UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

In the Matter of the Search of premises known as:	
A NEXTEL Cellular Telephone with [redacted] (Unknown Assigned Telephone Number) Belonging to and Seized from [redacted]	**SEARCH WARRANT**
	CASE NUMBER: 14-MJ-8005-DJW

MEMORANDUM AND ORDER DENYING APPLICATION FOR SEARCH WARRANT

This court has been asked to issue a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure for the contents of a cell phone that is currently in the custody of the Drug Enforcement Agency (DEA). Based on this courts previous rulings and other case law this request has been denied. This memorandum will more explicitly explain the reasons for the denial.

I. BACKGROUND

The following was in the application submitted to the court:[1]

1. On December 26, 2013, at approximately 10:00am, I was contacted via telephone by DEA S/A Christopher Kline regarding information he had received from a DEA Source of Information (SOI) earlier that morning.
2. S/A Kline informed me that the DEA SOI had provided information that there was a Toyota Tacoma with Mexico license plates at the Drury Inn hotel near Interstate 35 and

[1] Pages 3–6 of the Affidavit as it was submitted to the Court have been included and have not been changed except for any redactions.

Shawnee Mission Parkway in Merriam, KS that contained approximately 15 pounds of methamphetamine.

3. At approximately 10:20am, I established surveillance at [redacted] hotel at [redacted], Merriam, KS 66202. Upon establishing surveillance, I observed a white Toyota Tacoma pick-up truck bearing Nuevo Leon Mexico license plate [redacted] parked on the west side of the hotel.

4. At approximately 10:30am, I observed a Hispanic male and a Hispanic male juvenile walk from the hotel, enter the Tacoma, and depart the parking lot of the hotel.

5. At approximately 10:40am, I observed the Tacoma arrive at [redacted] at [redacted], Merriam, KS 66202. I observed the Hispanic male driver and Hispanic male juvenile passenger exit the Tacoma and enter the store.

6. At approximately 10:45am, I observed the Hispanic male and Hispanic male juvenile exit the [redacted] store, re-enter the Tacoma, and travel southbound through the shopping center parking lot. I then observed the Tacoma stop and park at a [redacted] store at [redacted], Merriam, KS 66202. I then observed the Hispanic male driver and Hispanic male juvenile passenger exit the Tacoma and enter the [redacted] store.

7. At Approximately 10:55am, I observed the Hispanic male and Hispanic male juvenile exit the [redacted] store and walk back to the Tacoma in the parking lot. At that time, DEA S/A Nick Wills and I approached the two individuals and made contact with the individuals outside the Tacoma. S/A Wills and I adorned police regalia clearly identifying ourselves as law enforcement.

8. Upon making contact with the two individuals, the driver was identified as [redacted], the juvenile was identified as his son, and the vehicle was verified as belonging to [redacted].

It was also determined that neither individual spoke English; therefore, a request for law enforcement assistance was immediately placed to the surrounding police departments for a Spanish-speaking officer. At that time, a Merriam uniformed officer arrived to provide site security. The Merriam officer did not speak Spanish.

9. At approximately 11:00am, S/A Wills and [redacted] entered my DEA official government vehicle and contacted via telephone Immigration and Customs Enforcement (ICE) S/A Timothy Ditter, an agent fluent in the Spanish language. During the telephone call, S/A Ditter asked [redacted] for verbal consent to search the Tacoma and the contents contained therein. [redacted] provided verbal consent to S/A Ditter to search his vehicle, as witnessed by S/A Wills.

10. At approximately 11:30am, S/A Wills and I initiated a consent search of the Toyota Tacoma. Soon thereafter, S/A Wills and I located seven large rectangular packages hidden inside the seat-backs of the rear truck seats of the vehicle. The packages were photographed in-place and then removed for further inspection. The packages appeared to be wrapped in plastic wrap and tape and appeared to contain a large quantity of suspected methamphetamine. S/A Wills then performed a field test of the contents of the packages, as witnessed by me, which provided a positive indication for the presence of methamphetamine.

11. At that time, [redacted] was placed under arrest and placed in a marked patrol vehicle for transport.

12. Subsequent to his arrest, DEA seized as evidence from [redacted] his NEXTEL cellular telephone which was identified as a black and orange NEXTEL smartphone having

International Mobile Equipment Identity [redacted]. The telephone number assigned to this telephone is currently unknown.

13. I hereby request the Court's permission to conduct a full and complete forensic telephone examination of the NEXTEL cellular telephone described above. This exam includes a search of contact lists, calendars, stored image and video files, internet history, SMS and MMS text messaging, and other data related to drug sales, cultivation, and distribution.

14. The following search methodology will be employed to examine the cellular telephone.

SEARCH METHODOLOGY TO BE EMPLOYED

The search procedure of electronic data contained in cellular telephone, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such cellular telephone hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in this affidavit.

II. ANALYSIS

A. The Constitutional Basis for the Court's Concerns

This Court reiterates its concern that the government's search warrants runs afoul of the probable cause and particularity requirements of the Fourth Amendment.[2] 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 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."[3]

The search warrant probable cause and particularity requirements serve two constitutional protections:

---

[2] *See In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, 13-MJ-8163-JPO, 2013 WL 4647554 (D. Kan. Aug. 27, 2013).

[3] U.S. Const. amend. IV.

> "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. The second, distinct objective is that 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. The warrant accomplishes this second objective by requiring a "particular description" of the things to be seized."[4]

The Fourth Amendment thus categorically prohibits the issuance of any warrant except one particularly describing (1) the place to be searched, and (2) the persons or things to be seized. The particularity requirement first mandates that warrants describe with particularity the place to be searched. "The test for determining the adequacy of the description of the location to be searched is whether the description is sufficient 'to enable the executing officer to locate and identify the premises with reasonable effort, and whether there is any reasonable probability that another premise might be mistakenly searched.'"[5]

This test "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."[6] Thus, 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.'"[7]

---

[4] *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

[5] *United States v. Lora–Solano*, 330 F.3d 1288, 1293 (10th Cir.2003) (quoting *United States v. Pervaz*, 118 F.3d 1, 9 (1st Cir.1997)).

[6] *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

[7] *Id.* at 84-85 (citing *United States v. Ross*, 456 U.S. 798, 824 (1982)).

While the manifest purpose of the Fourth Amendment particularity requirement is to prevent general searches,[8] it also provides assurances to the individual whose property is searched or seized of the lawful authority of the executing officer, the officer's need to search, and the limits of the officer's power to search.[9]

In addition to the places to be searched, the warrant must also describe the things to be seized with sufficient particularity. This is to avoid a "general exploratory rummaging of a person's belongings," and was included in the Fourth Amendment as a response to the evils of general warrants.[10] First, the description of the things to be seized must be "confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause."[11] Second, a warrant must describe the things to be seized with sufficiently precise language so that it informs the officers how to separate the items that are properly subject to seizure from those that are irrelevant.[12] Stated another way: "As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."[13] Taken together, a warrant is overly broad if it does not contain sufficiently particularized language that creates a nexus between the suspected crime and the things to be seized.[14]

The Court remains concerned that, in its current form, the government's Application violates both of these provisions.

B. Applying Constitutional Protections in the Digital Era

---

[8] *Id.*

[9] *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (citations omitted).

[10] *United States v. Campos*, 221 F.3d 1143, 1147 (10th Cir.2000).

[11] *Mink v. Knox*, 613 F.3d 995, 1010 (10th Cir.2010).

[12] *See Davis v. Gracey*, 111 F.3d 1472, 1478–79 (10th Cir.1997) ("We ask two questions: did the warrant tell the officers how to separate the items subject to seizure from irrelevant items, and were the objects seized within the category described in the warrant?").

[13] *Marron v. United States*, 275 U.S. 192, 196 (1927).

[14] *Campos*, 221 F.3d at 1147.

Applying the foregoing Fourth Amendment requirements has rapidly evolved over the years in the absence of helpful guidance from the Supreme Court or agreement among the lower courts. Consider the following timeline of the evolution of the Fourth Amendment's requirements as applied to cases overlapping with the digital realm.

1. The Supreme Court's View of Cellular Phones

On June 25, 2014, the United States Supreme Court decided *Riley v. California*.[15] This case was principally about the search of a cellular phone incident to lawful arrest. Importantly, the Supreme Court expressly reserved the right to consider the type of search at issue in this case.[16] However, the Supreme Court's discussion of cellular phones and any accompanying government search is *generally* helpful.

From the start, the Supreme Court is blunt: "[M]odern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy…[as] a significant majority of American adults now own such phones."[17] The Supreme Court's conclusion is equally forceful: "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life,' The fact that technology now

[15] *Riley v. California*, No. 13-132 (June 25, 2014), *available at* http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

[16] *Id.* at 18 fn. 1 ("Because the United States and California agree that these cases involve searches incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.")

[17] *Id.* at 9.

allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[18]

Having shown that the Fourth Amendment directly applies to cellular phones, the general discussion of the rights implicated by such a search is illuminating. For instance, the United States argued that the search of all data stored on a cellular phone is "materially indistinguishable" from searches of these sorts of physical items."[19] "The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items."[20] The Supreme Court rejected this argument because cell phones are "in fact minicomputers that also happen to have the capacity to be used as a telephone."[21] Further, just as Judge John Facciola explains in his opinions, *infra* Section B. 3, "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity."[22] Such storage capacity has "several interrelated consequences for privacy."[23] "Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house[.]"[24]

Finally, *Riley* addresses additional concerns with the search of a cell phone generally, such as encryption, remote-wiping, and a phone's connection with cloud computing.[25] For

---

[18] *Id*. at 28 (citations omitted).
[19] *Id*. at 16.
[20] *Id*.
[21] *Id*.
[22] *Id* ("The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos […] We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future.").
[23] *Id*. at 18 ("For instance, "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions.").
[24] *Id*. at 20-21.
[25] *See id*.

instance, it discusses a search of files, *accessible via the cell phone*, but which are stored in the cloud.[26]

2. The Tenth Circuit's Timeline

In 1988, the Tenth Circuit set out the general standard for evaluating when the Fourth Amendment's particularity requirement for things to be seized has been met:

> "A description is sufficiently particular when it enables the searcher to reasonably ascertain and identify the things authorized to be seized. Even a warrant that describes the items to be seized in broad or generic terms may be valid when the description is as specific as the circumstances and the nature of the activity under investigation permit. However, the Fourth Amendment requires that the government describe the items to be seized with as much specificity as the government's knowledge and circumstances allow, and warrants are conclusively invalidated by their substantial failure to specify as nearly as possible the distinguishing characteristics of the goods to be seized."[27]

In 1999, the Tenth Circuit applied the particularity requirement to a warrant authorizing the search of computer files.[28] The court noted that comparing computers to closed containers or file cabinets may be inadequate and lead to oversimplification of a complex area of Fourth Amendment doctrines by ignoring the realities of massive modern computer storage. "Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information."[29] It proposed that a court could alternatively acknowledge that computers often

---

[26] *Id*. As it relates to a search *incident to arrest*, the government conceded this point in their brief.

[27] *United States v. Leary*, 846 F.2d 592, 600 (10th Cir.1988).

[28] *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir.1999).

[29] *Id*. (citing Raphael Winick, *Searches and Seizures of Computers & Computer Data*, 8

contain "intermingled documents" and thus law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant.[30] The court stated that the magistrate judge should then require officers to specify in a warrant which type of files are sought.[31]

In 2009, the Tenth Circuit recognized that the Fourth Amendment's warrant particularity requirement has increased importance with respect to electronically stored information.

> "The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important. Because of this, our case law requires that "warrants for computer searches must affirmatively limit the search to evidence of specific federal crimes or specific types of material."[32]

Even with these concerns, in the digital realm, the particularity requirement with respect to the place to be searched remains complicated, at best. For example, in the digital realm, whether a description of a place to be searched is sufficiently particular is a complicated question because of the differences between the physical and digital worlds.[33] In one sense, the data is seized because the device has been seized.[34]

Given *Riley*,[35] the Court expects this evolution to progress further.[36] As of this opinion, however, the Tenth Circuit has not issued any guidance concerning the probable

---

Harv. J.L. & Tech. 75, 104 (1994)).

[30] *Id.*

[31] *Id.*

[32] *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir.2009) (quoting *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir.2005)) (emphasis in original).

[33] Nichole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E–Mail Surveillance*, 90 Neb. L.Rev. 971, 987 (2012).

[34] In another sense, the data has not been seized because law enforcement has neither searched (read: viewed) the data's contents nor seized the relevant files as evidence.

[35] *Riley*, *supra* note 15.

cause and particularity clauses of the Fourth Amendment, as applied to searches of lawfully seized cellular phones.

2. Another Persuasive Approach

Most recently, Magistrate Judge John Facciola of the United States District Court for the District of Columbia has also denied search warrants based upon concerns that the warrants violate the Fourth Amendment's probable cause and particularity requirements.[37] Indeed, much of his rationale is implicitly authorized by the Supreme Court's dicta in *Riley*.[38] Like the Tenth Circuit timeline above, it is useful to view Judge Facciola's opinions in chronological order.

a. In re Search of Black iPhone[39]

In *In re Search of Black iPhone*, the government submitted six search warrant applications referencing the same affidavit. The items sought were three cellular phones and three hard drives. Accompanying each application was an "Attachment B" that read:

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

---

[36] Despite *Riley*'s application only to searches incident to arrest.

[37] *See In re Search of Apple iPhone, IMEI 013888003738427*, No. 14-278 (D.D.C. filed March 36, 2014) (hereinafter "IMEI"); *In the Matter of the Search of Black iPhone 4, S/N Not Available*, No. 14-235, 2014 WL 1045812 (D.D.C. Mar. 11, 2014) (Facciola, M.J.) (hereinafter *Black 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 (D.D.C. Mar. 20, 2014) (Facciola, M.J.) (hereinafter *Odys Loox*).

[38] *Riley*, *supra* note 15.

[39] 2014 WL 1045812 (D.D.C. Mar. 11, 2014).

> 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.[40]

There were three issues that concerned the court. First, the government's continued to use boilerplate language in its search warrants. For example, Attachment B was identical for all six applications, yet it specifically requested "All records contained in the *cellular telephones*" (emphasis added), even though three of the devices were computer hard drives, not cellular phones. Accordingly, the court summarily denied those applications because it had "once again used formulaic language without careful review."[41]

---

[40] *Id*. at 1–2.

[41] *Id*. (citing *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, ___F.Supp.2d ___, ____, 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.")).

Second, the government's search warrants attempted to seize data for which they had no probable cause. In this case, the crime being investigated was the distribution and possession of child pornography. Probable cause was established for items 1, 2, 3, 9, and 10 in Attachment B; but, items 4, 5, 6, 7, and 8 lacked probable cause because the government requested *all* information.[42] "With one simple modification, these Applications would 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)."[43]

Finally, these warrants presented Judge Facciola with a "Fourth Amendment oddity." Pursuant to a prior valid search warrant of a hotel room, the government had already seized the phone. Now, the government requested the ability to search the phone's *contents*.[44] Thus, the applications were viewed as requests for additional warrants under *United States v. Tamura*.[45] "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 to search for each thing it intends to seize, and it must explain how it will deal with the issue of intermingled documents."[46] This explanation, or "search protocol," needed to answer the following questions:

> "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?

---

[42] *Id*. at 2–3.

[43] *Id*. at 3.

[44] *Id*. ("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.").

[45] 694 F.2d 591 (9th Cir.1982).

[46] *Id*. at 4.

> 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?"[47]

And, with respect to any data that has been seized but is outside the scope of the warrant, the government needed to answer: "[w]ill such information be returned, destroyed, or kept indefinitely?"[48]

b. In re Search of Odys Loox[49]

Nine days later, Judge Facciola revisited the issue. Attempting to comply with *In re Search of Black iPhone* (discussed above), the government submitted a revised Attachment B. This revised version fully complied with the Fourth Amendment.[50] The government submitted a first of its kind, Attachment C, which read:

> ***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.

---

[47] *Id*. (formatting altered).
[48] *Id*. at *5.
[49] *Odys Loox*, 2014 WL 1063996. (D.D.C. Mar. 20, 2014).
[50] The court noted that this new Attachment B should serve as a model for future attachments. *Id*. For brevity, the full text of this compliant Attachment B is omitted.

> 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.[51]

It was the first time, in the court's experience, that the government had supplied anything that purported to be a "search protocol."[52] The government's search warrant was denied because, on the whole, the court found Attachment C problematic for a variety of reasons.

First, the government indicates a "computer forensic specialist" will image each device.[53] The government then stores each image "until the target/defendant's appeals and habeas proceedings are concluded."[54] "This is unacceptable."[55] The government is not permitted to keep data outside the scope of the warrant, especially indefinitely while on appeal. "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

---

[51] *Odys Loox*, 2014 WL 1063996, at *23.

[52] Notably, the government did include 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.'" In a footnote, the court responded: "For a rebuttal of Professor Kerr's article, *see* Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges,* 97 Va. L. Rev. In Brief 1 (2011); *see also In re Search Warrant,* 193 Vt. 51, 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)." *Id*. at *5.

[53] Imaging a device is essentially cloning all of the device's data and storing it in another area. Put another way, if one backs up her computer hard drive to an external drive, an identical copy will reside on the external drive regardless of whether it is plugged into that computer or not.

[54] *Odys Loox*, 2014 WL 1063996, at *3.

[55] *Id*. at *5.

seize."[56] Anticipating the government's concerns with chain of custody, the court instructed that a " 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."[57]

Second, the court found that while Attachment C is labeled "Search Protocol," it provides no actual search protocol. Attachment C failed to answer any of the questions posed by the court in *In re Search of Black iPhone*. Instead, it merely indicated a "computer forensic specialist" would image, search, and keep the data on each device.[58] Consequently, the court denied the government's search warrant application.

c. In the Matter of the Search of Apple iPhone, IMEI 013888003738427[59]

Six days after his opinion in *In re Search of Odys Loox*, Judge Facciola considered another attempt by the government to provide an adequate search protocol in *In the Matter of the Search of Apple iPhone, IMEI 013888003738427* ("IMEI"). The government sufficiently answered the question of what will happen to seized data that falls outside the scope of the warrant.[60] However, the government removed their indication that a device would be imaged. "As a practical matter, the [c]ourt 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."[61]

---

[56] *Id*.

[57] *Id*.

[58] Additionally, the government did not indicate the relationship between itself and the computer forensic specialist.

[59] *IMEI*, No. 14-278 (D.D.C. filed March 36, 2014).

[60] *Id*. ("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.")

[61] *Id*. at 8.

More importantly, the court articulated another Fourth Amendment reason for requiring a search protocol—particularly describing the place to be searched.[62] In one sense, the government has already indicated the particular place to be searched—the iPhone with a specific IMEI number. Electronic searches, however, are more complicated than that.[63] Thus, a sufficient search protocol is an "explanation of the scientific methodology the government will use to separate what is permitted to be seized from what is not."[64] An explanation like this "explain[s] to the Court how the government intends to determine where it will search (which 'parts'—or blocks—of the iPhone's NAND flash drive) 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."[65] Put another way, the government needs 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."[66]

Having failed to provide an adequate search protocol, the court denied the government's search warrant application.

---

[62] *Id.*

[63] As Judge Facciola lucidly explains: "An iPhone 4 has either 16 GB or 32 GB of flash memory, which could allow storage of up to around two million text documents. 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.' *Id.* (citations omitted).

[64] *Id.* at 8–9.

[65] *Id.* at 9–10 (citing *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* http://www.micron.com/-/media/documents/products/technical%20note/nand%20flash/tn2919_nand_101.pdf).

[66] *Id.* at 10.

3. Analysis of the Present Application

The present application is for the search of a cellular phone already lawfully seized.[67] As such, this Court adopts Judge Facciola's view that the applications are viewed as requests for additional warrants to search the phone's contents.[68] Additionally, the Court is persuaded by *Riley*'s dicta concerning the implications of searching a phone, generally.[69] The Court finds that the present search warrant application violates the Fourth Amendment's probable cause and particularity requirements.

This Court has already denied government search warrants in other digital content contexts, such as email communications.[70] There, we stated "[t]o comport with the Fourth Amendment, the warrants must contain sufficient limits or boundaries so that the government-authorized agent reviewing the communications can ascertain which email communications and information the agent is authorized to review."[71] In an effort to comport with this, the government's application included a search methodology ("Methodology").[72] While certainly helpful, it contains neither sufficient limits nor boundaries. This Methodology suffers from two systemic, fatal issues.[73] First, the Methodology, as written, will result in the overseizure of data and indefinite storage of data that it lacks probable cause to seize. Second, the Methodology is so broad that it appears to be nothing more than a "general, exploratory

---

[67] Accordingly, *Riley*, *supra* note 15, is merely dicta.

[68] *Black iPhone*, 2014 WL 1045812, at *4 (citing *United States v. Tamura*, 694 F.2d 591 (9th Cir.1982)).

[69] *See* Section B. 1, *supra*.

[70] *See In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, 13-MJ-8163-JPO, 2013 WL 4647554 (D. Kan. Aug. 27, 2013).

[71] *Id*. at 20.

[72] Affidavit at 5–6. A search methodology is akin to Judge Facciola's "search protocol."

[73] To be sure, there is significant overlap between these two points. For instance, the same language that permits the overseizure of data can also fail to particularly describe the items to be seized.

rummaging in a person's belongings."[74] Thus, the application fails to satisfy the particularity requirement of the Fourth Amendment.

a. The Overseizure and Indefinite Storage of Data

A warrant is overly broad if it does not contain sufficiently particularized language that creates a nexus between the suspected crime and the things to be seized.[75] Here, the application does limit the data it seeks to seize, and connects that data to the crimes being investigated—"contact lists, calendars, stored image and video files, internet history, SMS and MMS text messaging, and other data" related to "drug sales, cultivation, and distribution."[76] However, the Methodology does not provide the Court with any guidance on *how* the government intends to determine what data has a nexus to the suspected crime and what data does not.

To begin with, the government does not indicate whether it will be imaging the device. Like *IMEI*, *supra* Section B. 2(c), this Court agrees that "if the device will be imaged, then there will be a complete copy of all its data—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."[77] The failure to clarify this point cannot allay this Court's fears that it is authorizing an unlawful search in which the government lacks probable cause to search or seize the data. Ultimately, that omission alone is fatal, but in the interest of specificity the Court will continue its analysis of the provided Methodology.

---

[74] *Coolidge*, *supra*, note 4 at 467.
[75] *Campos*, 221 F.3d at 1147.
[76] Affidavit at 5.
[77] *IMEI*, *supra*, at 7–8.

The closest the government comes to accounting for the data it has seized is a parenthetical in paragraph b, which states:

> "any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified [in the Affidavit]."[78]

To the government's credit, this partially answers one of the questions posed by Judge Facciola—"[w]ill such information be returned, destroyed, or kept indefinitely?"[79] As written, however, this answer only applies to data that is both encrypted and unreadable. Otherwise, the accounting for and return of data that is either unencrypted or readable is never addressed. Although the language implies that the government will return to the individual all data outside the scope of the warrant, the government does not expressly indicate such an action. This Court cannot accept the government's compliance with the Fourth Amendment by implication. Therefore, the government must clarify this point before this Court with authorize its search warrant applications concerning digital content.

It is worth pointing out that the government is limiting its storage request to data that is encrypted and unreadable. Presumably, this language is attempting to provide the government the ability to use future, but currently unavailable, techniques to read this data that may become available during the course of a potential trial. While that is reasonable, the government is requesting the *indefinite* storage of this data.[80] This is problematic because the request is to store data that it may *never* be able to read or identify on an indefinite basis. Compounding the

[78] Affidavit at 5–6.
[79] *Id.*
[80] To be sure, any evidence that the government has probable cause to seize may be stored indefinitely, or at least until the conclusion of any proceedings.

problem is that almost every device may have installed applications that employ encryption. For example, Apple encrypts customers' text messages and Facetime conversations.[81] What this potentially means is that the government could store an iPhone owner's *entire correspondence* via iMessage indefinitely, much of which may lack probable cause having have no connection to the crimes being investigated. Consequently, the government may be indefinitely storing data for which it has no probable cause. This is precisely why this Court is requesting the government explain "once it is engaged in the search, how it will determine which blocks [of data] should be searched for data within the scope of the warrant."[82]

Because the government's application does not address these issues, the Court is concerned that authorizing this search warrant will result in the overseizure and indefinite storage of data for which the government lacks probable cause to seize in the first place.[83] Accordingly, this Court requests the government fully explain its Methodology to allay these fears.

b. Particularly Describing The Place(s) to be Searched

The Fourth Amendment also requires that a warrant particularly describe the place(s) to be searched and the items to be seized. The Court is concerned that the present application does not. It is true that, in one sense, the government describes a place to be searched—a "cellular

[81] Apple, Inc., Apple's Commitment to Customer Privacy, Apple (June 16, 2013), https://www.apple.com/apples-commitment-to-customer-privacy, ("For example, conversations which take place over iMessage and FaceTime are protected by end-to-end encryption so no one but the sender and receiver can see or read them. Apple cannot decrypt that data.").

[82] Affidavit at 10.

[83] *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).

telephone, its computer software, and/or memory storage devices."[84] Certainly, this describes the actual *thing* to be searched. But, an electronic search is not as simple.

Of course, the Fourth Amendment's text must be malleable to the practical realities of modern day searches. The Tenth Circuit acknowledges as much in *United States v. Burgess*, saying, "[o]ne 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.'"[85] The digital realm is no different. Regardless, a request to search must be accompanied by "sufficiently specific guidelines for identifying the documents sought…and [those] are followed by the officers conducting the search."[86] This is precisely what a search protocol is. The Court is therefore asking the government to explain, with particularity, its "methodology for determining, once it is engaged in the search, how it will determine which [NAND flash drive] blocks should be searched for data within the scope of the warrant."[87] Here, the government's application does nothing of the sort.

On its face, the Methodology, describes *nothing* with particularity. Indeed, a plain comparison of the search protocol in *IMEI* and the methodology included here underscores the woeful broadness and generality of the application before this Court. For instance, *IMEI*'s search protocol states, *inter alia*, that:

> "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

[84] Affidavit at 5.
[85] 576 F.3d 1078, 1094 (10th Cir. 2009).
[86] *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir.1982).
[87] *IMEI*, *supra*, at 10.

> 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."[88]

This paragraph alone contains more explanation and detail than the entire Methodology presented to this Court. Compare the above with description of three procedures to be used in this case: "c. surveying various file directories and the individual files they contain; d. opening files in order to determine their contents; [and] e. scanning storage areas."[89] The lack of detail is glaring and the explanation tells the Court nothing about *how* the government intends determine what data falls into the list of items to be seized and what data does not. "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."[90]

What is more, the government does not even explain whether or not its procedures are "computer-assisted."[91]. Saying it will "perform[] keyword searches through all electronic storage areas"[92] is the closest the government comes to indicating whether these procedures are computer-assisted. Moreover, the Methodology does not indicate at what point, if any, these computer-assisted procedures give way to human inspection. In *IMEI*, the government's search protocol stated that its "computer-assisted scans of the entire medium […] might expose many parts of the device *to human inspection to determine whether it is evidence described by the*

---

[88] *Id*. at 4.
[89] Affidavit at 6.
[90] *Id.* at 12.
[91] As a practical matter, the Court presumes that they are.
[92] Affidavit at 6. Additionally, the keyword list, itself, may pose problems. But that is not presently before the Court.

warrant."[93] Here, it is unclear if human inspection *ever* takes place after the operator activates the presumed computer-assisted scanning software. Is the determination of whether the evidence is described by the warrant left to a computer? If so, how is the computer making this decision? If not, at what point is a human intervening to determine what evidence is authorized for seizure?

The same language that exemplified broadness above—"c. surveying various file directories and the individual files they contain; d. opening files in order to determine their contents; [and] e. scanning storage areas."—is also problematic for more specific reasons. Not only do each of those individually listed procedures seem to be steps in the same process, the procedures are described no further than the basic usage of a modern computer's file system. More importantly, these procedures include no limitation language. This is an important omission because, as written, the government is requesting it be allowed to search everywhere and seize anything regardless of whether or not the data contained therein falls under the scope of its warrant. Further buttressing this conclusion is that, on each of the remaining procedures listed, the government included the language—"to view the data and determine whether that data falls within the items to be seized as set forth herein."[94] Therefore, the government is insisting that some procedures are limited to *where* evidence is likely to be found while others permit an unlimited search for evidence.

This is akin to saying that the government will search a residence by looking in all the rooms of the house and opening any desk drawers and cabinets to see what's inside, even though the government is looking for a stolen lawnmower.[95] Put another way, "[j]ust as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search

---

[93] *IMEI*, *supra*, at 4 (emphasis added).
[94] Affidavit at 5–6.
[95] *See United States v. Ross*, 456 U.S. 798, 824 (1982).

an upstairs bedroom,"[96] probable cause to believe drug trafficking communication may be found in phone's the mail application will not support the search of the phone's Angry Birds application. The Fourth Amendment would not allow such a warrant and should therefore not permit a similarly overly broad warrant just because the information sought is in electronic form rather than at a residence.[97]

Essentially, the present Methodology does not provide this Court with any meaningful description of the scope of the search it is requesting be authorized. For example, there is no explanation as to whether officers (or law enforcement forensic technicians) are searching areas of the phone that may be *wholly* off-limits to search. *Riley* illustrates a general example. There, the United States conceded that a search—albeit incident to arrest—may not include "a search of files in the cloud."[98] "Such a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[99] More importantly, the "officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud."[100] While reserving judgment on searches involving cloud computing,[101] the Supreme Court is implicitly reaffirming the sentiment in *Marron*, which states, "As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."[102] Thus, an acceptable search protocol

---

[96] *United States v. Ross*, 456 U.S. 798, 824 (1982).

[97] *See In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, 13-MJ-8163-JPO, 2013 WL 4647554, at *18 (D. Kan. Aug. 27, 2013).

[98] *Riley*, *supra*, note 15 at 21.

[99] *Id.*

[100] *Id.*

[101] *Id.* at note 1.

[102] *Marron*, 275 U.S. 192, 196 (1927).

educates (1) the Court as to what the government is doing when it searches a cell phone, and (2) the executing officer as to what places and things may or may not be searched and/or seized.

III. CONCLUSION

Reinforcing this Court's conclusion is the following passage from *Riley*:

> "[the government] suggests that officers could disconnect a phone from the network before searching the device […] Alternatively, the Government proposes that law enforcement agencies 'develop protocols to address' concerns raised by cloud computing. Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols."[103]

That quote's last sentence is important to this case for two reasons. First, the Supreme Court implicitly approves of the government providing "search protocols"—the very thing Judge Facciola and this Court are requesting. Second, even if the government provides a protocol, there may be a question as to whether it is enough. Consequently, the Supreme Court is implicitly saying that merely submitting a purported "search protocol" may not be enough to insulate the government from a Fourth Amendment violation. This is important because this is precisely *why* the Court is requesting the search protocol in the first place. The Court is trying to find out if the government is conducting its searches in a reasonable way at the present moment.[104]

With that in mind, on a scale between *In re Search of Black iPhone* and *IMEI*, *supra* Sections B. 1 & 2, the present application falls somewhere in between. The government must provide the court with a search methodology substantially more detailed than the one provided here. Such methodology should reflect the questions presented in *In re Search of Black iPhone* and its progeny, as well as the questions raised in this opinion.

---

[103] *Id*. at 21–22.

[104] This Court is comfortable with the fact that the Supreme Court may later decide that the conduct found in a search protocol that this Court *does* authorize is improper.

If the Court were to authorize this warrant, it would be contradicting the manifest purpose of the Fourth Amendment particularity requirement, which is to prevent general searches.[105] "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[106]

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

IT IS SO ORDERED.

Dated in Kansas City, Kansas on this 26th day in June, 2014.

s/ David J. Waxse
DAVID J. WAXSE
U.S. Magistrate Judge

[105] *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).
[106] *Riley*, *supra* note 15 at 28.