UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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	Magistrate Case No. 14-265 (JMF)
IN THE MATTER OF THE SEARCH OF A FUJIFILM CAMERA FINEPIX CONTAINING A 16 GB DISC, SERIAL NUMBER 2UG62662, IN CUSTODY OF UNITED STATES POSTAL INSPECTION SERVICE, 1400 NEW YORK AVE NW, WASHINGTON, DC	Magistrate Case No. 14-266 (JMF)
IN THE MATTER OF THE SEARCH OF AN LG CELL PHONE, SERIAL NUMBER 107KPED087260, IN CUSTODY OF UNITED STATES POSTAL INSPECTION SERVICE, 1400 NEW YORK AVE NW, WASHINGTON, DC	Magistrate Case No. 14-267 (JMF)
IN THE MATTER OF THE SEARCH OF SONY LAPTOP COMPUTER, SERIAL NUMBER 275558235000498 IN CUSTODY OF UNITED STATES POSTAL INSPECTION SERVICE, 1400 NEW YORK AVE NW, WASHINGTON, DC	Magistrate Case No. 14-268 (JMF)

MEMORANDUM OPINION AND ORDER

Pending before the Court are four Applications for search and seizure warrants pursuant to Rule 41 of the Federal Rules of Criminal Procedure for four electronic devices. See Affidavit In Support of an Application for a Search Warrant at 29 (hereinafter the "Affidavit").[1] For the first time, the government's Application includes an "Attachment C (Search Protocol)," which purports to address concerns the Court raised in In the Matter of the Search of Black iPhone 4,

[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.

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).[2] Attachment C, however, fails to adequately detail the proposed search protocol and thus fails to adequately address the Court's concerns. For the reasons stated below, the government's Applications for search and seizure warrants will be denied.

I. Background

Each of the four Applications is based on the same Affidavit, and each pertains to an investigation of the distribution and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A, by a German national who was arrested while in New York City.[3] According to the Affidavit, the owner of the devices at issue in the Application operated a child pornography web forum. Affidavit at 19. Upon his arrest—and following a search of his hotel room—the government seized: 1) a Sony laptop; 2) a Fujifilm digital camera; 3) an LG cell phone; 4) an ODYS tablet; and 5) a sealed letter.[4] Id. at 30-31.

Using a standard format, the Application contains an "Attachment A" that describes the devices to be searched and an "Attachment B," which lists "Items to Be Seized." Affidavit at 32. Specifically, Attachment B says:

[2] The same Memorandum Opinion and Order was also used in In the Matter of the Search of Samsung SGH-T989 AKA Galaxy S II Cellular Telephone IMEI 359858/04/531905/8, SN R31CC12PDBN, Mag. Case No. 14-236; In the Matter of the Search of Samsung SGH-S150G Cellular Telephone, Black in Color, IMEI 564082/05/308324/2, S/N R21D5951DTV, Mag. Case No. 14-237; In the Matter of the Search of Western Digital TV, S/N WNT291019173, Mag. Case No. 14-238; In the Matter of the Search of Western Digital Hard Drive, S/N WCAUK1341857, Mag. Case No. 14-239; and In the Matter of the Search of Western Digital Mybook Essential Hard Drive, S/N WCAZA5015009, Mag. Case No. 14-240.

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

[4] The letter, which the subject of the search warrant application in In re Matter of the Search of Sealed Letter Addressed to Klaus Von Der Heide, in custody of United States Postal Inspection Service, 1400 New York Ave, NW, Washington, DC, Mag. Case No. 14-269, is not addressed in this Memorandum Opinion. The Court will grant that search warrant application separately.

ATTACHMENT B – ITEMS TO BE SEIZED

The following items to be seized constitute contraband, fruits, and evidence of violations of Title 18, United States Code, Sections 2251, 2252 and 2252A found on the property described in Attachment A or relate to the identity of an individual identified as "Athemis," the lead administrator of an Internet bulletin board dedicated, in part, to the trading of images of child pornography:

a. visual depictions of minors engaged in sexually explicit conduct;
b. evidence of or pertaining to the production, advertising, promotion, transportation, accessing with intent to view, and possession of such visual depictions of minors engaged in sexually explicit conduct, including child erotica, in or affecting interstate or foreign commerce;
c. Evidence of user attribution showing who had dominion, ownership, custody, or control of the digital media device corresponding to any evidence described in "a" or "b."
d. Information, correspondence, records, documents or other materials constituting evidence of or pertaining to items "a", "b" or "c" above, including, but not limited to (and to the extent applicable to the Fujifilm Camera FinePix S4400, the LG Cell Phone, and the sealed letter):
    i. correspondence or communications, such as electronic mail, chat logs, or other written communication;
    ii. Internet usage records, user names, logins, passwords, e-mail addresses and identities assumed for the purposes of communication on the Internet, billing, account, and subscriber records, membership in online groups, clubs or services, connections to online or remote computer storage;
    iii. diaries, calendars, address books, names, and lists of names and addresses of individuals who may have been contacted by computer and internet websites; and
    iv. shared images, "contacts' lists," and image "thumbnails."

All of the items listed in "a" through "d" above include in whatever form and by whatever means they may have been created or stored on the a Sony laptop computer, with serial number 275558235000498, a Fujifilm Camera FinePix S4400 containing a 16 GB disc, with a serial number 2UG62662, a LG Cell Phone, with a serial number 107KPED087260, and a ODYS LOOX Plus Tablet, with a serial number 4707213703415, as described in separate Attachments A.

Id. at 32.

For the first time in this Court's experience, the government has also included Attachment C, which purports to provide a search protocol. Attachment C provides:

ATTACHMENT C (SEARCH PROTOCOL)

> To the extent practical, if persons claiming an interest in seized computers or other digital media devices so request, the United States will make available to those individuals copies of the requested files (so long as those files are not considered contraband or evidence as described in Attachment B) within a reasonable time after the execution of the search warrant. In order to preserve the integrity of the original evidence, these copies will be made from an exact duplicate or a mirror copy of these items, rather than the original evidence. This should minimize any impact the seizures may have on the computer user's personal and/or business operations.
>
> If, after inspecting the device or computer system, including all input-output devices, system software, and instruction manuals, the computer specialist conducting the forensic examination determines any of these seized items do not contain evidence of the crimes enumerated in Attachment B, and do not contain or constitute contraband, the United States will return these items.
>
> Only items authorized to be seized will be printed out for evidence purposes. Other records that may be found on the same storage medium will not be shown to anyone else or printed for any purpose.
>
> In order to preserve the integrity of original evidence, the computer forensics specialist(s) conducting the searches will make duplicate copies or mirror images of any device seized pursuant to these search warrants and any evidence (including images of child pornography or other contraband) will be stored or maintained by the United States until the target/ defendant's appeals and habeas proceedings are concluded.
>
> If the United States discovers unrelated incriminating evidence, it will return for a separate search and seizure warrant.

Affidavit at 33-34. The government also included a substantial footnote indicating that, based on Professor Orin Kerr's article Ex Ante Regulation of Computer Search and Seizure, 96 Va. L. Rev. 1241, 1242 (2010), it "is not conceding a search protocol is necessary." Affidavit at 33, n.1.[5]

[5] For a rebuttal of Professor Kerr's article, see Paul Ohm, Massive Hard Drives, General Warrants, and the Power of Magistrate Judges, 97 Virginia Law Review In Brief 1 (2011); see also In re Search Warrant, 71 A.3d 1158, 1186 (Vt. 2012) (upholding nine ex ante restrictions on a search warrant for electronic data but holding that the issuing officer could not prevent the government from relying on the plain view doctrine).

II. Attachment C Fails to Address this Court's Concerns

The present matter, and this Memorandum Opinion, is a direct sequel to the Court's opinion in In re Search of Black iPhone. Nine days ago, this Court denied without prejudice six search and seizure warrants for electronic devices because the government failed to "explain to the Court what the basis for probable cause is 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. The Court therefore required the government to "give some indication of how the search will proceed" and indicated that this decision was motivated by issues such as:

> 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?

Id.

The government has partially complied with the Court's opinion. The present Application's Attachment B addresses all of the Court's concerns about *what* will be seized and *what* is within the scope of the warrant—indeed, it should serve as a model Attachment B for future applications. The government has not, however, adequately addressed the Court's concerns by explaining *how* the search will occur and *how* the government will avoid overseizure by avoiding keeping documents and other information outside the scope of Attachment B.

A. What Attachment C Means

Attachment C is far from a paragon of clarity. The Court has thoroughly studied it to understand the purpose of each of the five paragraphs.

In the first paragraph, the government writes:

> To the extent practical, if persons claiming an interest in seized computers or other digital media devices so request, the United States will make available to those individuals copies of the requested files (so long as those files are not considered contraband or evidence as described in Attachment B) within a reasonable time after the execution of the search warrant. In order to preserve the integrity of the original evidence, these copies will be made from an exact duplicate or a mirror copy of these items, rather than the original evidence. This should minimize any impact the seizures may have on the computer user's personal and/or business operations.

Affidavit at 33. As far as the Court can tell, this paragraph indicates that the government will return *copies* of all data (that are not contraband or evidence described in Attachment B) within a "reasonable time after the execution of the search warrant." There is no indication, however, that the original files will be returned.

In the second paragraph, the government writes:

> If, after inspecting the device or computer system, including all input-output devices, system software, and instruction manuals, the computer specialist conducting the forensic examination determines any of these seized items do not contain evidence of the crimes enumerated in Attachment B, and do not contain or constitute contraband, the United States will return these items.

Affidavit at 33. This paragraph indicates that the government will return all *actual devices* that—after a thorough search—are determined not to have any evidence described in Attachment B. It also implies that the actual search will be carried out by a separate computer forensics specialist and not by the affiant or other individual directly involved with the investigation.

In the third paragraph, the government writes:

> Only items authorized to be seized will be printed out for evidence purposes. Other records that may be found on the same storage medium will not be shown to anyone else or printed for any purpose.

Affidavit at 33. In essence, this paragraph is a truism: any data that are not within the scope of Attachment B will not be copied or shared; any data that are within the scope of attachment B will be copied and shared.

In the fourth paragraph, the government writes:

> In order to preserve the integrity of original evidence, the computer forensics specialist(s) conducting the searches will make duplicate copies or mirror images of any device seized pursuant to these search warrants and any evidence (including images of child pornography or other contraband) will be stored or maintained by the United States until the target/ defendant's appeals and habeas proceedings are concluded.

Affidavit at 33. This paragraph indicates that the computer forensics specialist performing the search will image the device, and the government will then keep that image until all appeals or habeas proceedings are concluded. This will occur regardless of how much data on that image is not within the scope of Attachment B.

In the fifth paragraph, the government writes:

> If the United States discovers unrelated incriminating evidence, it will return for a separate search and seizure warrant.

Affidavit at 33. This paragraph indicates that, should the government in the course of its search discover any incriminating material outside the scope of Attachment B, it will secure an additional search and seizure warrant before looking for further evidence related to that material.

B. Attachment C Is Inadequate

Taken as a whole, Attachment C raises serious questions. First, it appears that a computer forensic specialist will image and search the drives, but there is no explanation of what that person's relationship is with the team investigating the underlying crime and whether the investigating officers will be directly involved in the search. Second, although the government will return data that are not within the scope of Attachment B, it will return only copies and thus keep the originals (unless the *entire device* contains no such relevant data). Furthermore, the reference to "print[ing]" materials for evidence purposes seems bizarre given that the government will presumably make electronic copies of documents. Even if non-relevant

documents "will not be shown to anyone else or printed for any purpose," the real question is what will happen with *electronic* copies—which it seems the government will retain indefinitely.

Although the above paragraph raises issues that need clarification, there are two larger systemic problems. First, the government intends to wholly image these devices and store them "until the target/ defendant's appeals and habeas proceedings are concluded." Affidavit at 33. This is unacceptable. The government cannot keep data that is outside the scope of the warrant. Accordingly, that data must be either returned or destroyed, and it certainly cannot be kept indefinitely pending appeal. See In re Search of Black iPhone, 2014 WL 1045812 at *5 ("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."). The alternative would be to allow the government to maintain data that it—and this Court—knows to be outside the scope of the warrant and for which the government has no probable cause to seize.

If the government is worried that it will have a chain of custody problem with respect to an image of a device that has had non-relevant documents deleted, it is mistaken. The same testimony that would be given for a complete device image is, with a slight modification, perfectly acceptable: the testifying individual need only say that, in compliance with this Court's rulings, the image is complete except for non-relevant files, which were deleted from the image.

The second major issue with Attachment C is that *it provides no actual search protocol*. This Court specifically instructed the government to tell it how it intends to conduct the search. See In re Search of Black iPhone, 2014 WL 1045812 at *4 ("But the Court will require the government to give some indication of how the search will proceed . . . What procedures will be

used to avoid viewing material that is not within the scope of the warrant?"). All Attachment C actually says with regards to an actual "search protocol" is that a computer forensic specialist will image each device, search them, and keep all files (regardless of whether they fall within the scope of Attachment B). This tells the Court precisely nothing more than it knew nine days ago—and it does nothing to address the Court's concerns that an inadequate search protocol will fail to deal with the problem of intermingled documents for which the government has no probable cause to seize. See id. ("[The government] must explain how it will deal with the issue of intermingled documents.").

Since the government has not taken the hint, the Court will be more explicit: the government needs to provide a sophisticated technical overview of how it plans to conduct the search. It need not be overly detailed—the Court is not asking for a list of search terms—but the overview must provide this Court with sufficient information such that it will not be authorizing the "general, exploratory rummaging in a person's belongings" that the Fourth Amendment prohibits. See Coolidge v. N.H., 403 U.S. 443, 467 (1971). A separate affidavit from a computer forensics specialist is not required, but the law enforcement officer affiant must include details in his affidavit about how that computer forensics specialist intends to complete his search. The Court expects to receive an overview that uses whatever technical terms are necessary to explain how the search will be done. No sophisticated search should occur without a detailed explanation of the methods that will be used, even if the explanation is a technical one, and no search protocol will be deemed adequate without such an explanation.

III. Conclusion

To its credit, the government has, in the span of just over one week, made progress in addressing this Court's concerns. In particular, Attachment B specifies with appropriate

particularity what will actually be seized from each device and ties those seizures directly to the criminal statutes underlying the investigation. However, Attachment C requires substantial modification, and, in its current form, it is wholly inadequate.

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: 2014.03.20 09:38:25 -04'00'

JOHN M. FACCIOLA
UNITED STATES MAGISTRATE JUDGE