-mail account even though it had only established probable cause for some of the e-mails. See In re Search of Apple E-mail, 2014 WL 945563, at *5. By doing so, the government asked this Court to issue a "general warrant that would allow a 'general, exploratory rummaging in a person's belongings'—in this case an individual's e-mail account." Id. (citing Coolidge v. N.H., 403 U.S. 443, 467 (1971)). Second, the government failed to explain what would occur with data that were seized but were outside the scope of the warrant application (and for which there was necessarily no probable cause to seize in the first place). In re Search of Apple E-mail, 2014 WL 945563, at *6. As a result, this Court was explicit that, "in light of the government's repeated submission of overly broad warrants that violate the Fourth Amendment, this Court can see no reasonable alternative other than to require the provider of an electronic communications service to perform the searches." Id.

The government's modifications in its Renewed Application fail to address the Court's concerns. In fact, the government has ignored the substance of the Court's warnings that its e-mail search warrant applications violate the Fourth Amendment. Although there are some cosmetic differences between the original application and the Renewed Application, the bottom line is that the government still gets *all* e-mails—regardless of their relevance to its investigation—and keeps them indefinitely. See Affidavit at 14-15. This is no different than what the government originally requested, and this Court still will not grant it.

[6] There were also serious drafting errors that raised questions about what the government actually intended to seize. These have now been corrected in the revised Attachment B. See In re Search of Apple E-mail, 2014 WL 945563, at *2-3.

A. The Government Still Seeks an Unconstitutional General Warrant

1. The Fourth Amendment Prohibits the Type of Warrant the Government Seeks

The Supreme Court has recognized two constitutional protections served by the warrant requirement of the Fourth Amendment. "First, the magistrate's scrutiny is intended to eliminate altogether searches not based on probable cause. The premise here is that any intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity." Coolidge, 403 U.S. at 467. Thus, it is this Court's duty to reject any applications for search warrants where the standard of probable cause has not been met. Second, "those searches deemed necessary should be as limited as possible. Here, the specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings." Id. To follow the dictates of the Fourth Amendment and to avoid issuing a general warrant, a court must be careful to ensure that probable cause exists to seize each item specified in the warrant application.

As this Court has previously noted, any e-mails that are turned over to the government are unquestionably "seized" within the meaning of the Fourth Amendment. See In re Search of Apple E-mail, 2014 WL 945563, at *5 (citing Brower v. Cnty. of Inyo, 489 U.S. 593, 596 (1989) (noting that a "seizure" occurs when there is "an intentional acquisition of physical control"). Although the Supreme Court has never specifically defined what constitutes a seizure in the electronic world, it has stated that, with regard to physical items, a "'seizure' of property only occurs when there is some meaningful interference with an individual's possessory interests in that property." United States v. Jacobsen, 466 U.S. 109, 113 (1984). In this Court's view, a seizure of property occurs when e-mails are copied and taken by the government without the owner's consent because an individual's "possessory interest [in the e-mails] extends to both the

original and any copies made from it." Orin Kerr, Fourth Amendment Seizures of Computer Data, 119 Yale L.J. 700, 703 (2010). After all, when a copy is made, "the person loses exclusive rights to the data," id., and it is at that time that the owner's property interest in the e-mail is affected. This reality has been assumed, if not stated outright, in the numerous cases that acknowledge that e-mails turned over to the government by an electronic communications service provider are "seized." See, e.g., In re Search of Target Email Address, 2012 WL 4383917, at *9; United States v. Taylor, 764 F. Supp. 2d 230, 237 (D.Me. 2011); United States v. Bickle, No. 10–CR–00565, 2011 WL 3798225, at *22 (D.Nev. July 21, 2011); United States v. Bowen, 689 F. Supp. 2d 675, 684 (S.D.N.Y. 2010).[7]

To conclude otherwise would yield unsatisfactory results.[8] First, if copying were not considered "seizing," that would suggest the irrelevance of the Fourth Amendment to that act:

> If copying data is not a seizure, then copying cannot logically be regarded as a search and it does not violate an expectation of privacy. It is possible to copy files without examining the files. Therefore, if copying is not a seizure, it is outside the scope of the Fourth Amendment's reasonableness requirements and is an activity which can be conducted at will, requiring neither the justification of a warrant nor an exception to the warrant requirement. This is not a satisfactory result. Copying has an effect upon the "ownership" rights of the party whose information is copied.

Susan Brenner and Barbara Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, 8 Mich. Telecomm. & Tech. L. Rev. 39, 113 (2002). Thus, this Court would have to believe that, if the act of copying e-mail is not a seizure, then the Fourth Amendment is powerless to prevent the wholesale copying of every single e-mail ever sent, a result that no court could ever reasonably embrace. It would also render hollow the Sixth Circuit's holding in

[7] On the other hand, one court has held that copying e-mail *does not* meaningfully interfere with a possessory interest "due to the nature of electronic information, which can be accessed from multiple locations, by multiple people, simultaneously." In re Application of the United States of America for a Search Warrant for Contents of Electronic Mail and for an Order Directing a Provider of Electronic Communication Services to not Disclose the Existence of the Search Warrant, 665 F. Supp. 2d. 1210, 1222 (D.Or. 2009).

[8] For a discussion of the relevant cases, which do not suggest a consistent approach, see Fourth Amendment Seizures of Computer Data, 119 Yale L.J. at 706-09.

United States v. Warshak, 631 F.3d 266, 285-88 (2010), that there is a reasonable expectation of privacy with respect to one's e-mails—even though those e-mails were copied by an electronic communications service provider and given to the government. Id. at 283.

Second, that approach suggests that a seizure could only occur if the actual hard drive that contains the target e-mail account, which is presumably in a server farm operated by Apple, is physically taken by the government. This ignores the reality that "[h]ardware is increasingly fungible" and that what really matters—and what the owner of the e-mails actually has a possessory interest in—"is the data." Fourth Amendment Seizures of Computer Data, 119 Yale L.J. at 712. A focus on hardware instead of data, in determining when a seizure occurs, would therefore miss the mark and ignore fundamental realities about how computers are actually used. See In re Southeastern Equipment Co. Search Warrant, 746 F. Supp. 1563, 1576 (S.D.Ga. 1990) ("As the LeClair Court pointed out, it is the information itself, not the paper and ink or tape recorder or other copying utensil, that is actually seized.") (citing LeClair v. Hart, 800 F.2d 692, 696 n.5 (7th Cir. 1986)).

Furthermore, the government itself characterizes the act of copying e-mails as a seizure by noting that it will "seize" some of the copied e-mails after the search is complete. See Affidavit at 13-15. It is, after all, seeking a "search and *seizure* warrant." See Fed. R. Crim. P. 41. Thus, even though the e-mails are only being copied by Apple (with other copies remaining on Apple's servers), a seizure is occurring. Because there is no principled distinction that suggests that copying data once is not a seizure but copying data twice is a seizure, it follows that the e-mails are seized the first time they are copied by Apple and given to the government. Any other position is unsatisfactory because the property interest in e-mails certainly suffers

"meaningful interference" when a third party has unauthorized access to those e-mails.[9] Thus, e-mails are seized when Apple gives them to the government just as surely as a physical letter is if it is taken by the postal service and given to the government. See Fourth Amendment Seizures of Computer Data, 119 Yale L.J. at 722-23.

The problem with the government's Renewed Application is not that it fails to specify with particularity what it intends to seize—and not that it suggests a seizure will not occur—but that it will *actually* seize large quantities of e-mails for which it has not established probable cause and which are outside the scope of Attachment B. The government asks Apple "to disclose the following information to the government for the account listed in Attachment A: all emails, including attachments, associated with the account, dating from [January], 2014, to the present . . ." Affidavit at 14. This Court has an affirmative obligation to "prevent[] the seizure of one thing under a warrant describing another." See Andresen v. Maryland, 427 U.S. 463, 479 (1976) (citing Stanford v. Texas, 379 U.S. 476, 485 (1965)). Here, the warrant describes only certain e-mails that are to be seized—and the government has only established probable cause for those e-mails. Yet it seeks to seize all e-mails by having them "disclosed" by Apple. This is unconstitutional because "[t]he government simply has not shown probable cause to search the contents of all emails ever sent to or from the account." See In re Search of Target Email Address, 2012 WL 4383917, at *9. As Judge David J. Waxse wisely analogized, if this were the physical world, it would be akin to "a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the

[9] One other absurd result bears mentioning: if copying e-mails did not interfere with the owner's possessory interests, then a cause of action for trespass to chattels would never accrue if e-mails were copied, again suggesting that private communications would be left essentially unprotected by the law. However, a cause of action for trespass to chattels arises when data is copied without authorization. See Oyster Software, Inc. v. Forms Processing, Inc., 2001 WL 1736382, at *13 (N.D.Ca. 2001) (holding that "copying . . . metatags" gives rise to a cause of action for trespass).

mail to find out whether it constitutes fruits, evidence or instrumentality of a crime. The Fourth Amendment would not allow such a warrant." Id. This Court agrees.

2. The Two-Step Procedure Is a Narrow Exception Due to Practical Considerations That Is Inapplicable Here

Nevertheless, there is a narrow exception that authorizes an otherwise unconstitutionally broad seizure if the *only* practical way to perform a search is to seize an entire repository, such as a file cabinet or computer, and take it offsite for a later search.[10] This is, in essence, the procedure outlined in United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982), where the Ninth Circuit deemed it acceptable to take a large quantity of documents offsite if the government explained that need to the magistrate. This two-step procedure—seize a large quantity of data and perform the specific search later at an offsite location—was later codified in Rule 41. See Fed. R. Crim. P. 41(e)(2)(B).

There is no question that the two-step procedure is constitutional under certain circumstances. See Facebook Opinion, 2013 WL 7856600, at *6 (citing cases holding that the two-step process under Rule 41 does not violate the Fourth Amendment). In fact, this Court has recently approved use of the two-step procedure in a series of opinions addressing the search of cell phones and hard drives—but only if the government provides an adequate search protocol explaining how it will perform the search and ensure that it is only searching sectors or blocks of the drives that are most likely to contain the data for which there is probable cause.[11] In those instances, the search protocol must "explain how [the government] is going to conduct this

[10] The question of what must happen with data that is seized and not within the scope of the warrant is discussed *infra*.

[11] See In the Matter of the Search of Apple iPhone, IMEI 013888003738427, Mag. Case No. 14-278, 2014 WL 1239702, at *6-7 (D.D.C. Mar. 26, 2014) (Facciola, M.J.) (hereinafter In re Apple iPhone); In the Matter of the Search of Odys Loox Plus Tablet, Serial Number 4707213703415, In Custody of United States Postal Inspection Service, 1400 New York Ave NW, Washington, DC, Mag. Case No. 14–265, 2014 WL 1063996, at *5-6 (D.D.C. Mar. 20, 2014) (Facciola, M.J.); In the Matter of the Search of Black iPhone 4, S/N Not Available, Mag. Case No. 14–235, 2014 WL 1045812, at *4 (D.D.C. Mar. 11, 2014) (Facciola, M.J.) (hereinafter In re Search of Black iPhone).

search to minimize the risk that files outside the scope of the warrant will be discovered." See In re Apple iPhone, 2014 WL 1239702, at *7.

The problem here, as previously pointed out by this Court, is that the government is "abusing the two-step procedure under Rule 41" by requiring Apple to disclose the entire contents of an e-mail account. See In re Search of Apple E-mail, 2014 WL 945563, at *5. A seizure unquestionably occurs once data is turned over from Apple to the government. See *supra*. The government cannot pretend that the seizure only occurs *after* it has searched and separated the relevant e-mails from the irrelevant ones. And the two-step Rule 41 process, which has essentially created a narrow exception to the general prohibition against seizing data for which there is no probable cause, is permissible only because there is no alternative that would allow the government to access the data for which it does have probable cause. See In re Search of Black iPhone, 2014 WL 1045812, at *4. The Court must emphasize that the two-step procedure is a *narrow* exception that requires an affirmative showing of need in the warrant application. The Renewed Application, however, fails to provide *any* explanation for why the two-step procedure is necessary.

3. By Requiring Apple to Perform the Search, the Court Avoids Issuing a General Warrant

Unlike a search of a hard drive or cell phone, there *is* an alternative that, in accordance with the Fourth Amendment, prevents the government from seizing large quantities of data for which it has not established probable cause: the electronic communication service provider, in this case Apple, can perform the search at the government's request and turn over any relevant data that it discovers. Otherwise, if the Court were to grant the Renewed Application as it is, the government would immediately seize a vast quantity of e-mails to which it is not entitled; in so doing, this Court would issue a general warrant, which it cannot do.

The Court fully understands that, in requiring a third party electronic communications service provider to perform the search that the government would otherwise perform, it is going a step further than—to its knowledge—any other court has. See Taylor, 764 F. Supp. 2d at 237 (the "Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching."); accord Bickle, 2011 WL 3798225, at *20 (but noting that "a filter process was mandated by Judge Foley to sort or filter privileged emails from non-privileged emails."); Bowen, 689 F. Supp. 2d at 682. But this Court reaches this conclusion out of exasperation that the government has, despite repeated warnings, refused to determine an alternative that does not involve the wholesale seizure of vast amounts of e-mails and other data protected by the Fourth Amendment to which it has no right. Unless the government can suggest an appropriate alternative, the Court can only conclude that the Fourth Amendment *does* require that the provider perform the search because nothing else will eliminate the present certainty that the government will unconstitutionally seize data for which it has not established probable cause to seize.

Cases involving searches and seizures of evidence held by third parties, such as Zurcher v. Stanford Daily, 436 U.S. 547, 559 (1978), do not suggest that this Court must take a different approach. In Zurcher, the Supreme Court held that a search and seizure warrant was the appropriate vehicle by which to obtain photographs held by a student newspaper that was itself not suspected of any wrongdoing. Id. at 551-52. That case addressed whether property held by a third party (not a suspect) could be searched and seized if it was nevertheless fruits, instrumentalities, or evidence of a crime. Id. at 559.[12] This Court does not disagree, and there is

[12] As the D.C. Circuit has held, "the tacit basis of the [Zurcher] decision" was that "the First Amendment offers no procedural or substantive protections against good faith criminal investigative activity beyond that afforded by the

no question that Apple, as the entity holding the target e-mails, may be served with a search and seizure warrant to turn over relevant e-mails.

Instead, there is a different question before this Court: can this Court order Apple to turn over e-mails that are necessarily outside the scope of the warrant and thus irrelevant? The answer is no. To hold otherwise would suggest that the Zurcher Court would have approved a search and seizure whereby the government entered the newspaper's office, copied every photograph, took them back to the station, and then searched through them to determine which ones were relevant to the investigation (and, as written, the Renewed Application would then have the police keep the non-relevant photographs indefinitely). Such a procedure would never be sanctioned because it would be precisely the type of "general, exploratory rummaging in a person's belongings" that the Fourth Amendment prohibits. Coolidge, 403 U.S. at 467. Given that third parties are permitted to assist in the execution of search warrants, see In re Search Warrant, 71 A.3d 1158, 1180 (Vt. 2012) (citing cases), it is certainly appropriate to have Apple perform the search when Apple's involvement is necessary to prevent a violation of the Fourth Amendment and limit the e-mails seized by the government.

B. The Government Has Failed to Even Suggest an Alternative to Having the E-mail Provider Perform the Search

Nothing in the Renewed Application even attempts to address the Court's rulings in In re Search of Apple E-mail, and the government makes no effort whatsoever to take advantage of Apple's technical expertise to perform the search in a way that will protect the target's Fourth Amendment rights. Instead, all the government has done is simply move the request that Apple "disclose . . . all emails, including attachments, associated with the account" from Attachment B

Fourth and Fifth Amendments." Reporters Comm. For Freedom of the Press v. American Tel. & Tel. Co., 593 F.2d 1030, 1055 (D.C. Cir. 1978). By contrast, the Court's ruling in this matter is based solely on the requirement of the Fourth Amendment that probable cause must exist to seize the materials specified in a warrant application.

to Attachment C. See Affidavit at 3. This obviously accomplishes nothing, and it indicates that the government is unwilling—for whatever reason—to give up its policy of seizing large quantities of e-mails and other Fourth Amendment protected data even after this Court has repeatedly warned it against doing so.

There may be circumstances in which it is not possible for the service provider to do the search. In such instances, in accordance with the principle of Tamura, practical considerations would necessitate that the government perform the search even if it means seizing—on a temporary basis—data for which it has not established probable cause. But that has not occurred here. Mere convenience does not allow the government to violate the Fourth Amendment and seize data wholesale.[13]

Here, the government has not even hinted that Apple cannot perform the search, let alone provided the Court with the evidence and sworn statements necessary to justify a wholesale seizure of the target Apple e-mail account. Instead, this Court has been presented with the same defective and unconstitutional request for a search and seizure warrant. This Court cannot issue it.

C. The Government Cannot Keep Data it Knows Is Outside the Scope of the Warrant

In its Renewed Application, the government first asks this Court to order Apple to turn over data for which the government knows it has not established probable cause; after it performs a search, it then wants to "seal any information from Apple that does not fall within the scope of Attachment B and [] not further review the information absent an order of the Court."

[13] Even if the government were to identify practical considerations that make a search by a service provider impossible, it would still need to provide this Court with an adequate search protocol so that the Court can be assured that the government is "limit[ing] the possibility that locations containing data outside the scope of the warrant will be searched" in line with the particularity requirement of the Fourth Amendment. In re Apple iPhone, 2014 WL 1239702, at *6. The Renewed Application provides no search protocol whatsoever.

Affidavit at 15. Such a request is inconceivable—and unacceptable—given the Court's repeated statements on this specific issue. In September and December 2013,[14] the Court modified approximately twenty warrants to specify that any data not within the scope of the warrant would be returned or, if copies, destroyed within a reasonable period of time. See Memorandum Opinion, 2014 WL 945563 at *3, *7. Moreover, through no less than *five* separate published opinions—four of them in the past month—this Court has made clear that any position short of "[a]ny information discovered on the Device to be seized which falls outside of the scope of this warrant will be returned or, if copied, destroyed within a reasonably prompt amount of time after the information is identified" is unacceptable. See In re Search of Apple iPhone, 2014 WL 1239702, at *5.

The government's apparent source for suggesting that it will "seal" the irrelevant e-mails until this Court orders otherwise is Tamura, where the Ninth Circuit said that "[g]overnment and law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search . . ." 694 F.2d at 595. Taken out of context, this quote appears to authorize the government's suggestion in its Renewed Application—but it does not. Tamura authorized the sealing pending further court order *only* "[i]n the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site." Id. That is not the issue here. Tamura does, however, serve as a useful reminder that it is illegal for the government to "refus[e] to return the seized documents not described in the warrant . . ." Id. at 596.

Here, the government implies that it will keep data indefinitely that it knows is outside the scope of the warrant. To return to the example from Zurcher, the government's position is akin to indefinitely keeping all copies of a newspaper's photographs merely because one or two

[14] This Court has a monthly criminal rotation once every three months.

may show evidence of a crime. For the *sixth* time, this Court must be clear: if the government seizes data it knows is outside the scope of the warrant, it must either destroy the data or return it. It cannot simply keep it.[15]

III. Conclusion

The government did not appeal the Court's ruling in In re Search of Apple E-mail, but it has all but ignored that ruling and merely engaged in cosmetic modifications by moving some unconstitutional language from Attachment B to Attachment C. The end result is, of course, no different. The government wants to seize the target's entire e-mail account, search through it for relevant data, and then keep indefinitely the irrelevant data that is outside the scope of the warrant. There is no question that the Renewed Application violates the Fourth Amendment, and this Court *cannot* issue it.

It is, therefore, hereby **ORDERED** that the government's Application is **DENIED**.

SO ORDERED.

[15] The exception to this admonishment is for evidence that falls within the plain view exception of the Fourth Amendment. See Horton v. California, 496 U.S. 128, 133-34 (1990). The potential for abuse of the plain view exception with respect to electronic data is great and has generated a great deal of discussion. For at least the last nine years, Professor Orin Kerr has advocated abolishing the plain view exception for digital searches. See Orin Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 582-83 (2005). Judge Alex Kozinski has suggested that magistrate judges should "insist that the government waive reliance upon the plain view doctrine in digital evidence cases." United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1180 (9th Cir. 2010) (Kozinski, J., concurring). However, the Vermont Supreme Court, in one of the few appellate opinions to carefully address the issue of *ex ante* warrant restrictions, has held that a magistrate has no authority to "alter what legal principles will or will not apply in a particular case." In re Search Warrant, 71 A.3d at 1174. There is another problem with relying on a waiver of the plain view doctrine to cure a problem of overseizure: the government will still have the data and, even if it does not directly use it as evidence for a criminal prosecution, it may use it for other purposes. In other words, this creates the problem that the data may be put into a larger database that would be ripe for abuse. Even if outright abuse does not occur, there is always the risk of troubling uses such as "parallel construction," where illegal or secret criminal investigations are recreated in a manner that is seemingly consistent with the Constitution without informing the accused or the court. See Hanni Fakhoury, DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations, Electronic Frontier Foundation, *available at* https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering (last visited Mar. 30, 2014). In light of this, the more prudent course of action is to require the government to destroy any data that it knows is outside the scope of the warrant.

Digitally signed by John M. Facciola
DN: c=US, email=john_m._facciola@dcd.uscourts.gov, o=United States District Court for the District of Columbia, cn=John M. Facciola
Date: 2014.04.07 08:48:05 -04'00'

JOHN M. FACCIOLA
UNITED STATES MAGISTRATE JUDGE