

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,

v.

ERLAND OLSON, *et al.*,

Defendants.

Case No. 1:25-cr-69-RCL

MEMORANDUM OPINION & ORDER

This matter comes before the Court on Defendant Buscher’s motion to preserve digital evidence, ECF No. 118, which was joined or supplemented by Defendants Gallagher and Olson, ECF Nos. 128, 135. Buscher’s motion challenges the government’s decision to transfer and delete 23 terabytes of digital evidence (the Subject Data) that it copied off physical devices following the execution of two search warrants in June 2021. Defendants ask the Court to compel the government to preserve and search this evidence, arguing that the government has an obligation under *Brady v. Maryland*, 373 U.S. 83 (1963), to do so; alternatively, Defendants ask that the Court either appoint a special master to conduct such review or simply order the government “to make the data available to the defense.” ECF No. 148 at 7–8.

The Court, however, cannot grant the relief sought because the government has violated the Fourth Amendment by unreasonably delaying in segregating the portions of the Subject Data for which it has probable cause from those it does not. The result of this delay is that “the government’s ongoing seizure of” the electronically stored information “that is not responsive to the [June] 2021 warrant is unreasonable under the Fourth Amendment.” *United States v. Maresca*, No. 1:23-cr-123, 2026 WL 948289, at *27 (D.D.C. Apr. 6, 2026). The Court therefore cannot provide the relief sought unless the government secures a new warrant authorizing its continued

seizure of the Subject Data, which it has not indicated it is likely to do. The motion is therefore denied.

I. BACKGROUND

The Court presumes familiarity with the facts alleged in the Indictment. ECF No. 1. As relevant here, on June 30, 2021, the government executed search warrants at Defendant Olson's residence in Albuquerque, New Mexico, and at Theia's headquarters in Washington D.C. ECF No. 110 at 2. The warrants authorized the government to seize any digital devices reasonably capable of containing specific types of evidence. Theia HQ Search Warrant, Attachment B, ECF No. 173-3 (sealed); Olson's Residence Search Warrant, Attachment B, ECF No. 173-2 (sealed). The search warrant affidavits described the probable cause supporting the government's belief that this evidence was subject to seizure and would be found at the respective premises. Theia HQ Search Warrant Affidavit at 9–25, ECF No. 173-3 (sealed); Olson's Residence Search Warrant Affidavit at 10–26, ECF No. 173-2 (sealed).

Pursuant to the warrants, the government forensically imaged 16 digital devices from Olson's residence and 26 digital devices from Theia's headquarters, culminating in about 23 terabytes of forensic images. Many of the physical devices were immediately returned and all or most of the remaining physical devices have since been returned. ECF No. 110 at 2 & n.3.

Following the seizure of this evidence, however, the government largely failed to review this evidence to determine which materials fell within the scope of the warrant—that is, it did not segregate the data for which probable cause to seize existed from the data for which it did not. *Id.* at 3. Several months after the searches of Olson's residence and Theia's headquarters, Theia was placed into receivership, and the government began issuing grand jury subpoenas for records to Theia's receiver. *Id.* The receiver provided the government with tens of thousands of responsive documents, which the government represents largely “obviated the need for evidence that may

exist on the forensic images seized pursuant to the search warrants.” *Id.*¹ In the end, the government reviewed only a few of the 42 forensic images—the rest remain unprocessed. *Id.* at 3.² This remainder constitutes the Subject Data at issue here.

On March 13, 2025, Defendants were charged by indictment in the District of Columbia on multiple offenses, including conspiracy to commit wire and mail fraud, in violation of 18 U.S.C. § 1349. ECF No. 1. In the year following the indictment, the government represented to varying degrees that it planned to produce at least some amount of the Subject Data to the defense. For example, on January 8, 2026, at a status conference, the government represented that it planned to make a large “filter side” production that would “include the images of approximately 16 devices imaged on site during the execution of the search warrant on Theia headquarters.” ECF No. 92 at 4:22–5:04.

But rather than search, filter, and produce this evidence to the defendants, the government now seeks to transfer the Subject Data to either Olson or Theia’s former creditor, Brevet (depending on the original ownership of the physical devices that were imaged), and then remove the data from the government’s systems. The government indicated that it would take this course of action on April 15, 2026, when it filed a “Notice of Return of Property.” ECF No. 110.

After attempting to sort out this matter without court involvement, Defendant Buscher filed a motion asking the Court to enter an immediate temporary order preserving the Subject Data and halting any further transfer or deletion of it pending full briefing and resolution of the issues raised

¹ Defendants represent that a significant number of documents produced by the receiver were corrupted and inaccessible to Defendants. ECF No. 118 at 3. This fact has, in part, precipitated this litigation over whether the government has a duty to retain and search the Subject Data currently in its possession.

² The government initially represented that the filter team searched only two of these devices, both belonging to Olson, in accordance with the privilege protocol and produced the data to the defendants but not the government trial team. ECF No. 110 at 3 & n.4. However, the government’s recent status report seems to suggest that there may have been four devices (two belonging to Olson and two belonging to Gallagher) that were processed and uploaded to the filter database and produced in filter-side discovery to Defendants. ECF No. 172 at 2 n.3.

by the government’s proposed course of action. ECF No. 118 at 2. To maintain the status quo while the issue was under consideration, the Court granted the temporary relief sought. ECF No. 119. Shortly thereafter, the Court set a briefing schedule and motion hearing. ECF No. 134. Defendants Gallagher and Olson eventually joined or supplemented Defendant Buscher’s motion seeking the preservation and disclosure of the Subject Data. ECF Nos. 128, 135. The motion hearing was held on July 7, 2026.³

II. DISCUSSION

Defendants primarily seek an order from the Court compelling the government to preserve and search the Subject Data to fulfill its constitutional duty to disclose exculpatory evidence to the defense, as required by *Brady v. Maryland*, 373 U.S. 83 (1963). *See* ECF No. 118 at 7–9; ECF No. 128 at 10–12. In favor of their position, they cite a line of cases holding that the prosecution’s *Brady* obligation to disclose exculpatory information includes a duty to search for evidence in the government’s possession. *See, e.g., United States v. Brooks*, 966 F.2d 1500, 1502–04 (D.C. Cir. 1992). Alternatively, Defendants ask that the Court either appoint a special master to conduct such review or simply order the government “to make the data available to the defense.” ECF No. 148 at 7–8.

The Court, however, will not reach the *Brady* question or Defendants’ alternative remedies because, under the Fourth Amendment, the government’s continued retention of the unscoped Subject Data is an unlawful seizure. Under these circumstances, the government has one of two options: it can “‘cease the seizure or secure a new justification’—*i.e.*, a new warrant authorizing

³ At the motion hearing, and in one of his filings, Defendant Gallagher’s counsel questioned the accuracy of the government’s representation that the filter team never scoped the Subject Data. ECF No. 157 at 6–7. Upon the Court’s request, the government filed a status report on July 21, 2026, confirming that the government did “not find any evidence that the [Subject Data] had been scoped,” ECF No. 172, and appended a memo prepared by Special Agents from the Internal Revenue Service’s criminal investigation team to support this finding.

the seizure of the non-responsive” portions of the Subject Data. *Maresca*, 2026 WL 948289, at *1 (quoting *Brewster v. Beck*, 859 F.3d 1194, 1197 (9th Cir. 2017)). It has chosen the former, and the Court cannot compel the latter.

As explained further below, the Court recognizes that this result raises fairness concerns. The government represented to Defendants that it would produce some portion of this evidence to them. In seeking to transfer and delete the Subject Data, the government now cites caselaw in which the exclusionary rule has been used to deter the exact Fourth Amendment violation at issue here—the unreasonably long delay in scoping vast troves of electronic data that undoubtedly contains unresponsive materials for which the government lacks probable cause. Thus, in a sense, the application of these precedents to this case rewards the very conduct they seek to deter. Nevertheless, the Court cannot order the government to continue retaining evidence when doing so has since become unlawful. Defendants’ motion will therefore be denied.

A. Overview of the Fourth Amendment Standard

“The execution of a warrant for electronic media poses unique challenges for law enforcement and implicates significant Fourth Amendment interests.” *Id.* at *27. “The problem is that the volume and nature of information stored on computers and other electronic devices makes it ‘often impractical . . . to review all of the information during execution of the warrant at the search location.’” *Id.* (quoting Fed. R. Crim. P. 41(e) advisory committee’s note to 2009 amendment). To address this problem, Rule 41(e) of the Federal Rules of Criminal Procedure sets out a two-step procedure for the seizure of electronically stored information. Under Rule 41(e)(2)(B), law enforcement may first “seize or copy [on-site] the entire storage medium” and then “review it later [off-site] to determine what electronically stored information falls within the

scope of the warrant.” *Id.* at *28 (quoting Fed. R. Crim. P. 41(e) advisory committee’s note to 2009 amendment).

This second step is known as “scoping” the data—that is, segregating that which falls within the scope of the warrant (responsive materials) from that which does not (non-responsive materials). *Id.* at *1. This two-step process is necessary because seizing all the information on a digital device will almost always sweep in evidence for which the government lacks probable cause. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (per curiam) (recognizing that Rule 41 anticipates the “over-seiz[ure]” of data outside the scope of the warrant as “an inherent part of the electronic search process”); *United States v. Ganas*, 824 F.3d 199, 218 (2d Cir. 2016) (en banc) (observing that “[w]hile physical searches for paper records or other evidence may require agents to rummage at least cursorily through much private material,” forensically imaging digital devices, by contrast, predictably results in the “seizure and subsequent retention by the government of . . . vast quantities of irrelevant” private information).

As was the case here, search warrants authorizing the seizure of electronically stored information often include “filter protocols,” which provide safeguards against the trial team inadvertently accessing any privileged materials or materials that fall outside the scope of the warrant by establishing a “filter team” to scope the data and evaluate the materials for any existing privilege. *Maresca*, 2026 WL 948289, at *8.

While Rule 41(e)’s two-step process may be “necessary in the digital age,” the Fourth Amendment law dealing with the seizure and search of electronically stored information is an evolving landscape, particularly in light of the strong interests that individuals have “in shielding” non-responsive information “from the government.” *Id.* at *28 (citing *Riley v. California*, 573

U.S. 373, 393–97 (2014)). Because the government only has authority to possess nonresponsive materials for the temporary purposes of segregating them from responsive materials, one such concern arises when the government does not act expeditiously in scoping the data. Put simply, excessive delay in scoping the data gives rise to an unlawful seizure of materials over which the government lacks probable cause. *Id.* at *29 (“[W]hen the government unreasonably delays its review of electronic media seized pursuant to a warrant, the Fourth Amendment violation is the seizure of non-responsive data for longer than reasonably necessary to serve the government’s legitimate law enforcement interests.”).

Courts have applied the Fourth Amendment’s “reasonableness standard to suppress evidence when the government delayed unreasonably in sifting through [electronic data] warrant returns for relevant evidence.” *United States v. Zelaya-Veliz*, 94 F.4th 321, 338 (4th Cir. 2024); *see also Asinor v. District of Columbia*, 111 F.4th 1249, 1258–59 (D.C. Cir. 2024) (“At both the moment of seizure and throughout its duration, the government’s conduct must be reasonable . . .”). In considering whether the government has, by failing to scope electronically stored information, retained materials over which it lacks probable cause for an unreasonably long period of time, courts have considered factors such as the “nature of the defendant’s property interests, the length of the delay, . . . evidence of bad-faith, . . . prejudice to the defendant,” and—perhaps most importantly—“the government’s justification . . . for the delay,” such as “the workload of forensic specialists, technical obstacles, and the need to conduct a privilege review, among other things,” which “may make even a lengthy delay reasonable.” *Maresca*, 2026 WL 948289, at *28; *see also United States v. Smith*, 967 F.3d 198, 212 (2d Cir. 2020) (“[T]he constitutional reasonableness of delay depends on the assessment and balancing of multiple factors.”). This rule “ensure[s] that, despite the large scope of information that the warrants here

returned, the searches and seizures they authorized were not insufficiently particularized.” *Zelaya-Veliz*, 94 F.4th at 338.

This issue very recently came before Judge Randolph D. Moss in *United States v. Maresca*, No. 1:23-cr-123, 2026 WL 948289, at *26 (D.D.C. Apr. 6, 2026), which involved the government’s retention of unscoped electronically stored information for about five years. Before applying the Fourth Amendment’s reasonableness standard to the facts at issue here, the Court begins by describing *Maresca* as it relates to this case.⁴

B. Recent *Maresca* Case

In investigating Maresca for wire fraud, tax evasion, and other offenses, law enforcement officers executed search warrants in 2021 at Maresca’s home and two office suites, seizing 29 digital devices, such as laptops, smartphones, and tablets, in the process. *Id.* at *1. The government did not, however, even begin scoping the devices for well over three years following the seizure of the devices. *Id.* at *29.

Maresca eventually sought an order preventing the government from continuing to search the devices and suppressing what the government had already found on the grounds that it had unreasonably delayed. *Id.* at *1–2. Initially, the government repeatedly assured the court that it would wait to resume searching while the matter was pending before Judge Moss, but despite these reassurances, the government reversed course, secured a new warrant, and began scoping the devices. *Id.* at *10.

⁴ Along with *Maresca*, the government relies on *United States v. Balwani*, No. 5:18-cr-258-2, 2022 WL 1405404, at *1 (N.D. Cal. May 4, 2022), and *United States v. Collins*, 409 F. Supp. 3d 228, 243 (S.D.N.Y. 2019), for support. But *Balwani* and *Collins* are inapt because in each, the court rejected a defendant’s demand that the government search portions of data already determined not to be responsive to the search warrants. *Balwani*, 2022 WL 1405404, at *5; *Collins*, 409 F. Supp. 3d at 243–44. In those cases, the government had lost lawful custody over the nonresponsive data because it had already been segregated from the materials over which the government had probable cause. Put differently, the nonresponsive data had served the only lawful purpose for which the government had temporary authority to possess it. These are not the facts of this case.

In considering Maresca’s motion to suppress, Judge Moss held that the evidence for which Maresca had standing to challenge was suppressible in part because “the government failed even to begin scoping those devices within a reasonable time.” *Id.* at *23. While the government pressed the argument that the new search warrant had “cure[d] any defect resulting from unreasonable delay in segregating the responsive from the non-responsive materials that were first seized in May 2021,” the court sided with Maresca’s view that the new warrant could not retroactively cure the constitutional violation arising from the fact that the government “seiz[ed] devices and then wait[ed] years before even attempting to segregate the material contained on those devices as to which the government undoubtedly lacks probable cause from the responsive material.” *Id.* at *24–25.

In concluding that the evidence should be suppressed, Judge Moss observed that “[i]f the exclusionary rule is to have any deterrent effect, the type of constitutional violation at issue here—failing to segregate responsive from non-responsive material contained on electronic devices for a period of years—must have some consequence, beyond requiring the government to undertake the burden of obtaining a new warrant, years after the fact.” *Id.* at *26. Simply put, attaining a new warrant could “not make the delay between May 2021 and January 2026 any less a violation of Maresca’s constitutional rights.” *Id.* at *25.

However, in considering Maresca’s request to prospectively bar the government from continuing to search the devices, Judge Moss held that the legality of the government’s ongoing retention of the data turned on the existence of new warrants. A new search warrant meant that the government’s possession of nonresponsive materials and scoping of those materials was not an ongoing violation of the Fourth Amendment, even if the evidence found pursuant to the new warrant could be suppressed if traceable to the unreasonable delay violation. *Id.* at *35. In other

words, while the exclusionary rule could retroactively remedy the Fourth Amendment violation that had already occurred, the government could not be prospectively barred from retaining and searching the devices covered by the new search warrant since there was no longer an ongoing Fourth Amendment violation as to those devices. *Id.*

C. Application

Here, in accordance with Rule 41(e), when searching the premises described in “Attachment A” of the July 2021 search warrants, Theia’s headquarters and Olson’s residence, the government seized digital devices containing electronically stored information as described in “Attachment B” of the search warrants. Specifically, Attachment B enumerated the types of data over which the government had probable cause, and the warrant affidavits described the probable cause supporting the seizure of these types of records. But, of course, the devices that the government forensically imaged undoubtedly contained irrelevant information—that is, data not described in Attachment B. So the warrants established a filter team to segregate these materials.

But the Subject Data was never scoped. Instead, the government represents that this evidence has remained “unprocessed, unfiltered, and unreviewed” for the entire period between today and the on-site execution of the search warrants in June 2021. ECF No. 110 at 3.

As to whether a Fourth Amendment violation has occurred, *Maresca* is largely on point. Here, the government retained the unscoped Subject Data nearly five years before attempting to address this issue. What’s more, no one has asserted (nor could reasonably assert) that the 23 terabytes of data constitute *only* responsive materials, meaning that, for half a decade, the government has retained evidence for which it “undoubtedly lacks probable cause.” *Maresca*, 2026 WL 948289, at *24–25. As in *Maresca*, “the government’s prolonged retention of non-responsive material, and its failure to make any meaningful effort to segregate non-responsive

material from responsive material for more than four years, cannot be reconciled with the Fourth Amendment’s reasonableness standard.” *Id.* at *28.

Much like *Maresca*, this case is distinguishable from the cases where courts have found multi-year periods reasonable to review large amounts of electronically stored information because here, several years passed during which the government did not even begin to scope the seized images. *See United States v. Bradley*, 644 F.3d 1213, 1256–58 & 1258 n.95 (11th Cir. 2011) (holding that the government’s off-site review of 103 computers containing more than a terabyte of data was not unreasonably delayed even when it took three years from start to finish in part because the government “made a preliminary pass over the imaged data” to “separate out potentially relevant documents from those that were certainly irrelevant” within the first year after seizing the data and began distributing batches of documents to case agents immediately thereafter); *see also United States v. Mendlowitz*, No. 17-cr-248, 2019 WL 1017533, at *11–12 (S.D.N.Y. Mar. 2, 2019) (holding that an eighteen-month period for reviewing an “exceedingly large” “universe of documents” was reasonable where the government began its review two months after the search warrant had been executed on-site). “Although lengthy delays are acceptable under some circumstances, the lacuna of more than four years in this case—when almost no effort was made to scope the devices—does not fall within the bounds of delay sanctioned by courts.” *Maresca*, 2026 WL 948289 at *29.

While not binding, the Court finds *Maresca* eminently persuasive and unavoidable on the facts presented here. And since the delay has resulted in an unlawful seizure, “[a]t this point, the government’s only options are to ‘cease the seizure or secure a new justification’—*i.e.*, a new warrant authorizing the seizure of the non-responsive material.” *Id.* at *33 (quoting *Brewster v.*

Beck, 859 F.3d 1194, 1197 (9th Cir. 2017)). Here, the government has chosen to do the former, and the Court knows of no basis for it to compel the latter.

The Court recognizes that this matter is peculiar in that the government seeks to use the Fourth Amendment as a shield against any potential *Brady* obligation it may have regarding the Subject Data, were that evidence in its lawful possession. In holding that the government may transfer and delete the 23 terabytes of electronically stored information at issue here, the Court recognizes that this opinion in some sense rewards the conduct that the *Maresca* line of cases seeks to deter. The Subject Data has been in the government's possession since June 2021. Since that time, troves of unscoped digital evidence have sat on the government's systems, and all the while the government made no effort to segregate responsive material from nonresponsive material, thereby retaining information over which it undoubtedly lacked probable cause well past the appropriate window for doing so.

What's more, in arguing that *Maresca*'s reasoning applies here, the government makes no mention of the fact that, in that case, it had argued to Judge Moss that its continued retention of materials not covered by the new search warrant was justified on the basis that barring the government's future access of the forensic images would prevent it from fulfilling its "obligation to provide discovery to Maresca's co-defendants under *Brady v. Maryland*, 373 U.S. 83 (1963) and its progeny." *Id.* at *32. Judge Moss disposed of this argument easily, since the defendants there had expressly waived their rights to assert any *Brady* rights with respect to the unscoped and unsearched devices. *Id.* at *12, *36.

Still, while there is obviously no such waiver here, the Court nevertheless concludes that the Fifth Amendment duty to search for and disclose exculpatory evidence is subordinate to the Fourth Amendment limitations on unreasonable seizures in this context. As several courts have

observed, “[t]he government’s obligations under *Brady* only extend to information in its possession, custody, or control,” meaning that a prosecutor has no duty “to seek out and disclose exculpatory or impeaching material not in the government’s possession.” *United States v. Celestin*, 612 F.3d 14, 22 (1st Cir. 2010) (first quoting *United States v. Hall*, 434 F.3d 42, 55 (1st Cir.2006), and then quoting *United States v. Bender*, 304 F.3d 161, 164 (1st Cir. 2002)); *see also United States v. Crump*, No. 24-3453, 2026 WL 1873674, at *14 (8th Cir. June 30, 2026) (holding that the government had no *Brady* obligation as to evidence that was “not in the government’s possession or control” because it fell outside the scope of the applicable warrant).

But more to the point, Defendants have cited no law suggesting that the Court can order the government to secure a new warrant, or else continue an unlawful seizure, for the sole purposes of fulfilling any existing *Brady* obligations. Absent such precedent, the Court has no grounds on which to grant the relief sought. The motion is therefore denied. However, Rule 17(c)(1) of the Federal Rules of Criminal Procedure contemplates that Defendants may be able to subpoena Brevet and Defendant Olson. The Court expects Brevet and Olson to preserve any responsive evidence in accordance with Rule 17(c)(1), should such subpoenas issue. The Clerk’s office shall provide a copy of this order to Brevet’s counsel.

III. CONCLUSION

For the reasons given above, Defendants’ motion to preserve the Subject Data is **DENIED**.

IT IS SO ORDERED.

Date: 7-22-26


 Royce C. Lamberth
 United States District Judge