UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF BLACK IPHONE 4, S/N NOT AVAILABLE	Magistrate Case No. 14-235 (JMF)
IN THE MATTER OF THE SEARCH OF SAMSUNG SGH-T989 AKA GALAXY S II CELLULAR TELEPHONE IMEI 359858/04/531905/8, S/N R31CC12PDBN	Magistrate Case No. 14-236 (JMF)
IN THE MATTER OF THE SEARCH OF SAMSUNG SGH-S150G CELLULAR TELEPHONE, BLACK IN COLOR, IMEI 564082/05/308324/2, S/N R21D5951DTV	Magistrate Case No. 14-237 (JMF)
IN THE MATTER OF THE SEARCH OF WESTERN DIGITAL TV, S/N WNT291019173	Magistrate Case No. 14-238 (JMF)
IN THE MATTER OF THE SEARCH OF WESTERN DIGITAL HARD DRIVE, S/N WCAUK1341857	Magistrate Case No. 14-239 (JMF)
IN THE MATTER OF THE SEARCH OF WESTERN DIGITAL MYBOOK ESSENTIAL HARD DRIVE, S/N WCAZA5015009	Magistrate Case No. 14-240 (JMF)

MEMORANDUM OPINION AND ORDER

Pending before the Court are six Applications for search and seizure warrants pursuant to Rule 41 of the Federal Rules of Criminal Procedure for various electronic devices that were seized in a hotel room in Solomons, Maryland. See Affidavit In Support of Search Warrant at 8 (hereinafter the "Affidavit").[1] Three of these Applications use inaccurate, formulaic language; the other three fail to limit the scope of the search and seizure to data for which there is probable

[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

cause and do not provide the Court with any indication of how the search will be conducted. For the reasons stated below, the government's Applications for search and seizure warrants will be denied.

I. Background

Each of the six Applications is based on the same Affidavit,[2] and each pertains to an investigation of the distribution and possession of child pornography. According to the Affidavit, an undercover officer communicated with a suspect and eventually arranged to meet him at a Holiday Inn in Solomons, Maryland. Affidavit at 6-7. Pursuant to a search warrant executed on that hotel room, the government seized: 1) an iPhone 4; 2) a Samsung SGH-T989 cell phone; 3) a Samsung SGH-S150G cell phone; 4) a Western Digital TV; 5) a Western Digital hard drive; and 6) a Western Digital Mybook Essential hard drive. Id. at 8. Each Application seeks a search and seizure warrant that will permit the government to search these devices because the government believes they contain "evidence of the distribution and possession of child pornography" in violation of 18 U.S.C. §§ 2252(A)(2) and 2252A(a)(5)(B).[3]

Using a standard format, each Application contains an "Attachment A" that describes the device to be searched and an "Attachment B," which lists "Specific Items to Be Seized." Affidavit at 11. Each Attachment B is identical:

ATTACHMENT B

SPECIFIC ITEMS TO BE SEIZED

All records contained in the cellular telephones listed in Attachment A, including:

1. Any information, including text and instant messages, relating to the transportation, travel, enticement, or sexual conduct involving a minor;
2. Evidence of user attribution showing who had dominion, ownership, custody, or control of the device at the time the communications described in this

[2] The only difference between each Affidavit is that each has a different device described on the second page.

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

warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records and things evidencing the use of any Internet Protocol address to communicate with the victim or her parents through e-mail or text, including:
   (a) records of Internet Protocol addresses used;
   (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, files uploaded and records of user-typed web addresses.
4. Any and all list of names, telephone numbers, and addresses stored as contacts to include pictures.
5. Any and all names of persons [sic] has contacted recently contacted [sic] through calls and text messages.
6. Images, pictures, photographs sent or received by user.
7. The content of any and all text messages sent or received by user.
8. The content of any and all voice mail messages.
9. All visual depictions of children, engaging in sexually explicit conduct, as defined in Title 18 U.S.C., § 2256, and child erotica, clothed or unclothed.
10. Any and all evidence of passwords needed to access the user cell phone.

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, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Affidavit at 11.

II. Inaccurate Boilerplate Language in Magistrate Case Nos. 14-238-40

In the government's Applications, the purpose of Attachment B is to specify what the government will actually seize from each device. See Affidavit at 11 (entitled "Specific Items to Be Seized"). Three of the Applications are for cell phones,[4] and the other three are for hard drives.[5] However, Attachment B is identical for each device, regardless of its use and function.

Despite this, it is evident to the Court that the Attachment B used in these Applications is only applicable to cell phones. Attachment B asks for "All records contained in the cellular telephones . . ." Id. It also specifies that the government will seize specific information including, *inter alia*, "text and instant messages," "names, telephone numbers, and addresses," "[t]he

[4] Magistrate Case. Nos. 14-235-237.
[5] Magistrate Case. Nos. 14-238-240.

content of any and all text messages" and "[t]he content of any and all voice mail messages." Id. Because the government has clearly submitted the wrong Attachment B for Magistrate Case Nos. 14-238-240, those warrants must be denied. The government has once again used formulaic language without careful review. See In the Matter of the Application of the United States of America for an Order Authorizing Disclosure of Historical Cell Site Information for Telephone Number [Redacted], 1:13-MC-199, 1:13-MC-1005, 1:13-MC-1006, 2013 WL 7856601, at *4 (D.D.C. Oct. 31, 2013) (Facciola, M.J.) ("Generic and inaccurate boilerplate language will only cause this Court to reject future § 2703(d) applications.").

III. The Government's Applications Are Overbroad

With respect to the three Applications that do have an appropriate Attachment B, the government seeks to seize data that are outside the scope of its investigation and for which it has not established probable cause. The government is investigating the distribution and possession of child pornography. Some of the items listed in Attachment B that it wishes to seize, such as items 1,[6] 2,[7] 3,[8] 9,[9] and 10,[10] are appropriately within the scope of its investigation.[11] Based on the Application, it has established probable cause for those items.

The government has not, however, established probable cause for the broad seizure of data in items 4,[12] 5,[13] 6,[14] 7,[15] and 8.[16] With one simple modification, these Applications would

---

[6] 1. Any information, including text and instant messages, relating to the transportation, travel, enticement, or sexual conduct involving a minor;

[7] 2. Evidence of user attribution showing who had dominion, ownership, custody, or control of the device at the time the communications described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

[8] 3. Records and things evidencing the use of any Internet Protocol address to communicate with the victim or her parents through e-mail or text, including: (a) records of Internet Protocol addresses used; (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, files uploaded and records of user-typed web addresses.

[9] 9. All visual depictions of children, engaging in sexually explicit conduct, as defined in Title 18 U.S.C., § 2256, and child erotica, clothed or unclothed.

[10] 10. Any and all evidence of passwords needed to access the user cell phone.

[11] These "items" refer to the numbered entries on Attachment B. See Affidavit at 11.

[12] 4. Any and all list of names, telephone numbers, and addresses stored as contacts to include pictures.

have avoided the overbreadth problem: seize this information only insofar as it pertains to violations of 18 U.S.C. §§ 2252(A)(2) and 2252A(a)(5)(B). However, no such limitation currently exists. Instead, the government apparently seeks to seize the entirety of these phones, including all communications, regardless of whether they bear any relevance whatsoever to this investigation. If this were not the intention, then Attachment B would not begin by saying that the government wishes to seize "[a]ll records . . . including . . ."; by using the term "including," the Applications make the seizure list broader than the categories that are specifically listed. Affidavit at 11.[17] That is precisely the type of "general, exploratory rummaging in a person's belongings" that the Fourth Amendment prohibits. Coolidge v. N.H., 403 U.S. 443, 467 (1971).

If the government intends to resubmit these Applications, it must be more discriminating when determining what it wishes to seize, and it must make clear that it intends to seize *only* the records and content that are enumerated and relevant to its present investigation. In their present state, however, the Applications are impermissibly lacking in specificity as to what exactly will be seized and are therefore overbroad.[18]

IV. The Present Applications Risk Government Overseizure

This matter presents the Court with a Fourth Amendment oddity. Pursuant to a search and seizure warrant of the Solomons, Maryland hotel room, the government seized the cell phones

---

[13] 5. Any and all names of persons [sic] has contacted recently contacted [sic] through calls and text messages
[14] 6. Images, pictures, photographs sent or received by user.
[15] 7. The content of any and all text messages sent or received by user.
[16] 8. The content of any and all voice mail messages.
[17] Although this Court generally distinguishes between "records" and "content," as in 18 U.S.C. § 2703, it is evident that these Applications include both records and content under the term "records."
[18] Case law on this issue is primarily concerned with an overbroad *search*. See United States v. Richards, 659 F.3d 527, 541-42 (5th Cir. 2011) ("[The warrant] was not unconstitutionally overbroad. The scope of the warrant was restricted to a search for evidence of child pornography crimes and did not permit a free-ranging search."); see also United States v. Burgess, 576 F.3d 1078, 1091 (10th Cir. 2009) ("[O]ur case law requires that warrants for computer searches must affirmatively limit the search to evidence for specific federal crimes or specific types of material."). Here, the government wants to *seize* an inordinate amount of material. The concern regarding seizing is the same as with searching in Richards and Burgess because, of course, in order for the government to *seize* some subset of data from these cell phones, it must first *search* the phones.

that are the focus of the present Applications.[19] See Affidavit at 8. As a result, those phones are clearly already "seized" within the meaning of the Fourth Amendment. See Brower v. Cnty. of Inyo, 489 U.S. 593, 596 (1989). Now, though, the government seeks a second search and seizure warrant to examine the *contents* of these phones. Assuming that the "search" does not occur until the contents of the phone are examined, see Orin Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 551 (2005), the government's Application—which specifically asks to seize the data that is, in reality, already seized—is operating under the implied assumption that the contents are not currently seized.

The best way of resolving this constitutional oddity is by treating these Applications as requesting additional warrants under United States v. Tamura, 694 F.2d 591 (9th Cir. 1982) and its progeny, including United States v. Hill, 459 F.3d 966 (9th Cir. 2006) and United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1180 (9th Cir. 2010). In Tamura, the Ninth Circuit addressed what should occur when "documents are so intermingled that they cannot feasibly be sorted on site." Tamura, 694 F.2d at 595. The court "suggest[ed] that the Government 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." Id. at 595-96. Although Tamura was primarily concerned with the removal of computer storage devices away from the site where the initial search and seizure occurred, the general overriding principal of these cases is that, if the government wishes to perform a "wholesale seizure," it must "justify it to the magistrate." See Hill, 459 F.3d at 976-77.

The bottom line is this: even though the cell phones are currently seized by the government, the government must still explain to the Court what the basis for probable cause is

[19] Although the Applications mention that warrant, this Court has not seen a copy of it and it is not part of the record in this matter.

to search for each thing it intends to seize, and it must explain how it will deal with the issue of intermingled documents. Because the government has come to ask for a search and seizure warrant, it can only address these issues by explaining in a revised application its intended search protocol. The Ninth Circuit has expressed repeated concern that some sort of search protocol may be needed if there is concern about the government "overseizing data and then using the process of identifying and segregating seizable electronic data 'to bring constitutionally protected data . . . into plain view.'" United States v. Schesso, 730 F.3d 1040, 1047 (9th Cir. 2013) (citing Comprehensive Drug Testing, 621 F.3d at 1047). That same concern is what animates the Court's present ruling.

The Court is unaware of any appellate decision that *requires* a search protocol before a warrant may be issued. See, e.g., Hill, 459 F.3d at 978 ("As we have noted, we look favorably upon the inclusion of a search protocol; but its absence is not fatal."). And many courts have expressed legitimate concerns about hamstringing a valid criminal investigation by binding the government to a strict search protocol *ex ante*. See, e.g., Burgess, 576 F.3d at 1094. Certainly, something like searching only for JPEGs or the term "sex" would be absurd. But the Court will require the government to give some indication of how the search will proceed. Will all of these devices be imaged? For how long will these images be stored? Will a dedicated computer forensics team perform the search based on specific criteria from the investigating officers of what they are looking for, or will the investigating officers be directly involved? What procedures will be used to avoid viewing material that is not within the scope of the warrant? If the government discovers unrelated incriminating evidence, will it return for a separate search and seizure warrant? See id. at 1095 (the searching officer "closed the gallery view when he observed a possible criminal violation outside the scope of the warrant's search authorization and

did not renew the search until he obtained a new warrant."). These types of issues must be addressed.

In the context of an e-mail search, this Court recently determined that the third-party provider must perform the search unless the government can suggest a sufficient alternative. 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 (D.D.C. Mar. 7, 2014).[20] Unless the government follows Judge Alex Kozinski's suggestion that "[s]egregation and redaction of electronic data must be done either by specialized personnel or an independent third party," that type of option is not available here. Comprehensive Drug Testing, 621 F.3d at 1180 (Kozinski, J. concurring). Accordingly, this Court wants more information on specific search protocols before allowing the government to sift through what may be thousands of files on these devices.

V. The Government Fails to Explain What Will Occur to Data Outside the Scope of the Warrant

The related question to the overbreadth issue—and one that was touched on in Tamura and in this Court's opinions—is what will occur with data that is seized by the government and is outside the scope of the warrant. See Tamura, 694 F.2d at 595. In Tamura, the government acted improperly by not returning documents that were seized but "not described in the warrant." Id. at 596. Will such information be returned, destroyed, or kept indefinitely? The government must specify what will occur—although it is admonished that any response other than "the information will be returned or, if copies, destroyed" within a prompt period of time will likely find any revised application denied. 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

[20] https://www.dcd.uscourts.gov/dcd/sites/dcd/files/14-228JMF.pdf

Controlled by Facebook, Inc., 13-MJ-742, 2013 WL 7856600, at *7 (D.D.C. Nov. 26, 2013) (Facciola, M.J.).

VI. Conclusion

For the reasons stated above, it is hereby **ORDERED** that the government's Applications are **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: 2014.03.11 16:52:17 -04'00'

JOHN M. FACCIOLA
UNITED STATES MAGISTRATE JUDGE