UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v. 5:15-CR-133 (BKS)

CHRISTOPHER FILIPPI,

Defendant.

Appearances:

For United States of America:
Nicolas Commandeur
Office of United States Attorney - Syracuse Office
100 South Clinton Street
P.O. Box 7198
Syracuse, NY 13261

For Christopher Filippi:
James F. Greenwald
Office of the Federal Public Defender - Syracuse Office
Districts of Northern New York & Vermont
The Clinton Exchange, 3rd Floor
4 Clinton Square
Syracuse, NY 13202

Hon. Brenda K. Sannes, United States District Court Judge:

MEMORANDUM-DECISION AND ORDER

I. INTRODUCTION

Defendant Christopher Filippi is charged with receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A), (b)(1), 2252A(b)(2), and 2256(8)(A). Defendant moves to suppress evidence obtained as a result of the government's search of his cellular phone, on the grounds that the search took place after the time period prescribed in an

Addendum attached to the search warrant by the issuing judge. (Dkt. No. 43). For the reasons that follow, the motion is denied.

II. FACTUAL BACKGROUND

A. The Search Warrant

On March 23, 2015, federal law enforcement officers obtained a search warrant for defendant's person, residence, and property, including "any computers, computer equipment or computer storage media and electronic storage media." (Dkt. No. 43-3, pp. 1-2).[1] Attachment B to the warrant described in detail the items to be seized and searched as evidence in violation of Title 18 U.S.C. §§ 2552 and 2252A (distributing, receiving, or possessing child pornography), including computers and electronic media. (*Id.*, pp. 3-4).[2]

The Magistrate Judge who authorized the warrant, the Honorable David E. Peebles, also attached an "Addendum to Search Warrant" (the "Addendum"), setting forth certain protocols for the search. Specifically, the Addendum provided that:

> 1. Completion of Computer Search. The computer or electronic media search authorized by this warrant shall be completed within sixty (60) days of the date of this warrant. This period may be extended by the court upon a showing of good cause.
>
> 2. Minimization. In executing the search of any computer or computer-related items authorized by this warrant, the law enforcement officers executing the search [hereinafter referred to as the "United States"] shall make reasonable efforts to utilize computer search methodology that avoids searching files, documents, or other electronically stored information which is not identified in the warrant.

[1] The affidavit supporting the warrant stated, in sum and substance, that probable cause was based on the fact that federal law enforcement officers had utilized a file-sharing software program to download images of child pornography from an Internet Protocol address associated with defendant's residence. (*See* Dkt. No. 1 in Case 5:15-MJ-112-DEP).

[2] Paragraph eight of Attachment B authorized search of "[a]ny electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data, obtained through computer or Internet-based communications, including data in the form of electronic records, documents and materials, including those used to facilitate interstate communications, included but not limited to telephone (including mobile telephone) and Internet Service Providers." (Dkt. No. 43-3, p. 4).

> 3. Return of Data. If a resident or occupant of the premises from which a computer is seized pursuant to this warrant makes a written request to the United States for a return of the seized data storage devices, the United States shall provide such person within sixty (60) days of the receipt of such request with a copy of any requested data and electronically stored information that does not constitute contraband or instrumentalities of a crime or which has not been searched in accordance with paragraph (1) above. If the United States withholds any data or electronically stored information requested by any resident of the premises searched, the United States shall identify such withheld information or data to such resident and state the reason such data or information is not being returned.
>
> 4. Return of Computer. The United States shall determine within sixty (60) days of the execution of the warrant whether any seized computer contains any of the Items for which the search was authorized or any contraband, instrumentalities of a crime, or property subject to forfeiture. If none is found, any such computer shall be returned forthwith to the premises from which it was seized. This period may be extended by the court upon a showing of good cause.
>
> 5. Retention of Rights. Nothing in this warrant or this addendum shall limit or prevent the United States from seizing any computer as contraband or as an instrumentality of a crime or from commencing forfeiture proceedings against a computer or the data contained therein. Moreover, nothing in this warrant or this addendum shall limit or prevent any person from filing a motion for the return of seized property pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure or seeking any other relief such person deems appropriate.

(Dkt. No. 43-3, p. 7).

B. Execution of the Search Warrant

The search warrant was executed at the defendant's residence on March 24, 2015. (Dkt. No. 46-5, ¶ 3). A certified digital forensic examiner, Special Agent Diego Collachi, conducted a "preview" examination of some of the electronic media on site. (*Id.*, ¶¶ 1, 3). SA Collachi found a number of images of suspected child pornography on the defendant's laptop during this initial review at the scene, and federal law enforcement officers seized the computer. (*Id.*, ¶ 5). SA Collachi determined that some of the electronic media did not contain any evidence of child pornography, and those items were left in the residence. (*Id.*, ¶ 4). Officers seized certain

electronic media that SA Collachi could not conclusively determine lacked evidence of child pornography, for review off site. (*Id.*, ¶ 4). According to SA Collachi, "[f]orensic review of computers is generally a time-consuming process, and certain electronic media require specific hardware and software to review them properly." (*Id.*). SA Collachi was not able to conduct a review on site of the defendant's Samsung Galaxy S5 phone; the phone was seized for later review off site. (*Id.*, ¶ 6). On April 8, 2015, SA Collachi performed a forensic extraction of data from the phone. (*Id.*). He did not find any images of child pornography, but the phone was maintained in connection with the investigation and preparation for trial. (*Id.*).

C. Subsequent Investigation

SA Collachi made a forensic image of defendant's computer hard drive on March 24, 2015, and provided the forensic image to Syracuse Police Detective Richard Smith, a computer forensics examiner, so that he could perform a more extensive forensic analysis. (*Id.*, ¶ 5). Detective Smith reviewed the forensic image and found two-password protected accounts on the computer: "Christopher" and "Kristin Filippi." (Dkt. No. 46-2, p. 5). The Christopher account showed a full name of Christopher Filippi associated with the email address c.filippi0713@gmail.com. (*Id.*). Detective Smith found over four thousand images of suspected child pornography which had been saved in a folder on the desktop of the Christopher user account, and were ultimately "moved from the Christopher user account to a hidden user created folder, titled System 4.2, within the Program Files directory in an effort to conceal the files from unintended parties." (*Id.*, p. 19). In addition, Detective Smith found that the download history for many of the images occurred in close temporal proximity to internet activity attributable to the use of the "c.filippi0713@gmail" email address. (*Id.*, pp. 6-8, 14-16, 18).[3]

[3] Although Detective Smith's report is dated June 25, 2015, according to defense counsel, Detective Smith's forensic analysis of defendant's laptop was completed on April 14, 2015. (Dkt. No. 43-1, ¶ 11).

Defendant was arrested on April 21, 2015, and has been in continuous custody since then. (Dkt. No. 43-1, ¶ 12). An indictment filed on April 30, 2015 charged defendant with three counts of receiving child pornography and one count of possessing child pornography. (Dkt. No. 8). On May 14, 2015, defense counsel sent an email message to government counsel, stating in relevant part: "I have not yet received the search warrant return, listing the items seized. I understand various computers, cell phones, etc. were taken. If they are clean, we would like them back ASAP. It is really disruptive for the family to not have their phones and computers. Please let me know what we need to do to arrange this." (Dkt. No. 43-1, ¶ 15).[4]

On May 26, 2015, law enforcement officers obtained a search warrant for information associated with defendant's Gmail email account that was maintained by Google, Inc. (Dkt. No. 46-1, ¶ 7). On June 17, 2015, government counsel and Detective Smith met regarding the case with Anthony Martino, another computer forensics expert. (Dkt. No. 46-3, p. 4). Detective Smith delivered several items of electronic media, including the defendant's laptop computer and the Samsung Galaxy S5 phone to Mr. Martino for his review to determine if they contained evidence of child pornography. (*Id.*, pp. 2-3).

D. Discovery of Evidence on Defendant's Cellular Phone

On June 22, 2015, Google produced records in response to the May 26, 2015 warrant, which appeared to show that defendant had been "backing up on his GMail account certain text messages from his cellular phone number and that some of these texts appeared to include links to a website." (Dkt. No. 46-1, ¶ 7). In light of this information, government counsel asked Mr. Martino to analyze defendant's phone. (*Id.*). Mr. Martino's report shows that he examined

[4] The search warrant return, dated March 24, 2015, and listing defendant's phone among the items seized, was filed on April 13, 2015 and ordered unsealed on May 4, 2015. (*See* Dkt. Nos. 5, 6 in Case 5:15-MJ-112-DEP). Defense counsel states that, on or around June 12, 2015, he received an Evidence Recovery Log listing the items seized from the defendant's home, but that to date none of the items listed have been returned. (Dkt. No. 43-1, ¶ 17).

defendant's phone on June 23, 2015. (Dkt. No. 46-3, pp. 5-6). On June 24, 2015, Mr. Martino informed government counsel of his preliminary findings, that he had identified: "(1) internet search activity on a Russian website and (2) download history of file names that matched the file names of images of child pornography found on the defendant's laptop." (Dkt. No. 46-1, ¶ 8). That same day, government counsel notified defense counsel of Mr. Martino's preliminary findings. (*Id.*). On June 29, 2015, Mr. Martino prepared a report, which concluded, among other things, that "the computer seized from Christopher Filippi was used to search for, download and save images of child pornography," and that "the cellular telephone seized from Christopher Filippi also contained artifacts of child pornography images that were obtained from web browsing activities that mirror those found on the computer." (Dkt. No. 46-3, p. 8).

III. DISCUSSION

Defendant argues that the evidence from his cellular phone must be suppressed because "the government did not begin its search" of the phone until June 18, 2015, approximately eighty-five days after the search warrant was issued on March 23, 2015, and that the Addendum to the warrant required the government to complete its search within sixty days and return seized property if no items for which the search was authorized were found within sixty days. (Dkt. No. 43-2, pp. 3-4). Thus, defendant argues, the search violated the sixty-day limit in the Addendum to the warrant, and was unreasonable under the Fourth Amendment. (*Id.*). The government counters that the evidence should not be suppressed for several reasons: 1) an initial forensic extraction of data was performed on the phone within the sixty-day limit, and Mr. Martino's forensic review was not a new "search" requiring a new or extended warrant; 2) the search was reasonable under the Fourth Amendment; and 3) the remedy of suppression is not warranted. (Dkt. No. 46-1).

As a preliminary matter, it is undisputed that law enforcement officers seized the phone pursuant to a valid search warrant supported by probable cause. The warrant, including the attachments and Addendum, expressly authorized the search of computers and electronic media, including defendant's phone. Although defendant argues that the search did not "begin" until after the sixty-day period had lapsed, SA Collachi has submitted an affidavit stating that he did a forensic extraction of data from the phone on April 8, 2015, well within the sixty-day time period. (Dkt. No. 46-5, ¶ 6). SA Collachi did not find child pornography at that time; he states that "the phone was maintained in connection with the investigation and preparation for trial." (*Id.*). There is also no challenge to the scope of Mr. Martino's subsequent forensic review of the phone; his report indicates that he searched for and obtained evidence of the child pornography offenses. (Dkt. No. 46-3).

The Court finds, for the reasons set forth below, that the government's failure to comply with the Addendum in this case is akin to a technical violation of Rule 41,which does not warrant suppression; that the search of the phone was reasonable and did not violate the Fourth Amendment; and that in any event that suppression is not warranted.

A. The Provisions in Federal Rule of Criminal Procedure 41(e)(2)(B) and the Addendum Regarding the Timing of the Search and Further Review of Defendant's Cellular Phone.

The government argues that Mr. Martino's forensic review of defendant's phone was not a new "search." (Dkt. No. 46, p. 7). However, at the very least it was a further review of electronically stored information which had been seized pursuant to the warrant. Under the Federal Rule of Criminal Procedure governing warrants for electronically stored information, the fourteen-day time period for *executing* the warrant "refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." Fed. R. Crim. P.

41(e)(2)(B). While the Rule does not impose any time limit on "a later review of the media," the Rule anticipates that the issuing judge might impose such a limit. The Rule states:

> A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Fed. R. Crim. P. 41(e)(2)(B). The Advisory Committee Note to Rule 41 further explains that:

> While consideration was given to a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place, the practical reality is that there is no basis for a "one size fits all" presumptive period. A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs. The rule does not prevent a judge from imposing a deadline for the return of the storage media or access to the electronically stored information at the time the warrant is issued. However, to arbitrarily set a presumptive time period for the return could result in frequent petitions to the court for additional time.
>
> It was not the intent of the amendment to leave the property owner without an expectation of the timing for return of the property, excluding contraband or instrumentalities of crime, or a remedy. Current Rule 41(g) already provides a process for the "person aggrieved" to seek an order from the court for a return of the property, including storage media or electronically stored information, under reasonable circumstances.
>
> Where the "person aggrieved" requires access to the storage media or the electronically stored information earlier than anticipated by law enforcement or ordered by the court, the court on a case by case basis can fashion an appropriate remedy, taking into account the time needed to image and search the data and any prejudice to the aggrieved party.

Id., Advisory Committee Note, 2009 Amendments.

In this case, the first paragraph of the Addendum issued by Magistrate Judge Peebles, entitled "Completion of the Computer Search," states that, "The computer or electronic media search authorized by this warrant shall be completed within sixty (60) days of the date of this

warrant." (Dkt. No. 43-3, p.7). The fourth paragraph of the Addendum requires that the government determine within sixty days of executing the warrant, "whether any seized computer contains any of the items for which the search was authorized or any contraband, instrumentalities of a crime, or property subject to forfeiture," and if none is found that the computer be "returned forthwith." (*Id.*). For the purposes of this decision, the Court will assume that the Addendum is enforceable as an *ex ante* restriction on the search warrant. *See In the Matter of a Warrant for All Content and Other Information Associate with the Email Account xxxxxxx@Gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F. Supp. 3d 386, 398 (S.D.N.Y. 2014).[5]

Applying Rule 41 and the requirements of the Addendum to the facts of this case, the warrant issued on March 23, 2015 was executed the next day when the phone was seized from the defendant. Fed. R. Crim. P. 41(e)(2)(B). SA Collachi performed a forensic extraction of the phone on April 8, 2015. (Dkt No. 46-5, ¶ 6). SA Collachi's affidavit states that his "review of the phone did not reveal any images of child pornography, but the phone was maintained in connection with the investigation and preparation for trial." (*Id.*). On June 23, 2015, almost three months after the warrant was issued, Mr. Martino reviewed the phone.

The government argues that the Addendum did not prevent it from doing a "second review of validly obtained evidence." (Dkt. No. 46, p. 7). However, under the first paragraph of the Addendum, the government was required to "complete" its "computer or electronic media search" within sixty days of the date of the warrant. (Dkt. No. 43-3, p. 7). The fourth paragraph of the Addendum also required the government to determine within sixty days whether "any

[5] The Court rejects the government's argument that the enforceability of the Addendum is "questionable because it is not specifically referenced in the warrant." (Dkt. No. 46, p. 9, n.3). The Addendum is part of the warrant: it is page seven of the warrant that was issued by Magistrate Judge Peebles. (Dkt. No. 43-3, p. 7; *see* Dkt. No. 5 in Case 5:15-MJ-112-DEP). In the case on which the government relies, the Supreme Court held that an underlying affidavit which did not accompany the warrant and was not incorporated by reference in the warrant could not be relied upon to save a deficient warrant. *See Groh v. Ramirez*, 540 U.S. 551, 558 (2004).

seized computer" contained "items for which the search was authorized or any contraband, instrumentalities of a crime, or property subject to forfeiture," and if none were found, to return the computer "forthwith." (*Id*).[6] While the latter paragraph does not specifically reference electronic media or data storage devices, its logical purpose is to ensure the return of seized property that is "clean," and the government assumes that this paragraph applies to the phone. (*See* Dkt. No. 46, p. 11).

The government argues that the search "was appropriate" under the Addendum because it did a forensic extraction of the data on the phone well within the sixty-day deadline; it determined within the sixty-day deadline that the defendant used his laptop computer to collect child pornography, and that there was, therefore "good reason to believe" that defendant's phone was an instrumentality of a crime and not subject to return under paragraph four of the Addendum; and that Mr. Martino's review took place within sixty days of defense counsel's request for the return of the phone, and "resulted in unequivocal confirmation that the phone was an instrumentality of a crime." (Dkt. No. 46, p. 11).

However, considering the Addendum as a whole and in the context of Rule 41, it appears that "completion" of the computer or electronic media search at the very least required the government to search the phone within sixty days to determine whether it contained any items for which the search was authorized or any contraband, instrumentalities of a crime, or property subject to forfeiture. SA Collachi's forensic extraction, while timely, did not find child pornography and there was no determination, within sixty days, that the phone contained items

[6] Defense counsel's request for the return of "clean" computers and phones on May 14, 2015, Dkt. No. 43-1, ¶ 15, did not affect the sixty day period for "completion" of the government's search. The third paragraph of the Addendum relates only to the return of "data" following a request for "seized data storage devices," requiring that the government provide, within sixty days of the receipt of such request, "requested data and electronically stored information that does not constitute contraband or instrumentalities of a crime or which has not been searched in accordance with paragraph (1)" of the Addendum. (Dkt. No. 43-3, p. 7).

for which the search was authorized or constituted an instrumentality of a crime or property subject to forfeiture. Therefore, on the facts of this case, the Court concludes that Mr. Martino's June 23, 2015 review of defendant's phone did not comply with the Addendum's requirement that the search "authorized by th[e] warrant" be "completed" within sixty days.

B. The Government's Failure To Comply with the Addendum Does Not Warrant Exclusion of the Evidence.

In analogous cases where a search failed to comply with the requirements of Rule 41 of the Federal Rules of Criminal Procedure, including the time limit for executing the warrant, the Second Circuit has held that such violations "should not lead to exclusion unless (1) there was 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule." *United States v. Pangburn*, 983 F.2d 449, 455 (2d Cir. 1993) (citing *United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir. 1975)); *see also United States v. Johnson*, 660 F.2d 749, 753 (9th Cir. 1981) ("Only a 'fundamental' violation of Rule 41 requires automatic suppression, and a violation is 'fundamental' only where it, in effect, renders the search unconstitutional under traditional fourth amendment standards.").

"Technical" violations of Rule 41 are not considered 'deliberate and intentional disregard' of the Rule that would justify suppression." *United States v. Deas*, No. 3:07-CR-73, 2008 WL 5063901, at *2, 2008 U.S. Dist. LEXIS 96088, at *8 (D. Conn. Nov. 24, 2008) (quoting *United States v. Williamson*, 439 F.3d 1125, 1134 n.7 (9th Cir. 2006)); *see also United States v. Rodriguez*, No. 3:11-CR-12, 2011 WL 2470714, at *8, 2011 U.S. Dist. LEXIS 65000, at *25-26 (D. Conn. June 20, 2011) (denying motion to suppress where, even assuming a "technical" violation of Rule 41 occurred, there was no evidence of prejudice to defendant or that law enforcement deliberately disregarded the rule); *United States v. Dewar*, 489 F. Supp. 2d 351,

365 (S.D.N.Y. 2007) (declining to suppress evidence where the warrant was supported by probable cause and defendants "suffered no prejudice from the technical violation of Rule 41."). Thus, in Rule 41 cases, "[c]ourts have declined to order suppression of evidence seized pursuant to belatedly-executed warrants where probable cause still existed at the time of the execution and the police did not deliberately disregard the terms of the warrant." *United States v. Ahmad*, No. 11-CR-6130L, 2012 WL 1944615, at *8, 2012 U.S. Dist. LEXIS 74325, at *24 (W.D.N.Y. May 29, 2012) (citing cases), *report and recommendation adopted*, No. 11-CR-6130L, 2012 WL 3028302, 2012 U.S. Dist. LEXIS 103003 (W.D.N.Y. July 24, 2012).

Here, there is no evidence that the government acted in bad faith or with deliberate disregard of the search warrant deadline. Rather, the government argues that any error was "inadvertent[7] and due to the failure to comply with Addendum's administrative requirements of seeking an extension of the 60-day period." (Dkt. No. 46, p. 16).

The defendant argues that his right to a speedy trial was prejudiced by the government's delay.[8] (Dkt. No. 43-2, p. 4). But defendant does not allege any prejudice "in the sense that the search might not have occurred or would not have been so abrasive" if the Addendum had been followed. *Pangburn*, 983 F.2d at 455. Given the child pornography found on defendant's laptop within sixty days, the government had good cause to extend the time to complete the search of another electronic storage device taken from the defendant, as allowed by the Addendum. A defendant does not establish prejudice if the search would have taken place in exactly the same way had the Addendum been followed. *Id.*

[7] The government has not provided any evidentiary support for that assertion.

[8] This case was scheduled to go to trial on July 6, 2015, within the seventy-day time period established in the Speedy Trial Act, 18 U.S.C. § 3161(c)(1). (Dkt. No. 13). On June 30, 2015, the day after the government produced Mr. Martino's report, defense counsel requested that the trial be continued to August 12, 2015. (Dkt. No. 46-4, pp. 3-6). Defendant filed this motion on July 30, 2015. (Dkt. No. 43).

Moreover, the government's one-month delay after the sixty-day limit did not diminish the probable cause for the search of defendant's phone. Rather, the probable cause to search the phone had grown stronger since the warrant was signed. At the time of the June 23, 2015 search by Mr. Martino, the government had found of images of suspected child pornography on defendant's computer, and evidence obtained from Google on June 22, 2015 indicated that defendant had also used his phone to send text messages which appeared to contain links to a website. Thus, there was ample probable cause to believe that defendant's phone contained evidence related to the receipt and possession of child pornography: the warrant was not "stale." *See United States v. Brewer*, 588 F.3d 1165, 1173 (8th Cir. 2009) (finding that forensic analyses conducted several months after state warrants expired did not violate the Fourth Amendment—the warrants were not stale since probable cause to believe electronic media contained child pornography "continued to exist" at the time of execution); *United States v. Bedford*, 519 F.2d 650, 655 (3d Cir. 1975) ("Timeliness of execution should not be determined by means of a mechanical test with regard to the number of days from issuance, nor whether any cause for delay was per se reasonable or unreasonable. Rather it should be functionally measured in terms of whether probable cause still existed at the time the warrant was executed.").

Given the lack of evidence of prejudice to defendant or deliberate disregard of the Addendum, and the probable cause at the time of the search, the Court concludes that the government's failure to comply with the Addendum does not warrant exclusion of the evidence.

C. The Search Did Not Violate the Fourth Amendment.

The "ultimate touchstone" of the Fourth Amendment with respect to searches and seizures is reasonableness. *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006). In general, "a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *United States v. Galpin*, 720 F.3d 436, 445 (2d

Cir. 2013) (quoting *Kentucky v. King*, 131 S.Ct. 1849, 1856 (2011)). "Unreasonable delay in the execution of a warrant that results in the lapse of probable cause will invalidate a warrant." *United States v. Marin-Buitrago*, 734 F.2d 889, 894 (2d Cir. 1984). But the Fourth Amendment does not set any specific time limit on the execution of search warrants. *See United States v. Metter*, 860 F. Supp. 2d 205, 215 (E.D.N.Y. 2012); *United States v. Gerber*, 994 F.2d 1556, 1559 (11th Cir. 1993) ("The Fourth Amendment does not specify that search warrants contain expiration dates.").

In this case, the government's search of defendant's phone approximately three months after it was seized was not unreasonable given the amount of information recovered, which also included defendant's computer and more than a dozen hard disks and flash drive storage devices, and the nature of the forensic review process. According to SA Collachi, "[f]orensic review of computers is generally a time-consuming process, and certain electronic media require specific hardware and software to review them properly." (Dkt. No. 46-5, ¶ 4). The Second Circuit has also recognized this fact, observing that "forensic analysis of electronic data may take months to complete." *United States v. Ganias*, 755 F.3d 125, 135 (2d Cir. 2014) *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015). For this reason, "there is no established upper limit as to when the government must review seized electronic data to determine whether the evidence seized falls within the scope of a warrant," and the issue "requires a careful case-by-case factual analysis because what may be appropriate under one set of facts and circumstances may not be so under another." *Metter*, 860 F. Supp. 2d at 215.

While the government cannot indefinitely retain evidence for use in future criminal investigations, *Ganias*, 755 F.3d at 145,[9] "[n]umerous cases hold that a delay of several months

[9] This case is distinguishable in several important respects from the Second Circuit's recent decision in *United States v. Ganias*. There, the government seized an accountant's computer files pursuant to a search warrant for a criminal

between the seizure of electronic evidence and the *completion* of the government's review of that evidence as to whether it falls within the scope of the warrant is reasonable." *Metter*, 860 F. Supp. 2d at 215 (citing cases); *see also United States v. Lustyik*, 57 F. Supp. 3d 213, 232 (S.D.N.Y. 2014) (finding that three months was not an "unreasonably long time" for the government to review emails); *United States v. Triumph Capital Grp., Inc.*, 211 F.R.D. 31, 66 (D. Conn. 2002) ("computer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search, more preparation and a greater degree of care in their execution.").

The search was also reasonable considering the chain of events that preceded it. In his affidavit, SA Collachi states that during an on-site inspection of the defendant's laptop during the search on March 24, 2015, he identified a number of images of suspected child pornography, and that he provided a forensic image copy of the computer to Detective Smith for further analysis. (Dkt. No. 46-5, ¶ 5). When SA Collachi was able to review defendant's phone at the FBI's offices on April 8, 2015, he did not find any images of child pornography. (*Id.*). As a result, forensic review efforts initially focused on defendant's computer. During that review, Detective Smith discovered evidence linking the computer to defendant's Gmail account, and the government then obtained a search warrant for Google records on May 26, 2015. (Dkt. No. 46-1, ¶ 7). On June 22, 2015, Google produced records which indicated that the phone was being used to save links to a website. (*Id.*). The very next day, on June 23, 2015, Mr. Martino

---

investigation regarding two of his clients; the government retained a forensic image of the files for over two and half years, which included Ganias's personal financial records, which were beyond the scope of the search warrant. 755 F.3d at 138-139. Eventually, the government discovered evidence of tax evasion in Ganias's personal financial records, and the Second Circuit held that the search was unreasonable because the government "violated Ganias's Fourth Amendment rights by retaining the files for a prolonged period of time and then using them in a future criminal investigation." *Id.*, at 138. In contrast, here the government's search occurred only three months after the warrant was issued, the defendant's phone was clearly within the scope of the warrant, and the search was part of the same ongoing child pornography criminal investigation.

searched defendant's phone and found the evidence at issue. Thus, the timing of the search was reasonable under the circumstances.[10]

In addition, the Supreme Court has held that a search in violation of a Magistrate Judge's directives regarding the execution of a warrant does not violate the Fourth Amendment, so long as the search was reasonable under the circumstances. *Richards v. Wisconsin*, 520 U.S. 385, 117 (1997). In *Richards*, officers executed a search warrant by making an unannounced entry at the defendant's home, even though the Magistrate Judge who authorized the warrant had crossed out the portion permitting no-knock entry; the Supreme Court found the search reasonable under the circumstances because the officers concluded that the defendant was about to dispose of drugs. *Id.*, 395-396.

Similarly, courts have found that a search after a deadline set by a Magistrate Judge on a warrant may be reasonable under the circumstances. *See, e.g., United States v. Rigmaiden*, No. CR 08-814, 2013 WL 1932800, at *29, 2013 U.S. Dist. LEXIS 65633, at *80 (D. Ariz. May 8, 2013) (finding search reasonable despite violation of thirty-day time limit set by Magistrate Judge for completion of review of computer and storage devices), *appeal dismissed* (Nov. 19, 2013), *reconsideration denied*, No. CR 08-814, 2013 WL 4525252, 2013 U.S. Dist. LEXIS 121886 (D. Ariz. Aug. 27, 2013); *United States v. Hernandez*, 183 F. Supp. 2d 468, 480-481 (D.P.R. 2002) (finding that although forensic examination took place after the search warrant deadline ordered by Magistrate Judge, it was "perfectly reasonable for the Government to take a longer time to search and inspect the images in the floppy disks, particularly after already having discovered child pornography in Defendant's hard disk.").

[10] *Cf. United States v. Brunette*, 76 F. Supp. 2d 30, 42 (D. Me. 1999) (suppressing evidence where the government did not even begin its review of defendant's computers within sixty day search warrant limit set by Magistrate Judge and "offered no legitimate reason for its delay") *aff'd*, 256 F.3d 14 (1st Cir. 2001).

Thus, although the government did not comply with the Addendum's sixty-day deadline, the one month delay in searching defendant's phone was reasonable given the amount of information seized, the complex nature of the forensic review process, and the unfolding investigation.

D. Suppression Is Not Warranted.

Moreover, even if the search was unreasonable under the Fourth Amendment, suppression of the evidence recovered from defendant's phone is not warranted in this case. "The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.*, at 144. Thus, the rule "serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Id.* However, "when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way." *Davis v. United States*, 131 S. Ct. 2419, 2427-28 (2011) (internal citations and quotations omitted). "[T]he rule's costly toll upon truth-seeking and law enforcement objectives presents a high obstacle for those urging [its] application." *Herring*, 555 U.S. at 141 (citing *Penn. Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 364-65 (1998)).

Here, the government did not exceed the substantive scope of the search warrant, which expressly authorized the search of defendant's phone. Although the government violated the Addendum, the government notes that the law regarding the enforceability of search protocols is not settled, and cites caselaw support for its assertion that Mr. Martino could lawfully conduct a

second review of the lawfully-seized phone. (*Id.*, pp. 7-8).[11] Under the circumstances of this case, the Court finds that that reasonable minds could differ on the application of the Addendum. The Court further notes that there is no challenge to any other aspect of the government's compliance with the warrant; that the government reviewed the phone in response to the unfolding investigation regarding the defendant's laptop containing child pornography; and that the search involved reviewing data that had already been lawfully extracted from the phone. After carefully considering all of the facts and circumstances in this case, the Court concludes that if the delay in searching defendant's phone violated the Fourth Amendment, the government's conduct was neither "sufficiently deliberate" nor "sufficiently culpable" to justify suppression of the evidence from the phone. *Herring*, 555 U.S. at 144.

IV. CONCLUSION

For these reasons, it is

ORDERED that Defendant's motion to suppress (Dkt. No. 43) is **DENIED**, and it is further

ORDERED that the Clerk of the Court provide a copy of this Memorandum-Decision and Order to the parties.

IT IS SO ORDERED.

September 9, 2015
Syracuse, New York

Brenda K. Sannes
U.S. District Judge

[11] *See Ganias*, 755 F.3d at 142 (Hall, J., concurring in part and dissenting in part) (observing that the deterrence rationale of suppression is not served where "the Government's actions did not violate established precedent at the time of the search.").