UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE DIVISION

UNITED STATES OF AMERICA

vs. **Case No.: 3:13-cr-00058-99MMH-JRK**

RICHARD DALE BROOKS

DEFENDANT'S OBJECTIONS TO REPORT AND RECOMMENDATION

The Defendant, Richard Dale Brooks, by and through his undersigned counsel, and pursuant to 28 U.S.C. § 636(b)(1) and Fed. R. Crim. P. 59(b), hereby objects to the Report and Recommendation ("R&R") of the Magistrate Judge filed on October 18, 2013 (Doc. 72), recommending denial of Defendant's Motion to Suppress. (Doc. 39). Upon the District Court's *de novo* review, said Motion should be granted. Defendant adopts, reasserts, and incorporates his previously stated arguments and grounds for suppression. *See* (Docs. 39, 55, 68). Defendant's objections are set forth below.

I. The search warrant lacked particularity and was overbroad.

Defendant objects to the Magistrate Judge's conclusion that the search warrant was sufficiently particularized and not overbroad. The warrant was not adequately limited by reference to Defendant's alleged crime because only three provisions out of twelve in the warrant referenced child pornography.[1] Accordingly, the warrant wrongfully authorized an exploratory rummaging for anything that might lead to a basis to prosecute.[2]

---

[1] Defendant maintains that "nine of the warrant's numbered provisions nine (9) of the warrant's twelve (12) numbered items permitted the government to go on a fishing expedition". (Doc. 39 at 22 n. 13). Although Paragraph 9 references child pornography, it also authorized the government to search Defendant's *entire home* for any documents demonstrating an interest in the "sexual exploitation of children," an undefined phrase. This could include *Lolita* under

The scope of a lawful search must be limited to the areas in which the object of the search reasonably may be found. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). Additionally, a search warrant must particularly describe the place to be searched and items of persons to be seized. *United States v. Jenkins*, 901 F.2d 1075, 1081 (11th Cir. 1990). A description is sufficiently particular when it enables the searcher to reasonably ascertain and identify the things to be seized. *United States v. Santarelli*, 778 F.2d 609, 614 (11th Cir. 1985).

Here, the warrant contained numerous, unbounded, boilerplate provisions, such as paragraph (1), which authorized the government to seize and search "any and all computer equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic magnetic, optical, or similar computer impulses or data". (Doc. 72 at 8). This provision, along with the warrant's eleven (11) other provisions, should have been limited by reference to the underlying crime. *See United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010). Even assuming five out of the twelve provisions in the warrant were facially valid, severance of the valid and invalid portions is not an available remedy because the other seven items were facially invalid, the

---

Defendant's bed pillow even though "[t]he warrant stated there was probable cause to believe that a *computer* or other *digital device* capable of accessing the internet was knowingly used as an instrumentality of the crime of creating, possessing or promoting child pornography and contained evidence of that crime." (Doc. 72 at 8)(emphasis added). Because Paragraph 9 authorized an inadequately bounded search that exceeded the scope of probable cause, it was insufficiently particularized and overbroad. *See United States v. Rubinstein*, 09-20611-CR-GOLD, 2010 WL 2723186, at *8 (S.D. Fla. 2010) ("[o]verbroad warrants authorize the seizure of things for which there is no probable cause") (citation omitted); *Jenkins*, 901 F.2d at 1081. Likewise, Paragraph 8 is insufficiently particularized and overbroad because it permitted the government to seize and search *written* documents and its scope is solely limited by the undefined phrase "sexual exploitation of children". (Doc. 72 at 9).

[2] While search warrants can incorporate by reference the words of supporting documents if the documents are attached to the warrant, *see United States v. Pratt*, 438 F.3d 1264, 1270 (11th Cir. 2006), the warrant here does not expressly incorporate the supporting affidavit. Accordingly, the affidavit cannot cure any deficiencies in the warrant. *Groh v. Ramirez*, 540 U.S. 551, 557 (2004).

warrant's valid sections were indistinguishable from the invalid sections, and the warrant's invalid parts comprised a much greater part of the warrant than its valid parts. *See, e.g., Cassady v. Goering*, 567 F.3d 628, 640 (10th Cir. 2009) (invalidating warrant which contained "one mostly valid and two invalid provisions" after evaluating (1) the number of invalid versus invalid provisions, (2) whether the valid section was sufficiently distinguishable from the invalid sections, and (3) the relative scope and invasiveness of the valid and invalid parts of the warrant). There is no way to determine whether the warrant's relatively bounded provisions limit the expansive provisions or merely provide examples of some of the items the broad provisions authorize the government to seize and search.

The Magistrate was wrong to conclude: "The fact that some of the specific numbered items in the search warrant do not reference child pornography is unremarkable under the circumstances." (Doc. 72 at 17). It is simply not true that "the warrant in this case limited the search to computer equipment, digital storage devices, and accessories that could contain contraband and evidence linked to the child pornography offenses specified in the warrant." (Doc. 72 at 20). Without any reference to contraband or child pornography offenses, the warrant authorized the government to seize and search:

> 1. Computer hardware to include any and all computer equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devises (such as central processing units, personal computers to include "laptop" or "notebook" or "pocket" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).

(Doc. 72 at 8).

Yet, as previously noted, the warrant provides no basis for distinguishing its broad and relatively narrow provisions. For example, Item 3 authorized the government to seize and later search:

> Computer storage media and the digital content to include but not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography.

(Doc. 72 at 8). But item 1 authorized the government to seize and later search:

> Computer hardware to include *any and all computer equipment* used to collect, analyze, create, display, convert, store, conceal, or transmit electronic magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, personal computers to include "laptop" or "notebook" or "pocket" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).

(Doc. 72 at 9)(emphasis added) Thus, it is unclear what exactly the warrant permitted the government to do because there is no way to determine whether item 3 limits the scope of item 1 or whether item 1 expands the scope of item 3. The government may only have been authorized to seize internal and peripheral storage devices "which can be accessed by computers to store or retrieve data or images of child pornography," as item 3 states, or the government may have been authorized to seize "any and all" internal and peripheral storage devices, as item 1 states. The juxtaposition of items 1 and 12 elicits similar questions. Item 12 authorizes the search and seizure of:

> Data maintained on the computer, or computer related storage devices such as floppy diskettes, tape backups, computer printouts, and "zip" drive diskettes, in particular, data in the form of images and/or videos and any accompanying text associated with those images, and/or log files recording the transmission or storage of

> images, as they relate to violations of Florida law cited herein as related to the possession of distribution of child pornography.

(Doc. 72 at 9). However, much of the "data maintained on the computer, or computer related storage devices" also appears in item 1's unbounded list. It is not apparent which provision trumps the other and, therefore, whether the warrant actually extends to "any and all computer equipment used to collect … data," as item 1 states.[3]

The warrant's lack of particularity is especially problematic because the hard drive of a computer "is the digital equivalent of its owner's home, capable of holding a universe of private information." *United States v. Mitchell*, 565 F.3d 1347, 1352 (11th Cir. 2009) (internal quotation marks and citation omitted). *See also Rosa*, 626 F.3d at 61-62 ("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.") (citing *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009); *United States v. Abdellatif*, 758 F. Supp. 2d 183, 189 (W.D.N.Y. 2010) ("There is no 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. Cioffi*, 668 F. Supp. 2d 385, 391 (E.D.N.Y. 2009) (citation and internal quotation marks omitted)

[3] The dissonance between items 1 and 8 is also irreconcilable. Item 8 refers to: "Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, origin or distribution of images involving the sexual exploitation of children." (Doc. 72 at 9). But that seemingly limited grant of authority may be rendered moot – at least with respect to digital correspondence – by item 1's authorization to search and seize "any and all … fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices." (Doc. 72 at 8). Again, the warrant provides no guidance regarding which provision reigns supreme.

("The dawn of the Information Age has only heightened . . . [privacy] concerns. The risk of exposing intimate (and innocent) correspondence to prying eyes is magnified because "computers often contain significant intermingling of relevant documents with documents that the government has no probable cause to seize."); Lily R. Robinton, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 Yale J. L. & Tech. 311, 320 (2010) ("The obscure nature of the digital search, and the lack of any spatial correlation between the evidence sought and the files examined, can mask potential privacy violations. It is easy to discount the danger of the general digital search and argue complacently.").[4]

Moreover, the warrants in some of the cases the Magistrate cited to support the proposition that "[f]ederal courts applying a reasonableness analysis on a case-by-case basis have rejected most particularity challenges," (Doc. 72 at 17-18), limited the scope of the search and seizure they authorized by defining key terms relating to the alleged criminal activity. *United States v. Richards*, 659 F.3d 527 (6th Cir. 2011) (affidavit, which was incorporated in application for search warrant, defined "child pornography," "visual depiction," "minor," "sexually explicit

[4] Legislatures, like courts, are increasingly recognizing and limiting the unique threats to privacy presented by modern digital technology. *See* National Conference of State Legislatures, *Employer Access to Social Media Usernames and Passwords* (January 17, 2013), http://www.ncsl.org/issues-research/telecom/employer-access-tosocialmediapasswords.aspx ("Six states--California, Delaware, Illinois, Maryland, Michigan and New Jersey--enacted legislation in 2012 that prohibits requesting or requiring an employee, student or applicant to disclose a user name or password for a personal social media account. California, Illinois, Maryland, and Michigan laws apply to employers. California, Delaware, Michigan and New Jersey have laws that apply to academic institutions. In all, fourteen states introduced legislation in 2012 that would restrict employers from requesting access to social networking usernames and passwords of applicants, students or employees.").

conduct," and "child erotica" by reference to federal law)[5]; *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (one of two warrant provisions at issue included "[a]ny and all visual depictions, in any format or media, of minors engaging in sexually explicit conduct [*as defined by the statute*]") (emphasis added). In contrast, neither the warrant nor affidavit here defines "child pornography" or "sexual exploitation of children".

Therefore, the warrant here, which contains at least seven provisions that are not limited by reference to criminal activity and fails to define the critical phrases "child pornography" and "sexual exploitation of children," is analogous to warrants courts have deemed insufficiently particularized and thus invalid. *Rosa*, 626 F.3d at 62 ("The warrant was defective in failing to link the items to be searched and seized to the suspected criminal activity—i.e., any and all electronic equipment potentially used in connection with the production or storage of child pornography and any and all digital files and images relating to child pornography contained therein—and thereby lacked meaningful parameters on an otherwise limitless search of Rosa's electronic media."); *United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009) ("If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment's particularity requirement."); *United States v. Riccardi*, 405 F.3d 852 (10th Cir. 2005) (warrant facially invalid because it did not limit scope of search to child pornography); *United States v. Bianco*, 998 F.2d 1112, 1116 (2d Cir. 1993) (noting that the subject warrant, when viewed by itself, was impermissibly broad because it described "neither the precise items to be seized nor the possible crimes involved").

Defendant does not demand surgical precision in the search warrant. It would not have been difficult or complex for the government to craft a sufficiently particularized warrant. For

[5] Said affidavit is located on the Middle District of Tennessee's docket, 3:05–cr-00185 (Doc. 3-1 at 5).

example, the warrant could have authorized investigators to search and seize "any and all computer equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic magnetic, optical, or similar computer impulses or data *which may be used to receive, distribute, store or retrieve images of child pornography*." Likewise, the warrant could have authorized the government to search for "items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized, which pertain to the *use, receipt, storage, or retrieval of images of child pornography*." *See In re U.S.'s Application For A Search Warrant To Seize & Search Elec. Devices From Edward Cunnius*, 770 F. Supp. 2d 1138, 1145 (W.D. Wash. 2011) ("The requested warrant is, in essence, boundless. This is made evident by the fact that the government seeks authorization, among other things, to obtain 'all passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.' "). Additionally, the warrant could have defined the phrases "child pornography" and "sexual exploitation of children".

The Magistrate also incorrectly concluded that the warrant was not overbroad even though non-contraband items contained within the computers and hard drives were subject to seizure. (Doc. 72 at 21-22). A generalized seizure of files may be justified if the government establishes probable cause to believe that all of the files are likely to evidence criminal activity. *See generally United States v. Offices Known as 50 State Distrib. Co.*, 708 F.2d 1371, 1374 (9th Cir. 1983), *cert. denied*, 104 S.Ct. 1272 (1984); *Garrison*, 480 U.S. at 84 (The scope of a lawful search must be limited to the areas in which the object of the search reasonably may be found.). However, Defendant and Defendant's wife's seized bank statements, professional records, personal photographs, and music – all of which were foreseeably located on their seized

computers and hard drives – could not rationally be connected to Defendant's alleged criminal activity. They certainly could not satisfy the probable cause standard. *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (Probable cause to issue the warrant exists when, "given all the circumstances set forth in the affidavit before him," the judge can conclude "there is a fair probability that contraband or evidence of a crime will be found in a particular place."); *Rubinstein*, 09-20611-CR-GOLD, 2010 WL 2723186, at *8 ("[o]verbroad warrants authorize the seizure of things for which there is no probable cause") (internal citation omitted). At a minimum, agents could have at least attempted to identify computers and hard drives that fell within the scope of probable cause on-site. *See United States v. Khanani*, 502 F.3d 1281, 1290 (11th Cir. 2007), ("The testimony at the suppression hearing established that the agents attempted to identify computers that contained information that was responsive to the warrants and that they did not seize every computer that they encountered.").

In addition, Defendant objects to the Magistrate's conclusion that the warrant's failure to delineate a search protocol was acceptable. (Doc. 72 at 18). Though a search protocol may not invariably be necessary, the warrant here lacked any other boundaries to prevent an excessive seizure and exploratory rummaging, such as consistent reference to the alleged crime and definitions of key terms relating to the offense charged. *See Garrison* 480 U.S. at 84 ("manifest purpose" of Fourth Amendment's particularity requirement is to prevent broad exploratory searches). Because a different kind of selectivity is possible as to computer files, it should be followed. *See* 2 Wayne R. LaFave, Search and Seizure § 4.10 (4th ed. 2011). Accordingly, various courts favor warrants that require a targeted approach to computer searches because it minimizes the possibility that the government will use a warrant for a narrow list of items to justify a broad search and seizure. *See United States v. Campos*, 221 F.3d 1143, 1148 (10th Cir.

2000); *United States v. Gawrysiak*, 972 F. Supp. 853, 866 (D.N.J. 1997) *aff'd*, 178 F.3d 1281 (3d Cir. 1999). *See also Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 463 (5th Cir. 1994); *United States v. Orefice*, No. 98 CR. 1295 (DLC), 1999 WL 349701, *2 (S.D.N.Y 1999); *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*, 846 F. Supp. 11, 13 (S.D.N.Y. 1994); Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. at 108.

There are several reasons why this District and Circuit's precedent in *Maali* and *Khanani* is inapplicable to the facts here. *United States v. Maali*, 346 F. Supp. 2d 1226, 1246 (M.D. Fla. 2004), *aff'd sub nom*, *Khanani*, 502 F.3d 1281 ("While it may be preferable and advisable to set forth a computer search strategy in a warrant affidavit, failure to do so does not render computer search provisions unduly broad."). First, the warrant here contained few substantive limits on the government's search and seizure authority, but, in *Maali*, the warrant was neither overbroad nor insufficiently particularized because (among other reasons) it expressly limited the seizure to records, documents, and property "relating to the employment and harboring of illegal aliens." *Maali*, 346 F. Supp. 2d at 1234, 1240-1241. Accordingly, even without describing computer search methodology, the *Maali* warrant did not authorize government conduct resembling a general search – at least not to the same extent as the warrant here.

Second, *Maali*'s holding should be limited to its facts. Defendants in that case were charged with crimes involving the employment and harboring of aliens and tax evasion, and the court repeatedly limited its analysis to crimes relating to fraud. *See Id*. at 1240-41 ("[A]t least in cases involving fraudulent schemes where the proof of guilt involves the piecing together of seemingly innocuous documents, some breadth and generality in warrant descriptions have been tolerated."); *Id*. at 1242 ("[I]n cases . . . involving complex financial transactions and widespread

allegations of various types of fraud, reading the warrant with practical flexibility entails an awareness of the difficulty of piecing together the paper puzzle.") (internal citation and quotation marks omitted); *Id*. at 1243-44 (rejecting particularity challenge to warrant after citing to the following cases, all of which involved fraud: *Andresen*, 427 U.S. at 479–81, *Wuagneux,* 683 F.2d at 1350 n. 5, *United States v. Majors,* 196 F.3d 1206, 1216 (11th Cir. 1999), *United States v. Sawyer,* 799 F.2d 1494, 1508–09 & n. 15 (11th Cir. 1986), *United States v. Santarelli,* 778 F.2d 609, 613–14 (11th Cir. 1985), *United States v. Weinstein,* 762 F.2d 1522, 1531–32 (11th Cir. 1985), *United States v. Blum,* 753 F.2d 999, 1001 (11th Cir. 1985)). No fraud is alleged here.

Third, the court's decision in *Khanani* not to require a written search protocol was at least in part based on the fact that the government's subsequent search and seizure was bounded in various ways.[6] In contrast, the government here made no effort to identify computers on site that did not contain information responsive to the warrant, and let five (5) months elapse after completing the search before making any effort to return Defendant's non-contraband property. *Id*.; *see also Maali,* 346 F. Supp. 2d at 1236 ("The seized computer hard drives were copied or 'mirrored' and the hard drives were returned to the Defendants approximately one week after the searches. Many of the documents and other items seized have also since been returned."). Finally, the *Maali* court's decision not to require a computer search strategy in the warrant was

[6] *See Khanani*, 502 F.3d at 1290 ("Khanani and Portlock also contend that the lack of a written 'search protocol' required the district court to suppress all evidence agents seized as a result of the search of the defendants' computers. The testimony at the suppression hearing established that the agents attempted to identify computers that contained information that was responsive to the warrants and that they did not seize every computer that they encountered. Thereafter, a computer examiner eliminated files that were unlikely to contain material within the warrants' scope. The culling process winnowed down the files seized from approximately three million to approximately 270,000. FBI Agent Scott Skinner testified that agents used 'keyword searches,' and 'if a document was opened and it wasn't . . . covered by the warrant, then it wasn't analyzed.'") (internal citations omitted).

exceedingly tentative. After acknowledging that "[s]ome courts have required a detailed description of the strategy to be employed in a computer search," the court went on to state: "The better practice would have been to . . . develop[] a search strategy and present[] that strategy to the magistrate judge, and the failure to do so is troubling." *Id*. at 1245-47. The government's failure to articulate a search strategy here is even more troubling because of the warrant's otherwise uncircumscribed nature and the unrestrained manner in which it was executed.

Probable cause to believe that a stolen lawnmower will be found in a garage will not support a search of an upstairs bedroom, nor will a warrant for a stolen refrigerator authorize the opening of desk drawers. *See Garrison*, 480 U.S. at 84; *United States v. Ross*, 456 U.S. 798, 824 (1982); *Walter v. United States*, 447 U.S. 649, 657 (1980). Likewise, probable cause to believe that Defendant possessed computer-accessible images of child pornography did not justify granting the government virtually unlimited access to all of Defendant's computer-accessible data.

II. <u>The warrant was executed in an unreasonable manner.</u>

Defendant objects to the Magistrate's conclusion that the warrant was executed in a reasonable manner. The execution of the search warrant following its service on August 2, 2012 was unreasonable[7] because government agents seized and continued to retain for more than five and a half (5½) months numerous items that fell outside the warrant's scope, including a computer and hard drive that agents knew, as of December 18, 2012, contained no evidence relating to child pornography.

Mitchell, 565 F.3d 1347 and *United States v. Laist*, 702 F.3d 608 (11th Cir. 2012) are squarely on-point. The key principle those cases represent here is that the government violates a

[7]The manner of the execution of a search warrant is subject to judicial review under a "reasonableness" standard. *Mitchell*, 565 F.3d at 1350.

defendant's Fourth Amendment rights when it seizes a defendant's computer equipment and then acts with unreasonable delay in returning non-incriminating property. This principal is not limited to warrantless seizures because "[t]he general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant." *United States v. Ramirez*, 523 U.S. 65, 71 (1998) (internal citation omitted). Further, "even 'a seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment's prohibition on 'unreasonable searches.' " *Mitchell*, 565 F.3d at 1350 (quoting *United States v. Jacobsen*, 466 U.S. 109, 124 (1984)).

While *Mitchell*'s facts are not identical to facts here, this disparity strengthens Defendant's claim that government agents unreasonably executed the warrant. In *Mitchell*, the court held that the defendant's motion to suppress should have been granted because there was "no compelling justification for the [government's twenty-one day] delay" in obtaining a search warrant for the defendant's seized hard drive. *Id.* at 1351. Thus, the *mere possibility* that the defendant's hard drive could be contraband-free, combined with the government's delay in taking steps to return non-incriminating property, i.e., obtain a warrant authorizing a search, was sufficient to warrant suppression of the seized evidence. *Id.* at 1352 ("the sooner the warrant issues, the sooner the property owner's possessory rights can be restored if the search reveals nothing incriminating") (internal citation and quotation marks omitted). But here, agents *knew* as of December 18, 2012 that a laptop and external hard drive seized from Defendant's residence contained no evidence relating to child pornography. (Doc. 72 at 10); *See also* Def. Ex. 2.

Moreover, Defendant's efforts to reacquire his lawfully owned property are irrelevant because "[i]t is the government's duty to comply with the Fourth Amendment." *Jacobsen*, 466

U.S. at 113. *See also Mitchell*, 565 F.3d at 1352 (general rule that the government should swiftly return non-incriminating evidence applies with "even greater force to the hard drive of a computer, which is the digital equivalent of its owner's home, capable of holding a universe of private information."); *United States v. Delancy*, 502 F.3d 1297, 1308 (11th Cir. 2007) (A consent to search may be insufficient where the consent itself springs from prior illegal activity by the police, such as an unlawful entry.).[8] While Defendant himself cannot possess or use any computer or access the internet, the government could have sought to return his contraband-free computer equipment to a designated individual outside Defendant's home, and given Defendant and Defendant's wife the opportunity to obtain copies of their many non-contraband computer files.

Well-established Fourth Amendment principles further support Defendant's claim that the government unreasonably executed the warrant. A " 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *Jacobsen*, 466 U.S. at 113. Even where one no longer holds a privacy interest in seized property, he may hold a possessory interest that continues to survive long after the seizure takes place. *See United States v. Paige*, 136 F.3d 1012, 1021-22 (5th Cir. 1998). Moreover, a seizure of property may begin as reasonable but then ripen into a seizure that violates the Fourth Amendment. *United States v. Place*, 462 U.S. 696, 710 (1983) (although warrantless detention of a traveler's luggage did not initially violate the Fourth Amendment, the retention of that luggage for over ninety (90) minutes rendered the seizure unreasonable and violated the Fourth Amendment).

[8] Fed. R. Crim. P. 41(g)-(h) also shows that the government alone is responsible for reasonably executing warrants. Fed. R. Crim. P. 41(g)-(h) states that both a motion to return property and motion to suppress are available remedies to a person aggrieved by an unlawful search and seizure, but does not state that the former must precede the latter.

Therefore, whenever the government meaningfully interferes with an individual's interest in property, a "seizure" subject to the reasonableness analysis of the Fourth Amendment takes place.

The Supreme Court's recent Fourth Amendment jurisprudence shows that property-based considerations lie at the heart of its protections. "The Amendment establishes a simple baseline, one that for much of our history formed the exclusive basis for its protections: When the Government obtains information by physically intruding" on persons, houses, papers, or effects, a 'search' within the original meaning of the Fourth Amendment has undoubtedly occurred." *Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013) (law enforcement officers' use of drug-sniffing dog on front porch of home to investigate an unverified tip that marijuana was being grown in the home was a trespassory invasion of the curtilage which constituted a "search" for Fourth Amendment purposes, and officers did not have an implied license for the physical invasion of the curtilage) (internal quotation marks and citation omitted). Thus, "[a]t bottom, [courts] must assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. … For most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates." *United States v. Jones*, 132 S. Ct. 945, 950 (2012) (government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a "search" because the government physically occupied private property for the purpose of obtaining information) (internal quotation marks and citations omitted).

Additionally, in the civil context, courts have recognized that constitutional violations can occur when the government acts with unreasonable delay in returning property that initially

was lawfully seized.[9] *Lathon v. City of St. Louis*, 242 F.3d 841 (8th Cir. 2001) (That ammunition and weapons were seized from resident's possession pursuant to valid search warrant did not preclude resident's Section 1983 claim that government's subsequent refusal to return ammunition and weapons constituted deprivation of property without due process; pivotal deprivation was not initial seizure of items, but the refusal to return them without court order after it was determined that items were not contraband or required as evidence in court proceeding); *see also Presley v. City Of Charlottesville*, 464 F.3d 480 (4th Cir. 2006) (In order for property owner to state a claim against city under § 1983 for unreasonable seizure of real property in violation of Fourth Amendment, based on city's publishing a map showing a public trail crossing owner's property and encouraging private individuals to trespass on the property, property owner did not have to allege that she was completely deprived of her possessory interests in her property; owner had only to allege that there was some meaningful interference with her possessory interests in the property). Similarly, for many years, courts have determined the reasonableness of the government's continued possession of private property in the adjudication of Rule 41(e) motions as civil equitable actions for the return of property. *See, e.g.*, *Soviero v. United States*, 967 F.2d 791, 792-93 (2d Cir. 1992); *Mora v. United States*, 955 F.2d

[9] The Fourth Amendment analysis that applies to section 1983 claims is, in general, identical to the analysis used in criminal cases. *See, e.g., Groh*, 540 U.S. 551 (ranch owners brought *Bivens* and § 1983 action against federal and county law enforcement officers, alleging that their Fourth Amendment rights were violated; court held that search warrant that utterly failed to describe the persons or things to be seized was invalid on its face, notwithstanding that requisite particularized description was provided in search warrant application; and residential search that was conducted pursuant to this facially invalid warrant could not be regarded as "reasonable," though items to be seized were described in search warrant application, and though officers conducting search exercised restraint in limiting scope of search to that indicated in application). *But see Elkins v. Dist. of Columbia*, 610 F. Supp. 2d 52, 61 (D.D.C. 2009) (fruit of the poisonous tree doctrine does not apply to § 1983 cases) *clarified on denial of reconsideration*, 636 F. Supp. 2d 29 (D.D.C. 2009) *aff'd*, 690 F.3d 554 (D.C. Cir. 2012) and *aff'd*, 690 F.3d 554 (D.C. Cir. 2012).

156, 158 (2d Cir. 1992); *United States v. Martinson*, 809 F.2d 1364, 1368 (9th Cir. 1987); *Sovereign News Co. v. United States*, 690 F.2d 569, 577 (6th Cir. 1982).[10]

Therefore, Defendant's claim that this Court should seriously evaluate the reasonableness of the government's prolonged retention of his property is hardly remarkable. What is remarkable is the government's utter disregard of Defendant and Defendant's wife's property rights to their computer equipment, which contained a "universe of information." *Mitchell*, 565 F.3d at 1352. It is undeniable that the government meaningfully interfered with Defendant and Defendant's wife's possessory interests in their seized property. Additionally, neither the Magistrate nor the government has offered any explanation, much less a reasonable one, for the government's months-long failure to even attempt to return computer equipment and files belonging to Defendant and his wife after the government determined that they were contraband-free and no longer needed them.

III. The *Leon* good faith exception does not apply.

For the reasons stated in Defendant's Motion to Suppress and Memorandum of Law in Support (Doc. 39), Defendant objects to the Magistrate's finding that the government acted in good faith. Because the government did not act in good faith, the suppression of all evidence seized pursuant to the warrant is necessary. *United States v. Martin*, 297 F.3d 1308, 1318 (11th Cir. 2002).

The need for this remedy is amplified by the fact the twelve (12) paragraphs in the government's affidavit describing items sought to be seized came from an unedited template and the corresponding twelve (12) paragraphs in the warrant were identical to the affidavit.

[10] The advisory committee's notes to Rule 41(e) urge courts to apply Fourth Amendment reasonableness standards to determine whether a person so aggrieved has a right to the return of his property. Fed. R. Crim. P. 41(e) advisory committee's note.

Therefore, the government likely will continue to execute overbroad, insufficiently particularized warrants unless this Court enters an Order granting Defendant's Motion to Suppress. This is especially troubling in the case of computer equipment because of the voluminous information computers typically contain and the difficulty of identifying and seizing electronic evidence that falls within the scope of probable cause on-site. *See, e.g., Cioffi*, 668 F. Supp. 2d at 391; Fed. R. Crim. P. 41(e)(2)(b) Commentary (2012) (rule acknowledges need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant). Consequently, when computer equipment is involved, there is a heightened need for judicial scrutiny of the particularity and breadth of search warrants and the manner of the execution of search warrants. *See United States v. Metter*, 860 F. Supp. 2d 205, 216 (E.D.N.Y. 2012) (granting motion to suppress electronic evidence seized pursuant to search warrants, and stating, "[T]he Court cannot, in the interest of justice and fairness, permit the government to ignore its obligations. Otherwise, the Fourth Amendment would lose all force and meaning in the digital era and citizens will have no recourse as to the unlawful seizure of information that falls outside the scope of a search warrant and its subsequent dissemination."). Here, suppression of all evidence seized is an appropriate remedy because it is in society's best interest to punish and deter government conduct that results in a constitutional violation of citizens' property and privacy rights. *United States v. Gilbert*, 942 F.2d 1537, 1542 (11th Cir. 1991).

Conclusion

For all the reasons stated above, the Magistrate Judge's Report and Recommendation (Doc. 85) should be rejected in whole, and Defendant's Motion to Suppress and Memorandum of Law in Support (Doc. 43) should be granted.

Respectfully submitted,

/s/ Bryan E. DeMaggio
Wm. J. Sheppard, Esquire
Florida Bar No.: 109154
Elizabeth L. White, Esquire
Florida Bar No.: 314560
Matthew R. Kachergus, Esquire
Florida Bar No.: 503282
Bryan E. DeMaggio, Esquire
Florida Bar No.: 055712
Jonathan W. Graessle, Esquire
Florida Bar No.: 10264
Sheppard, White & Kachergus, P.A.
215 Washington Street
Jacksonville, Florida 32202
Telephone: (904) 356-9661
Facsimile: (904) 356-9667
Email: sheplaw@att.net
COUNSEL FOR DEFENDANT

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on November 4, 2013, I electronically filed the foregoing with the Clerk of the Court by using CM/ECF System which will send a notice of electronic filing to the following:

Kelly Karase, Esquire
D. Rodney Brown, Esquire
Assistant United States Attorney
300 North Hogan Street
Suite 700
Jacksonville, Florida 32202

I HEREBY CERTIFY that on November 4, 2013, a true and correct copy of the foregoing document and the notice of electronic filing was sent by United States Mail to the following non-CM/ECF participants:

N/A

/s/ Bryan E. DeMaggio
ATTORNEY

mlh[brooks.richard.objections.rr.msw]