UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

IN THE MATTER OF THE SEARCH OF:

Case No. l4-MJ-8017-DJW

Cellular Telephones within Evidence Facility
Drug Enforcement Administration, Kansas
City District Office

MEMORANDUM AND ORDER
DENYING APPLICATION FOR SEARCH WARRANT

The Court has been asked to issue a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure for the contents of cell phones that are currently in the custody of the United States Drug Enforcement Agency ("DEA"). Based on this Court's previous rulings and other case law, this request has been denied without prejudice. This memorandum will more explicitly explain the reasons for the denial and what process would allow the warrant to be issued.

I. BACKGROUND

As part of its investigation of possible violations of 21 U.S.C. §§ 841(a)(1), 843(b) and 846, the Government submitted an application for a search warrant seeking information stored on five (5) cellular phones. In the accompanying affidavit, the DEA Task Force agent alleges there is probable cause to believe the cellular phones were used in connection with and contain evidence of such violations. Thus, the Government requests authorization to search the devices and seize any names, addresses, telephone numbers, text messages, digital images, video depictions, or other identification data or communications that are evidence of violations of 21 U.S.C. §§ 841(a)(1), 843(b) and 846.

Previously, the Court denied a government search warrant application for email communications and 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."[1] Thereafter, the Court expanded and applied that same rationale to two cases involving search of cell phones: *In re Search of Nextel Cellular Telephone* ("Cellular")[2] and *In re Search of Three Cellphones and One Micro-SD Card* ("Three Cellphones").[3]

In *Cellular*, the government submitted a search warrant application that included what it called a "Search Methodology,"[4] which attempted to explain how searches on the already lawfully seized cellphones would be conducted. The Court explained that *Riley v. California*[5] supported the Court's request for a search protocol.[6] Accordingly, the Court denied the government's application because it violated the probable cause and particularity requirements of the Fourth Amendment.

In *Three Cellphones*, the government submitted a search warrant application that did not include a search methodology. On that ground, alone, the Court could have denied the search warrant application. Instead, the Court further explained its *Cellular*

---

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

[2] No. 14-MJ-8005-DJW, 2014 WL 2898262 (D. Kan. June 26, 2014), *available at* https://ecf.ksd.uscourts.gov/cgi-bin/show_public_doc?2014mj8005-2.

[3] No. 14-MJ-8013-DJW, 2014 WL 3845157 (D. Kan. Aug. 4, 2014), *available at* https://ecf.ksd.uscourts.gov/cgi-bin/show_public_doc?2014mj8013-2.

[4] "Search Methodology" and "search protocol" are interchangeable terms. For consistency vis-à-vis other opinions, this opinion will use "search protocol."

[5] *Riley v. California*, 134 S. Ct. 2473 (2014) (*Riley* was a landmark Fourth Amendment case involving the search of cellular phones incident to a lawful arrest).

[6] *Cellular*, *supra* note 2.

rationale by clarifying why it requested a search protocol. Because searches of electronically stored information—be it a cell phone, thumb drive, or computer hard drive—expose substantial amounts of private, personal data to the government, an "explanation of the government's search techniques is being required in order to determine whether the government is executing its search in both good faith and in compliance with the probable cause and particularity requirements of the Fourth Amendment."[7]

Currently pending before the Court is a DEA search warrant application for five cell phones. Like *Three Telephones*, the government's application lacks a search protocol. Thus, the Court cannot grant the government's application. In an effort to clarify its position, and in light of recent decisions outside this jurisdiction in which courts have granted search warrants in similar circumstances,[8] the Court would, once again, like to further explain its reasoning for requiring a search protocol before issuing a search warrant seeking to search devices containing electronically stored information.

II. DISCUSSION

A. The Constitutional Basis for the Court's Concerns

The Fourth Amendment guarantees the right of citizens against unreasonable searches and seizures:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated,

---

[7] *Three Cellphones*, *supra* note 3.

[8] *See In the Matter of a Warrant for All Content and Other Information Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc.*, No. 14 MAG 309, 2014 WL 3583529 (S.D.N.Y. July 18, 2014) ("S.D.N.Y. Opinion"); *In the Matter of the Search of Information Associated with [redacted]@mac.com That is Stored at Premises Controlled by Apple, Inc.*, No. 14-228, 2014 WL 4094565 (D.D.C. Aug. 8, 2014) ("D.D.C. Opinion").

> 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.[9]

The fundamental purpose of the Fourth Amendment is to "safeguard the privacy and security of individuals against arbitrary invasions by government officials."[10] "As the text makes clear, 'the ultimate touchstone of the Fourth Amendment is reasonableness.'"[11] "A search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing . . . reasonableness generally requires the obtaining of a judicial warrant."[12] Such a warrant must: (1) be issued by a neutral magistrate; (2) allow the magistrate to find probable cause to believe that the evidence sought will "'aid in a particular apprehension or conviction' for a particular offense;" and (3) describe with specificity the "'things to be seized,' as well as the place to be searched."[13]

The Supreme Court has established that judicial scrutiny of proposed search warrants "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 careful prior determination of necessity."[14] Determining probable cause in a warrant requires the "judicial officer [to] decide 'whether, given all the circumstances set forth in the affidavit before him, including the

---

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

[10] *Camara v. Mun. Court of City & Cnty. of San Francisco*, 387 U.S. 523, 528 (1967).

[11] *Riley*, *supra* note 5 (quoting *Brigham City v. Stuart*, 547 U. S. 398, 403 (2006) (internal quotation marks omitted)).

[12] *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995).

[13] *Dalia v. United States*, 441 U.S. 238, 255 (1979) (quoting *Warden v. Hayden*, 387 U.S. 294, 307 (1967); *Stanford v. Texas*, 379 U.S. 476, 485 (1965)).

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

veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.'"[15]

The Fourth Amendment particularity requirement enables the court to "ensure 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."[16] It also assures both the court and 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.[17] "To determine if the *place* to be searched is particularly described, courts ask "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.'"[18] To determine if the *things* to be seized are particularly described, there must be language in the warrant that creates a nexus between the suspected crime and the things to be seized.[19] Thus, the description of the items to be seized must be confined to "particularly described evidence relating to a specific crime for which there is demonstrated probable cause."[20] Taking the above together, 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

---

[15] *United States v. Warren*, 42 F.3d 647, 652 (D.C. Cir. 1994) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)).

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

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

[18] *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)).

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

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

> undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase.[21]

The manifest purpose of the Fourth Amendment particularity requirement is to prevent the Framers' chief evil: general searches.[22] A general search "le[aves] to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched . . . [and] provide[s] no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular home."[23] A warrant must provide the officer conducting the search with sufficiently precise language to allow him to determine which items are properly subject to seizure and which items are irrelevant.[24] Thus, "'[t]he requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another."[25] In other words, "[a]s to what is to be taken, nothing is left to the discretion of

---

[21] *Maryland*, *supra* note 16, at 84–85 (citing *United States v. Ross*, 456 U.S. 798, 824 (1982)).

[22] *Id*. at 84. *See also Ashcroft v. al-Kidd*, 131 S. Ct. 2074, 2084 (2011) ("The Fourth Amendment was a response to the English Crown's use of general warrants, which often allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes or affronts to the Crown."); *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013).

[23] *Steagald v. United States*, 451 U.S. 204, 220 (1981); *Coolidge*, *supra* note 14, at 467 ("general exploratory rummaging of a person's belongings.").

[24] *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?"); *accord. United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) (Stating that a request to search must be accompanied by "sufficiently specific guidelines for identifying the documents sought . . . [to be] followed by the officers conducting the search.")

[25] *Stanford*, *supra* note 13, at 485 (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)).

the officer executing the warrant."[26] Preventing the issuance of general warrants in the context of electronically stored information ("ESI") has been the chief aim of this Court's recent opinions.

B. Applying Constitutional Protections in the Digital Era

As technology continues to evolve at a rapid pace, applying the Fourth Amendment requirements to search warrants for ESI has become increasingly difficult.[27] The absence of guidance from the Supreme Court and lack of agreement among lower courts have resulted in conflicting approaches to these types of warrants around the country. Though these various approaches have given rise to some confusion on the issue, one thing remains clear: a court's objective in deciding whether to authorize a search is to strike the proper balance "between protecting an individual's right to privacy and ensuring that the government is able to prosecute suspected criminals effectively."[28] In its previous opinions, this Court has attempted to strike this balance by requiring that a warrant contain sufficiently particular limits and boundaries on the scope of the proposed search and seizure.

Although the Supreme Court has not specifically addressed the particularity requirement in the context of cell phones, both *United States v. Jones*[29] and *Riley v.*

---

[26] *Marron*, 275 U.S. at 196.

[27] Even Fed. R. Crim. P. 41 itself provides little guidance on the subject. The Advisory Committee notes to the 2009 amendment of Rule 41 explain that "[t]he amended rule does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development."

[28] *United States v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006).

[29] 132 S. Ct. 945 (2012).

California[30] highlight the Supreme Court's concerns regarding emerging technologies vis-à-vis the Fourth Amendment. Read together, *Jones* and *Riley* explain why a search protocol is necessary and bolster this Court's interpretation of the Fourth Amendment's particularity requirement.

Because of their vast storage capacity and ability to store many different types of information, the Supreme Court characterizes cell phones as "hold[ing] for many Americans 'the privacies of life.'"[31] The Court acknowledges that modern cell phones 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."[32] Until recently, "people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception."[33]

With technological developments moving at such a rapid pace, Supreme Court precedent is and will inevitably continue to be absent with regard to many issues district courts encounter. As a result, an observable gap has arisen between the well-established rules lower courts *have* and the ones they *need* in the realm of technology. Courts cannot, however, allow the existence of that gap to infiltrate their decisions in a way that compromises the integrity and objectives of the Fourth Amendment. As the Supreme Court stated in *Riley*, "[t]he 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

[30] 134 S. Ct. 2473 (2014).
[31] *Id*. at 2494–95 (internal citation omitted).
[32] *Id*. at 2484.
[33] *Id*. at 2490.

for which the Founders fought."[34] The danger, of course, is that courts will rely on inapt analogical reasoning and outdated precedent to reach their decisions. To avoid this potential pitfall, courts must be aware of the danger and strive to avoid it by resisting the temptation to rationalize the application of ill-fitting precedent to circumstances.

The Supreme Court has demonstrated an acute awareness of the fact that the foregoing problem could have potentially dire implications with regard to an individual's constitutionally protected right to privacy. Justice Sotomayor's "mosaic theory"[35] concurrence in *Jones* cautioned that recent technological advances implicate substantial amounts of data regarding a person's private life: "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[36] *Riley* points out that GPS is a standard feature of modern cellphones and the "[d]ata on a cell phone can also reveal where a person has been. . . [so as to] reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."[37]

And that is just the GPS data.[38] Cell phones "could easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions,

---

[34] *Id*. at 2494–95.

[35] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012).

[36] *Jones*, *supra* note 29 ("[d]isclosed . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on[.]") (quoting *People v. Weaver*, 909 N.E.2d 1195, 1199 (2009)).

[37] *Riley*, *supra* note 5, at 2491.

[38] *See id*. ("Mobile application software on a cell phone, or "apps," offer a range

maps, or newspapers."[39] As the Supreme Court noted, cell phones are "minicomputers that also happen to have the capacity to be used as a telephone"[40] with "[o]ne of the most notable distinguishing features [being] their immense storage capacity."[41] The Court further recognized that the location of and manner in which individuals store their private information has changed drastically with the evolution of technology:

> In 1926, Learned Hand observed … that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contain a broad array of private information never found in a home in any form – unless the phone is.[42]

After years of lower courts analogizing cell phones to cigarette packs or tape recorders, *Riley* recognized that it is 2014, not 1973,[43] and the analogy no longer holds water.

Although the foregoing passage references cell phones specifically, the Supreme Court's conclusion holds true for other forms of modern technology including, yet certainly not limited to, computer hard drives.[44] As with cell phones, this Court

---

of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life.")

[39] *Id*. at 2489.

[40] *Id*.

[41] *Id*.

[42] *Id*. at 2490–91 (internal citation omitted) (emphasis in original).

[43] *See United States v. Robinson*, 414 U.S. 218 (1973).

[44] *See Galpin, supra* note 22, at 447 ("Where, as here, the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance. As numerous courts and commentators have observed, advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain."); *United States v. Payton*, 573 F.3d 859, 861–82 (9th Cir. 2009) ("There is no

recognizes that searches of hard drives cannot rest upon analogical reasoning based on precedent that largely predates the modern computing era.[45] As we develop into an increasingly digital society, it comes as no surprise that examination of an individual's electronic footprint could reveal vastly more about his life than would a search of his home. It is now easier than ever to digitally store immense quantities of personal information and to share that information among multiple devices; a modern cell phone can be synced with a personal computer, tablet, or other device so that a person can access all of his information whenever he likes from wherever he likes. This ability is a convenience, to be sure, but it also increases the risk that, given an unrestricted warrant, the government will be able to access a plethora of information which it has no constitutional foundation to view. As the Tenth Circuit has recognized, "[s]ince 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."[46] Practically, cell phones make for equally, if not more tempting targets than computers, as they are usually kept on an individual's person, used

---

question that computers are capable of storing immense amounts of information and often contain a great deal of private information. Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (noting a computer's potential "to store and intermingle a huge array of one's personal papers in a single place").

[45] *See United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) ("Relying on analogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.'") (quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 104 (1994)); Orin Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 569 (2005) (Computers "are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more.").

[46] *Carey*, *supra* note 45, at 1275.

relatively continuously, rarely turned off, and able to keep a comprehensive log of an individual's interactions and movements in real time.

Further, cell phones allow a person to access a wide variety of personal data stored with third party Internet service providers ("ISP"), such as email accounts, social media accounts, and accounts dedicated specifically to the end of going entirely digital. Applications like Dropbox and Google Drive utilize cloud computing to allow users to centralize their data storage so that it can be accessed remotely from any device with an Internet connection. These developments are indicative of both the remarkable progress being made in the technological sphere, and the challenge courts face in applying precedent to an increasingly complex and technologically-advanced world. As the practices of syncing devices and using the cloud become more prevalent, the ability of courts to limit the scope of proposed warrants to places and things for which the government has probable cause to search becomes far more difficult. A warrant for the search of an individual's cell phone may, in some cases, be practically equivalent to a warrant for the search of the individual's entire digital presence wherever found. The question then becomes: does a warrant authorizing the search of a cell phone also authorize the search of data, *accessible via* the cell phone, but not actually *stored* there? If so, the potential for abuse becomes abundantly clear. For instance, in *Riley*, the government conceded that the search of a cell phone incident to arrest may not include "a search of files in the cloud."[47] "Such a search," the Court stated, "would be like finding a

[47] *Riley*, *supra* note 5, at 2491.

key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[48]

Some courts have already allowed this practice, to a certain degree, with regard to email accounts. The information contained in email accounts is stored with an ISP, but is accessible via many modern cell phones. Email accounts can contain a vast amount of various types of personal information, which render them, for purposes of Fourth Amendment analysis, very similar to cell phones and hard drives.[49] Given this similarity, it seems counterintuitive that a warrant should be required for the search of a cell phone, but not for the search of an email account, simply because the email account is accessible via the cell phone.

The prospective dangers of unrestricted warrants are innumerable.[50] For instance, if the government desires to search an individual's hard drive, but cannot establish probable cause to do so, it could likely obtain a search warrant for the individual's cell phone instead.[51] Given the understanding that personal devices are often networked and/or are sharing information in the cloud, the government could potentially access the information it sought from the hard drive via the cell phone,

---

[48] *Id.*

[49] *See United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010) ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."); *S.D.N.Y. Opinion*, *supra* note 8 ("We perceive no constitutionally significant difference between the searches of hard drives [ ] and searches of email accounts.").

[50] *See In re Appeal of Application for SEARCH WARRANT*, 193 Vt. 51, 85, 71 A.3d 1158, 1181 (2012)("In re Search Warrant") (citing *United States v. Gourde*, 440 F.3d 1065, 1077–78 (9th Cir. 2006) ("There are just too many secrets on people's computers, most legal, some embarrassing, and some potentially tragic in their implications, for loose liberality in allowing search warrants.").

[51] *See Warshak*, *supra* note 49, at 2492. ("It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found a cell phone.")

essentially circumventing the Fourth Amendment's probable cause requirement.[52] The practical effect of these types of warrants, if granted without further limitation as to their scope, would be that every warrant issued for the search of ESI would give the government carte blanche to examine the entirety of an individual's digital presence with impunity. This effect would plainly be an affront to the Fourth Amendment as contemplated by the Founders. Thus, the Fourth Amendment particularity requirement takes on increased importance with regard to the search and seizure of ESI, and courts must take special care when authorizing a warrant in these cases.[53]

Of course, the Fourth Amendment's text must be malleable to the practical realities of modern day searches.[54] "The fact of an increasingly technological world is not lost upon us as we consider the proper balance to strike between protecting an individual's right to privacy and ensuring that the government is able to prosecute suspected criminals effectively."[55] After all, "[t]he warrant process is primarily concerned with identifying *what* may be searched or seized – not how."[56] Thus, a warrant's execution is "generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized

---

[52] *See e.g., United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) ("Where computers are not near each other, but are connected electronically, the original search might justify examining files in computers many miles away, on a theory that incriminating electronic data could have been shuttled and concealed there.").

[53] *See Otero*, *supra* note 44, at 1132; *Galpin*, supra note 22, at 447 (discussing the need for "a heightened sensitivity to the particularity requirement in digital searches").

[54] *See United States v. Burgess*, 576 F.3d 1078, 1094 (10th Cir. 2009) ("[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.'").

[55] *Adjani*, *supra* note 28, at 1152.

[56] *United States v. Upham*, 168 F.3d 532, 537 (1st Cir. 1999) (emphasis in original).

by warrant[,]"[57] and "the manner in which a warrant is executed is subject to *later* judicial review as to its reasonableness."[58] Some courts have pointed out that, in many ways, requesting a search protocol before issuing a warrant is putting the cart before the horse.[59] On this point, there are a few important things to note.

First, while it may be true that the reasonableness of the manner of search is subject to ex post judicial determination, it is important to recognize that "[t]here is interplay between probable cause, particularity, and reasonableness that judicial officers reviewing a warrant application must consider in authorizing a form of privacy invasion."[60] Admittedly, "[n]othing in the language of the Constitution or in th[e] Court's decisions interpreting that language suggests that, in addition to the requirements set forth in the text [of the Fourth Amendment], search warrants also must include a specification of the precise manner in which they are to be executed."[61] However, "[n]othing in the Fourth Amendment *precludes* a magistrate from imposing ex ante warrant conditions to further constitutional objectives such as particularity in a warrant and the least intrusion necessary to accomplish the search."[62] In cases where this Court has required ex ante search protocol, it has been not *in addition to* the requirements of the Fourth Amendment, but *in satisfaction of* them. This use of ex ante restrictions in search

---

[57] *Dalia*, *supra* note 13, at 257.
[58] *Dalia*, *supra* note 13, at 258 (emphasis added).
[59] *See D.D.C. Opinion*, *supra* note 8; *S.D.N.Y. Opinion*, *supra* note 8.
[60] *In re Search Warrant*, *supra* note 50, at 1172.
[61] *United States v. Grubbs*, 547 U.S. 90, 97-98 (2006) (citation omitted; some bracketing in original).
[62] *In re Search Warrant*, *supra* note 50, at 1186 (citing *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976); *United States v. Payton*, 573 F.3d 859, 864 (9th Cir. 2009)) (Burgess, J., concurring and dissenting) (emphasis added).

warrants is far from a novel concept.[63] And, while the Court recognizes that the nature of ESI makes satisfaction of the Fourth Amendment requirements inherently more difficult than in traditional contexts involving the search and seizure of physical objects, it cannot be said to be entirely uncharted territory. As the Supreme Court of Vermont noted:

> [T]he need for a nonphysical concept of particularity is one that the courts have already confronted. Warrants for electronic surveillance routinely set out "minimization" requirements—procedures for how and under what conditions the electronic surveillance may be conducted—in order to "afford[ ] similar protections to those that are present in the use of conventional warrants authorizing the seizure of tangible evidence."
> …
> These provisions in the warrants are ex ante conditions on how a search may be conducted, but we believe they are well within the scope of a judicial officer's role in ensuring that searches are targeted with sufficient particularity. The same reasoning applies with even more force in the computer context.[64]

This Court agrees. In making a particularity determination with regard to a warrant for ESI, reasonableness of the manner of search is necessarily implicated because particularity and reasonableness are functionally related. A proposed warrant must particularly describe both the place to be searched and the things to be seized. "As the description of such places and things becomes more general, the method by which the search is executed becomes more important – the search method must be tailored to meet allowed ends."[65] It would be a "serious error," then, "to infer from the fact that we must often evaluate ex post whether a search sufficiently respected a citizen's privacy to the

---

[63] *Id*. at 1169–70. ("Even in traditional contexts, a judicial officer may restrict a search to only a portion of what was requested – a room rather than an entire house, or boxes with certain labels rather than an entire warehouse. In other words, some ex ante constraints – of the form 'here, not there' – are perfectly acceptable.")

[64] *Id*. at 1170–71 (internal citation omitted). *See also Otero*, *supra* note 44, at 1132 ("[W]arrants for computer searches must affirmatively limit the search" to keep it within the bounds of the Fourth Amendment.") (internal citation omitted).

[65] *Burgess*, *supra* note 54, at 1094.

conclusion that we can make no ex ante judgments about what sort of privacy invasions are and are not warranted."[66]

The second point to note is that the Court is not requesting a search protocol in order to dictate how the warrant is executed.[67] This Court readily acknowledges that not every search is created equal and not every warrant must include search protocol to comply with the Fourth Amendment. The government is free to determine the best procedures and techniques to use, so long as the government provides notice as to what the procedures are.[68] This notice, in the form of an enumerated search protocol, helps the court to determine if the proposed warrant satisfies the requirements of the Fourth Amendment, that is, whether the search and seizure requested will be governed by sufficient boundaries and limits to ensure the protection of the Fourth Amendment rights of the individual whose property is subject to the warrant.

---

[66] *In re Search Warrant*, *supra* note 50, at 1172; *See also S.D.N.Y. Opinion*, *supra* note 8 ("As for whether the Court should give direction as to the manner in which the government conducts the search of the emails, we will again assume without deciding that a court has the power to include protocols in a warrant as to the type of search to be conducted."); *United States v. Cartier*, 543 F.3d 442, 447–48 (8th Cir. 2008) (acknowledging that "there may be times that a search methodology or strategy may be useful or necessary."); *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 957 (N.D. Ill. 2004) ("[W]hen deciding to issue a warrant that would involve the seizure and subsequent search of a home computer, a magistrate judge has the authority to require the government to set forth a search protocol that attempts to ensure that the search will not exceed constitutional bounds."); Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. In Brief 1 (2011) (arguing that ex ante restrictions may be necessary in searches of electronic evidence to ensure that the Fourth Amendment's particularity and probable cause requirements are met).

[67] *See In the Matter of the Search of Apple iPhone, IMEI 013888003738427* ("IMEI"), No. 14-278 (JMF), 2014 WL 1239702, at *7 (D.D.C. Mar. 26, 2014).

[68] Perhaps it is best viewed like the Court, *sua sponte*, serving the government with a motion for a more definite statement.

Simply put, "[p]articularity is the requirement that the warrant must clearly state what is sought."[69] The Tenth Circuit has established the general standard for evaluating when the Fourth Amendment's particularity requirement 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 the 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.[70]

The government must provide the court with as specific a description of the place to be searched and the things to be seized as the circumstances reasonably allow. Failure to do so "offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary."[71] ESI, by its nature, makes this task a complicated one.[72] Regarding the place to be searched, the Supreme Court of Vermont adeptly noted that, "[i]n the digital universe, particular information is not accessed through corridors and drawers, but through commands and queries. As a result, in many cases, the only feasible way to specify a

---

[69] *S.D.N.Y. Opinion*, *supra* note 8 (citing *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006)).

[70] *United States v. Leary*, 846 F.2d 592, 600 (10th Cir. 1988) (internal quotations and citations omitted).

[71] *Galpin*, *supra* note 22, at 446 (quoting *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992).

[72] See Nichole Freiss, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance*, 90 Neb. L. Rev. 971, 987 (2012) (discussing how the "difference between the physical and digital worlds" makes the sufficiency of the description in a search warrant a complicated thing to assess).

particular 'region' of the computer[73] will be by specifying how to search."[74] Similarly, in attempting to describe the things to be seized, "[o]ften the way to specify particular objects or spaces will not be by describing their physical coordinates but by describing how to locate them."[75] By providing a search protocol explaining how it will separate what is permitted to be seized from what is not, the government can more easily and satisfactorily explain to the court how it will decide where it is going to search. In doing so, the government should not compromise the thoroughness of its description by trying to avoid the use of technical language. In fact, the court *wants* a "sophisticated technical explanation of how the government intends to conduct the search so that [it] may conclude that the government is making a genuine effort to limit itself to a particularized search."[76] The search protocol is "squarely aimed at satisfying the particularity requirement of the Fourth Amendment"[77] and must be as detailed as specifically as possible to do so.

The final point of note is that, without a search protocol, *ex ante*, the balance—between an individual's right to privacy and the government's ability to efficiently and

---

[73] The same holds true for other forms of ESI. In the context of cell phones, for instance, it is insufficient to describe the place to be searched as merely an iPhone with a specific IMEI number; the warrant must specify which sectors or blocks of the phone it will search. *See Cellular*, *supra* note 2; *IMEI*, *supra* note 67; *State v. Henderson*, 289 Neb. 271, 290 (2014) (holding that a warrant authorizing the search of a cell phone's call logs, texts, voicemail and "any other information that can be gained from the internal components and/or memory cards" was not particular enough to satisfy the requirements of the Fourth Amendment).

[74] *In re Search Warrant*, *supra* note 50, at 1171.

[75] *Id*. at 1170.

[76] *IMEI*, *supra* note 67 (citing *In the Matter of the Search of Odys Loox Plus Tablet, Serial Number XXXXXXXXXXXX, In Custody of United States Postal Inspection Service, 14001 New York Ave NW, Washington, DC* ("Odys Loox"), Mag. Case No. 14-265, 2014 WL 1063996 (D.D.C. Mar. 20, 2014).).

[77] *See id*.

effectively investigate crimes—swings too far in favor of the government. One of the main ways courts have balanced these interests with regard to ESI is by permitting the government to copy an individual's hard drive for off-site review,[78] a practice authorized in certain circumstances by Rule 41 of the Federal Rules of Criminal Procedure.[79] Use of this two-step process implicates another necessary facet of the use of ex ante restrictions in the satisfaction of the Fourth Amendment. To be certain, "[m]ere convenience does not allow the government to violate the Fourth Amendment and seize data wholesale."[80] However, this court recognizes that there are circumstances where "[a]s a practical matter, the Court cannot imagine that an image would not be created."[81] Thus, if the government can affirmatively show that imaging and off-site review is necessary to effectively facilitate its investigation, the court may authorize the use of the two-step process provided that it is otherwise constitutional. As with every warrant, the court has an obligation to make certain that the search and seizure contained therein complies with

---

[78] *See e.g. United States v. Ganias*, 755 F.3d 125, 135 (2d Cir. 2014) ("In light of the significant burdens onsite review would place on both the individual and the Government, the creation of mirror images for offsite review is constitutionally permissible in most instances, even if wholesale removal of tangible papers would not be."); *United States v. Schesso*, 730 F.3d 1040, 1046 (9th Cir. 2013) (upholding government's seizure of electronic data for a subsequent off-site search where there was a fair probability that evidence would be found on the defendant's personal computer and other electronic devices); *United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012) ("The federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a 'sufficient chance of finding some needles in the computer haystack.'") (quoting *Upham*, *supra* note 56, at 535.)).

[79] *See* Fed. R. Crim. P. 41(e)(2)(B)

[80] *In the Matter of the Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.* ("[Redacted]@mac.com"), No. 14-228 (JMF), 2014 WL 1377793, at *155 (D.D.C. Apr. 7, 2014), *vacated sub nom. Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, No. 14-228, 2014 WL 4094565 (D.D.C. Aug. 8, 2014).

[81] *IMEI*, *supra* note 67.

the Fourth Amendment. When it authorizes use of the two-step process, the court is allowing the government to copy all of the information on the device, even though the copy will inevitably include data that falls outside the scope of the search warrant. While the court is willing to do so in some circumstances, "the reality that over-seizing is an inherent part of the electronic search process requires th[e] Court to exercise greater vigilance in protecting against the danger that the process of identifying seizable electronic evidence could become a vehicle for the government to gain access to a larger pool of data that it has no probable cause to collect."[82]

Accordingly, the court must ensure that the search warrant reflects the exact scope of the government's authority to mitigate the potential for abuse as a result of authorizing of what is, in practical effect, an unconstitutionally broad search and seizure.[83] Limitations must exist "to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases."[84] The most efficient way for the court to ensure the constitutionality of the investigation is to require the government to disclose, ex ante, a proposed search protocol explaining not only "how it will perform the search and ensure that it is only searching sectors or blocks of the drives that are most likely to contain the data for which there is probable cause[,]"[85] but also "[w]hether the target devices [will] be imaged in full, for how long those images will be kept, and what will happen to data that is seized but is ultimately determined not to be

---

[82] *Id*. (internal citations omitted).

[83] *See Hill*, *supra* note 69, at 976–77 (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).

[84] *Comprehensive Drug Testing*, *supra* note 52, at 1170.

[85] *[Redacted]@mac.com*, *supra* note 80.

within the scope of the warrant."[86]

The facts of *United States v. Ganias* bear out the serious risks of what can happen when a court fails to use minimization procedures and/or procedural safeguards to limit the amount of ESI to be seized and to provide for the appropriate treatment of non-responsive data.[87] There, the government seized a computer, but did not purge, delete, or otherwise return the non-responsive files.[88] The government "retain[ed] them for another year-and-a-half until it finally developed probable cause to search and seize them in 2006."[89] The government then used that evidence in future criminal investigations.

This scenario is precisely what concerned Justice Sotomayor in *Jones*—the "[g]overnment can store such records and efficiently mine them for information years into the future."[90] As the court pointed out in *Ganias*, even if off-site review is justified under the circumstances, it does not provide an "independent basis for retaining any electronic data other than [those] specified in the warrant."[91] Without such an independent basis,[92] the prolonged retention and future use of such data by the

---

[86] IMEI, *supra* note 67.

[87] *Ganias*, *supra* note 78, at 139. *See also* Ben Barnett and Rebecca S. Kahan, *Judicial Battles Over Criminal Subpoenas for Online Data* (Sept. 9, 2014) *available at* http://www.law.com/sites/articles/2014/09/09/judicial-battles-over-criminal-subpoenas-for-online-data/ (explaining that *Ganias* "perfectly illustrates why court-imposed minimization procedures and secondary orders should demarcate the government's access to and use of ESI").

[88] *Id.* at 129.

[89] *Id.* at 138.

[90] *Jones*, *supra* note 29, at 955–56 (citing *United States v. Pineda-Moreno*, 617 F.3d 1120 (9th Cir. 2010) (opinion of Kozinski, C.J.)).

[91] *Ganias*, *supra* note 78, at 136 (citing *Comprehensive Drug Testing*, *supra* note 52, at 1171).

[92] This Court is unpersuaded by the contention that retaining information outside the scope of the warrant in order to preserve the chain of custody is such an "independent basis." See *Odys Loox*, *supra* note 76 (advising that, in such a case, a "testifying individual need only say that, in compliance with this Court's rulings, the image is

government is clearly unconstitutional[93] because "[i]f the Government could seize and retain non-responsive electronic records indefinitely, so it could search them whenever it later developed probable cause, every warrant to search for particular electronic data would become, in essence, a general warrant."[94]

Moreover, "[b]ecause the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools."[95] Justice Sotomayor cautioned that "because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary check[ ] that constrain[s] abusive law enforcement practices: 'limited police resources[.']"[96] The same is true of searching cellular phones, email accounts, and hard drives in 2014. What used to take massive amounts of time and manpower can be done by law enforcement tech teams significantly faster and more efficiently. These sophisticated new techniques, including metadata filtering, predictive coding, and other forms of technology-assisted review, are immensely advantageous for the government in terms of efficiency. However, they also increase the risk that a search performed pursuant to an unrestricted warrant will effectively eviscerate an individual's right to privacy under the Fourth Amendment. By disclosing a proposed search protocol ex ante, the government is able to work with the court to make certain that the techniques it will use to make its investigation easier will also serve to refine its search as much as

---

complete except for non-relevant files, which were deleted from the image").

[93] *Ganias*, *supra* note 78, at 138.

[94] *Id.*

[95] *Id.* at 134.

[96] *Jones*, *supra* note 29, at 956.

possible in an effort to minimize the intrusion into an individual's private life and preserve the integrity of the Fourth Amendment.

On this note, this Court is aware that there is some opposition to the use of search protocol in warrants because of the risk that such limits "will unduly hamper detection of crime" by limiting its ability to carry out a dynamic investigation.[97] The Court finds this fear to be unfounded. As Judge John Facciola explains:

> Any concerns about being locked into a particular search protocol are unnecessary for two reasons. First, the government can always return for additional authorization of this Court as needed. Second, the application need only explain that some searches require additional techniques and that what is proposed is merely *what the government intends to do at the time it submits its application, based on its experience searching such devices and in light of the particular data it seeks to seize*.[98]

On balance, this Court is far more willing to grant additional authorization based on a subsequent showing of particularized need, than it is to grant an initial application for a warrant granting the government unconstitutionally broad authority to search. The Court does not believe that requiring an ex ante protocol in the warrant will impede the government's investigations in any way.

Finally, *Ganias* also illustrates the ineffectiveness of only supplying judicial oversight, *ex post*. The Supreme Court held that the Constitution interposes, *ex ante*, "the deliberate, impartial judgment of a judicial officer" and provides "*ex post*, a right to suppress evidence improperly obtained and a cause of action for damages'" for an

---

[97] *See In re Search Warrant*, *supra* note 50, at 1182.

[98] *IMEI*, *supra* note 67 (emphasis in original). *See also In re Search Warrant*, *supra* note 50, at 1184–85 ("After exhausting its search options as permitted by the conditions of particularity, nothing precludes the State from seeking a new warrant to employ more sophisticated search techniques or a more probing analysis of the electronic media based on the results – or frustration – of their initial search, providing probable cause remains.").

unreasonable search.[99] Additionally, Rule 41(g) of the Federal Rules of Criminal Procedure "likely provide[s] a remedy in addition to suppression and a civil damages suit once the owner of the electronic information has notice of the seizure."[100] While it is true that "ex post review will always remain open, [ ] this does not mean that [ ] ex ante instructions are without legal significance."[101] While ex post remedies are aimed at mitigating harm resulting from an unconstitutional search and seizure, ex ante restrictions help ensure that no violation of an individual's Fourth Amendment rights takes place at all. The fact of the matter is that a court is attempting to avoid entirely the harm that ex post remedies are meant to assuage. By only deciding reasonableness of the government's actions *ex post*, the government not only possesses a substantial portion of an individual's private life, but it also fails to prevent a person from having to defend against subsequent unreasonable searches stemming from the initial search and seizure. Requiring search protocol in a warrant allows the court to more effectively fulfill its duty to render, as the Supreme Court put it, a "deliberate, impartial judgment" as to the constitutionality of the proposed search, thus avoiding the need for ex post remedies resulting from an unconstitutional search.

III. CONCLUSION

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.[102] Given the substantial amount of data collected by the government upon searching or seizing a cell phone, as discussed in *Riley*, requesting an unrestricted search

---

[99] *Grubbs*, *supra* note 61, at 99.
[100] *S.D.N.Y. Opinion*, *supra* note 8, at 18.
[101] *In re Search Warrant*, *supra* note 50, at 1182.
[102] *Maryland*, *supra* note 16, at 84.

is tantamount to requesting disclosure of a vast array of intimate details of an individual's private life.[103] For the reasons discussed in this opinion, to issue this warrant would swing the balance between an individual's right to privacy and the government's ability to effectively investigate and prosecute crimes too far in favor of the government.

Accordingly, the Court again finds that "an explanation of the government's search techniques is being required in order to determine whether the government is executing its search in both good faith and in compliance with the Fourth Amendment."[104] The Court does not believe that this request will overburden the government. In fact, in *Riley*, the government advocated—and it can be concluded that the Supreme Court endorsed—the implementation of search protocols:

> 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.[105]

It is this Court's belief that a search protocol is the most effective mechanism for determining whether the warrant and the search proposed therein are constitutional. In light of this Court's previous opinions and this opinion's further explanation as to why the Court is requesting a search protocol, the government's present search warrant application must be denied without prejudice. The government may resubmit its application for consideration once it includes a search protocol that addresses the concerns expressed in *Cellular, Three Cellphones,* and in this opinion.

IT IS SO ORDERED.

---

[103] *Riley*, *supra* note 5, at 2494–95.
[104] *Three Cellphones*, *supra* note 3.
[105] *Riley*, *supra* note 5, at 2491–92.

Dated this 30th day of December 2014, at Kansas City, Kansas.

s/ David J. Waxse
David J. Waxse
United States Magistrate Judge