UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
APPLE IPHONE, IMEI 013888003738427 Magistrate Case No. 14-278 (JMF)

MEMORANDUM OPINION AND ORDER

Pending before the Court is an Application for a search and seizure warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure for an Apple iPhone 4. See Affidavit In Support of Application for Search Warrant at 6 (hereinafter the "Affidavit").[1] In response to this Court's recent rulings with respect to the proper scope of searches of electronic devices,[2] the government has provided a detailed "Attachment B"—which lists the items to be seized from the iPhone—and a new section, entitled "Electronic Storage and Forensic Analysis" (hereinafter "Forensic Analysis section"). See Affidavit at 10-15. Although Attachment B provides a sufficiently particularized list of the data that the government will search for and seize, the Forensic Analysis section fails to provide this Court with the same level of detail as to the methodologies to be used to conduct the search. Specifically, the government fails to articulate how it will limit the possibility that data outside the scope of the warrant will be searched. For the reasons stated below, the government's Application for a search and seizure warrant will, therefore, be denied.

I. Background

The government's Application is part of its investigation of Daniel Milzman, a Georgetown University student suspected of creating ricin in his dorm room in violation of 18

[1] Because the Clerk's office does not index filings on ECF for a search warrant application until after an order has been issued granting or denying an application, this opinion cannot reference specific ECF filing numbers.
[2] See In the Matter of the Search of Black iPhone 4, S/N Not Available, Mag. Case No. 14-235, 2014 WL 1045812 (D.D.C. Mar. 11, 2014) (Facciola, M.J.) (hereinafter In re Search of Black iPhone); see also 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 (D.D.C. Mar. 20, 2014) (Facciola, M.J.) (hereinafter In re Search of Odys Loox).

U.S.C. § 175.[3] See Affidavit at 3-4. Pursuant to a search and seizure warrant issued by this Court on March 18, 2014, see In the Matter of the Search of the Premises Located at Georgetown University [REDACTED], Mag. Case No. 14-263 (sealed), the government seized the iPhone at issue.[4] In that warrant, the Court interlineated a requirement that a separate search and seizure warrant must be obtained to actually search the *contents* of the iPhone. See Id., Mag. Case No. 14-263 [#4] at 5-6.

The government has now returned for that subsequent search and seizure warrant. Pursuant to a standard format used by the government, the Application contains an "Attachment A," which describes the device to be searched, and Attachment B, which lists the specific data to be seized. See Affidavit at 13-15. Specifically, Attachment B says:

ATTACHMENT B

LIST OF ITEMS AUTHORIZED TO BE SEARCHED FOR AND SEIZED PURSUANT TO FEDERAL SEARCH WARRANT AT THE TARGET RESIDENCE

1. All records on the Device described in Attachment A that reference or relate to violations of Title 18, United States Code, Section 175 (development, production, stockpile, transfer, acquisition, retention, or possession of a biological agent, toxin, or delivery system) and involve DANIEL HARRY MILZMAN, including:

   a. Records of or information about the Device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

   b. Records of activities relating to the operation and ownership of the Device, such as telephone incoming/outgoing call records, notes (however and wherever written, stored, or maintained), electronic books, diaries, and reference materials.

   c. Records of address or identifying information for DANIEL HARRY MILZMAN and (however and wherever written, stored,

[3] All references to the United States Code are to the electronic versions that appear in Westlaw or Lexis.

[4] The Affidavit states that the government conducted a consent search of Milzman's dormitory room and then seized the phone. See Affidavit at 6. However, this Court issued a warrant for its seizure the same day.

or maintained) contact lists, user IDs, eIDs (electronic ID numbers), and passwords.

d. Any digital images documenting, referencing, or related to the production, storage, or dissemination of biological agents, toxins, or delivery systems;

e. GPS data stored on the Device to include the Device's location and search history;

f. Any records of activity indicative of purchases potentially related to materials used in the production and/or storage of biological agents, toxins, or delivery systems;

g. Evidence of user attribution showing who used or owned the Device during the time the violation described in this warrant is suspected of being committed, such as logs, phonebooks, saved usernames and passwords;

h. Any communications referencing or relating to the production or possession of ricin, to include text messages and e-mails;

2. Records evidencing the use of Internet Protocol addresses, including:

a. Records of specific Internet Protocol addresses used and accessed;

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored.

4. Contextual information necessary to understand the evidence described in this attachment.

Id. at 14-15.

For the first time in this Court's experience, the government has also included a Forensic Analysis section. That section provides:[5]

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device to be seized was used, the purpose of its use, who

[5] The numbered paragraphs reflect the original numbering in the Affidavit. For the sake of completeness, the entire Forensic Analysis section is reproduced in full.

used it, and when. There is probable cause to believe that this forensic electronic evidence might be on this Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

25. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant, noting the following:

    a. The examination will be conducted jointly between investigators and an FBI technical review team with subject matter expertise in reviewing and analyzing electronic devices. The length of such examinations will vary greatly depending on the amount of data on the Device and the scope of the search authorized.

    b. Traditionally used forensic methods to target information specifically related to an offense, such as keyword searches for related terms, are not compatible with all types of files and applications on the Device. Therefore the examination may require authorities to employ techniques including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

    c. The process of identifying the exact files, application data, registry entries, logs, or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on the Device to be seized is evidence may depend on other information stored on the Device and the application of knowledge about how the Device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

26. Data outside the scope of the warrant. Any 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.

27. Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

28. Therefore, it is respectfully requested that the warrant sought by this application explained above, and further authorize a full physical and forensic examination of the seized items at a secure location.

Affidavit at 10-12.[6]

II. Analysis

In In re Search of Black iPhone and In re Search of Odys Loox, two opinions issued by this Court over the past two weeks, the Court admonished the government to explain how it intends "to search for each thing it intends to seize [and] how it will deal with the issue of intermingled documents." In re Search of Black iPhone, 2014 WL 1045812, at *4.[7] The government has made some improvements in its current Application, yet it still fails to satisfy the particularity requirement of what will be searched and fails to fully explain to the Court how much data for which it does not have probable cause will likely be seized. The only way to address these issues is for the government to provide the Court with its search protocol, which would explain how the search will occur.

A. The Constitutional Basis for the Court's Concerns

The concerns raised by the Court in this opinion, which are repeated in In re Search of Odys Loox, are based on the probable cause and particularity requirements of the Fourth Amendment.[8] The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants

[6] The affiant is Special Agent David Goldkopf of the Federal Bureau of Investigation. See Affidavit at 1. He uses the first person throughout the entire affidavit.

[7] The Court has also raised concerns about overbroad search warrant applications that failed to limit the data the government intended to seize to the data for which it had established probable cause to seize. See In re Search of Black iPhone, 2014 WL 1045812, at *2-3. The government's revised Attachment B in both the present matter and in In re Search of Odys Loox, 2014 WL 1063996, at *2, have corrected these deficiencies. In particular, the Attachment B in this case represents a paragon of what an Attachment B should be: it leaves no doubt as to what the government intends to seize and uses clear descriptions. See Affidavit at 14-15.

[8] The issue of particularity of items to be seized, which is addressed in footnote 7 and fixed by this Application's Attachment B, is firmly rooted in the requirement that warrants must particularly describe the "things to be seized." U.S. Const. amend. IV.

> 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. Items, such as data, can only be seized if there is probable cause to support their seizure. See Coolidge v. N.H., 403 U.S. 443, 467 (1971). With respect to the particularity requirement, the Supreme Court has recognized that it "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." Maryland v. Garrison, 480 U.S. 79, 84 (1987). As a result, "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 (citing United States v. Ross, 456 U.S. 798, 824 (1982)). The Court remains concerned that, in its current form, the government's Application violates both of these provisions.

1. Oversiezure Remains a Problem, Violating the Requirement of Probable Cause

In its previous two opinions, the Court was concerned about the overseizure of data for which there was no probable cause. As written, the government's application indicated that it would take and sift through massive amounts of data for which it had no probable cause to seize in the first place. See In re Search Black iPhone, 2014 WL 1045812, at *4-5. The Court thus required an intended search protocol so that it could better understand the scope of the warrant it was asked to issue. Whether the target devices would be imaged in full, for how long those images will be kept, and what will happen to data that is seized but is ultimately determined not

to be within the scope of the warrant—or, more precisely, Attachment B—can only be addressed by a search protocol; after all, the imaging actually occurs as part of the search process.

The government failed to adequately address this issue in In re Search of Odys Loox because it indicated that it would "image these devices and store them until the target/ defendant's appeals and habeas proceedings are concluded." 2014 WL 1063996, at *5 (internal quotation and citation omitted). The government was therefore admitting that, even though it had probable cause for only some of the data on the devices, it intended to keep all of the data for an indefinite period of time. That would constitute an unconstitutional seizure, which this Court could not permit. See United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982) ("However, the wholesale seizure for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as 'the kind of investigatory dragnet that the fourth amendment was designed to prevent.'") (citing United States v. Abrams, 615 F.2d 541, 543 (1st Cir. 1980)).[9]

The present Application has largely, but not entirely, solved this problem. The government's position is now:

> Data outside the scope of the warrant. Any 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.

Application at 11. This answers the question of what will happen to the data that the government, having finished its search, determines is outside the scope of Attachment B and thus outside the scope of the warrant. The Court's only remaining quibble is that, unlike in In re Search of Odys Loox, the government does not specify here that the iPhone will be imaged. This is important because, if the device will be imaged, then there will be a complete copy of all its data—

[9] Certainly, the data is, in one sense, already seized because the device is seized. The device, however, was seized pursuant to an earlier warrant issued by this Court.

including the data for which there is no probable cause to seize—that must be accounted for and which ultimately must be purged of data outside the scope of the warrant. As a practical matter, the Court cannot imagine that an image would not be created, so the government must clarify this aspect and make clear in its applications that the non-relevant data will be deleted from any system images. Including such a statement in a search protocol would address this concern. See United States v. Hill, 459 F.3d 966, 976-77 (9th Cir. 2006) (holding overbroad a warrant authorizing the "blanket seizure" of computer storage media without sufficiently explaining the process—in that case removing all storage media offsite—to the issuing magistrate).

2. A Search Protocol Is Needed to Address the Particularity of the Place to Be Searched

The Court also requires a search protocol for a separate Fourth Amendment reason—to particularly describe the place to be searched. In a broad manner, describing the iPhone and its specific IMEI number certainly describes the "place to be searched" in a particular manner. But an electronic search is not that simple. An iPhone 4 has either 16 GB or 32 GB of flash memory,[10] which could allow storage of up to around two million text documents.[11] Obviously no one—especially not a college student—would fill an iPhone with text documents, but it is inconceivable that the government would go file by file to determine whether each one is within the scope of the warrant. Instead, as the government has explained in extremely general terms, it will use some sort of "computer-assisted scans" to determine *where* to look because those scans will determine which parts will be exposed "to human inspection in order to determine whether it is evidence described by the warrant." Affidavit at 11. Thus, a sufficient search protocol, *i.e.* an explanation of the scientific methodology the government will use to separate what is permitted

[10] See iPhone 4 – Technical Specifications, *available at* http://support.apple.com/kb/sp587.
[11] See How Many Pages in a Gigabyte?, *available at* www.lexisnexis.com%2Fapplieddiscovery%2Flawlibrary%2Fwhitepapers%2Fadi_fs_pagesinagigabyte.pdf.

to be seized from what is not, will explain to the Court how the government will decide where it is going to search—and it is thus squarely aimed at satisfying the particularity requirement of the Fourth Amendment.

In drawing this conclusion, the Court finds persuasive the 2012 opinion from the Supreme Court of Vermont, which authorized *ex ante* restrictions on search warrants because "the only feasible way to specify a particular 'region' of the computer will be by specifying how to search." In re Search Warrant, 71 A.3d 1158, 1171 (Vt. 2012). This also distinguishes the Court's requirement for a search protocol from cases like Dalia v. United States, 441 U.S. 238, 257-58 (1979). In that case, the government obtained a warrant to bug the petitioner's office, but it did not specify in the warrant application that the bug would be planted surreptitiously. Id. at 242, 245. Although petitioner argued that the warrant failed "to specify that it would be executed by means of a covert entry of his office," the Supreme Court was unpersuaded that the Fourth Amendment requires an issuing court to "set forth precisely the procedures to be followed by the executing officers" because "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." Id. at 257-58.

Unlike in Dalia, however, this Court is not requiring a search protocol so that it may specify how the warrant is to be executed. Instead, the protocol will explain to the Court how the government intends to determine where it will search (which "parts"—or blocks—of the iPhone's NAND flash drive)[12] and how those decisions with respect to how the search will be conducted will help limit the possibility that locations containing data outside the scope of the warrant will be searched (which is the intermingled documents problem, see In re Search Black

[12] See NAND Flash 101: An Introduction to NAND Flash and How to Design It in Your Next Product ("The NAND Flash array is grouped into a series of blocks, which are the smallest erasable entities in a NAND Flash device."), *available at* www.micron.com%2F-%2Fmedia%2FDocuments%2FProducts%2FTechnical%2520Note%2FNAND%2520Flash%2Ftn2919_nand_101.pdf

iPhone, 2014 WL 1045812, at *4). Instead of identifying specific blocks of the iPhone's flash drive will be searched ahead of time—which would be impossible—the Court is instead asking the government to explain its methodology for determining, once it is engaged in the search, how it will determine which blocks should be searched for data within the scope of the warrant. See In re Search Warrant, 71 A.3d at 1171. This is a subtle but, depending on one's interpretation of the breadth of Dalia, constitutionally significant distinction.

One other point is worth noting. In the physical world, a search of an entire file cabinet or building for a particular document is constitutionally permissible only because there is no way to know with any certainty ahead of time how the search location can be narrowed so that only the specific folder containing the document will be searched. See United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009) ("One would not ordinarily expect a warrant to search filing cabinets for evidence of drug activity to prospectively restrict the search to 'file cabinets in the basement' or to file folders labeled 'Meth Lab' or 'Customers.'"). In such instances, the textual admonitions of the Fourth Amendment must give way to the practical reality of how the search must be conducted. Tamura, 694 F.2d at 595 ("It is true that all items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search.").

The digital world however, is entirely different. For example, sophisticated search tools exist, and those search tools allow the government to find specific data without having to examine every file on a hard drive or flash drive. When searching electronic devices to seize the data, the potential for abuse has never been greater: it is easy to copy them and store thousands or millions of documents with relative ease. But, by using search tools, there is also the potential

for narrowing searches so that they are more likely to find only the material within the scope of the warrant. It is, of course, also in the government's best interest to do so, as it would be a waste of resources to, for example, search file by file looking for data in the scope of the warrant—assuming that, on a 16 or 32 GB flash drive, it is even possible to do so and ever finish the search.

a. The Government Has Still Not Provided a Search Protocol

All the Court is asking the government to do is explain how it is going to conduct this search to minimize the risk that files outside the scope of the warrant will be discovered. As the Ninth Circuit has made clear, "the reality that over-seizing is an inherent part of the electronic search process" requires this Court to "exercise 'greater vigilance' in protecting against the danger that the process of identifying seizable electronic evidence could become a vehicle for the government to gain access to a larger pool of data that it has no probable cause to collect." United States v. Schesso, 730 F.3d 1040, 1042 (9th Cir. 2013) (citing United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam)). This Court agrees with that court's reasoning, and an appropriate search protocol is the answer to protecting against the government searching data on an electronic device when it has no right to search that data.

The government searches hard drives and cell phones on a regular basis—this Court is aware of this fact because warrant applications for these devices are a regular occurrence. Furthermore, the government has already told the Court that it uses some methods such as "keyword searches for related terms" and "computer-assisted scans." Affidavit at 11. These statements are a useful step in the right direction, but they still do not actually give the Court a *search protocol* as the Court has defined the term. In the Court's view, the government's

statement that it will use a "computer-assisted scan" is equivalent to saying, in Attachment B, that it will seize "all records" relevant to a particular crime. It tells the Court nothing about what will actually happen and does not provide a means of searching so that this Court is assured that it is the type of particularized search that the Fourth Amendment demands. What the government has submitted is no better than the vague explanation in In re Search of Odys Loox that it will "image each device, search them, and keep all files." 2014 WL 1063996, at *5.

b. The Government Must Provide a Search Protocol

The government need only tell the Court what it already intends to do and what it does in every other similar search of an iPhone. The government should not be afraid to use terms like "MD5 hash values," "metadata," "registry," "write blocking" and "status marker," nor should it shy away from explaining what kinds of third party software are used and how they are used to search for particular types of data. The Court is *not* dictating that particular terms or search methods should be used. Instead, the Court is attempting to convey that it wants a sophisticated technical explanation of how the government intends to conduct the search so that the Court may conclude that the government is making a genuine effort to limit itself to a particularized search. See In re Search of Odys Loox, 2014 WL 1063996, at *5.

This is the third time the Court has asked the government for this explanation, and the government should provide it. Any concerns about being locked into a particular search protocol are unnecessary for two reasons. First, the government can always return for additional authorization of this Court as needed. Second, the application need only explain that some searches require additional techniques and that what is proposed is merely *what the government intends to do at the time it submits its application, based on its experience searching such devices and in light of the particular data it seeks to seize.*

III. Conclusion

The government has solved the problem of a lack of particularity with respect to the items specified in Attachment B, and, with a few modifications, its Application could satisfy the Court that it will not keep seized data that it knows fall outside the scope of the warrant and for which it has no probable cause to seize. Until the government actually explains how the search will proceed, and thus how the government intends to limit its search of data outside the scope of the warrant, this warrant cannot be issued.

For the reasons stated above, it is hereby **ORDERED** that the government's Application is **DENIED** without prejudice.

SO ORDERED.

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: 2014.03.26 10:30:00 -04'00'

JOHN M. FACCIOLA
UNITED STATES MAGISTRATE JUDGE