UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF TWENTY-SIX (26) DIGITAL DEVICES AND MOBILE DEVICE EXTRACTIONS THAT ARE CURRENTLY IN THE POSSESSION OF LAW ENFORCEMENT IN WASHINGTON D.C.	Case No. 21-sw-233 (GMH) Chief Judge Beryl A. Howell **REDACTED**

MEMORANDUM OPINION AND ORDER

Pending before the Court is the government's request for review of a magistrate judge's denial of a warrant to search data extractions from four cell phones, which were lawfully seized and previously lawfully searched pursuant to search warrants issued in connection with now completed investigations and prosecutions of the two individuals from whom the cell phones were seized. Gov't's Mot. Review Mag. J.'s Partial Denial Search Warrant Appl. ("Gov't's Mot.") at 2, 6–9, ECF No. 27.[1] In denying the requested warrant for further search of the cell phone data extractions, the magistrate judge acknowledged the instant warrant is supported by probable cause to believe the search may uncover evidence relevant to a new investigation into various firearm offenses [REDACTED], and satisfies the particularity requirement of the Fourth Amendment. Mag. J. Mem. Op. & Order (Nov. 30, 2021) at 6–8, ECF No. 16 (hereinafter "MJ Decision"); *Matter of Search of Twenty-Six (26) Digital Devices & Mobile Device Extractions That Are Currently in Possession of L. Enf't in Washington D.C.*, No. 21-SW-233 (GMH), 2021 WL 5822583, at *3–4 (D.D.C. Nov. 30, 2021) (hereinafter "*Redacted MJ Decision*").

[1] This matter is directly assigned to the undersigned Chief Judge under this Court's Local Civil Rule 40.7 and Local Criminal Rule 57.14, which provide that "the Chief Judge shall . . . hear and determine requests for review of rulings by magistrate judges in criminal matters not already assigned to a district judge." D.D.C. LCvR 40.7(e); D.D.C. LCrR 57.14(e).

Nonetheless, in a thorough decision echoing possessory- and privacy-related concerns expressed *in dicta* by courts outside this Circuit about the government's retention of data extracted from digital devices, the magistrate judge concluded "the government lacks an entitlement to retain possession of the devices and the data extractions following completion of the underlying prosecutions," making its request to search the extractions again "unreasonable." *Redacted MJ Decision*, 2021 WL 5822583, at *25.

This matter raises a novel Fourth Amendment issue in this Circuit: whether an otherwise appropriate search warrant runs afoul of the general warrant prohibition and is therefore barred when its execution involves a search of cell phone data extractions obtained during execution of a prior valid search warrant on devices that lawfully came into the government's possession in connection with a closed, unrelated prosecution. *Id.* at *4. While agreeing that the requested warrant meets both the probable cause and particularity requirements to search the extracted cell phone data for evidence relevant to a new investigation, this Court disagrees with the magistrate judge's ultimate conclusion that the Fourth Amendment bars the government from executing this search warrant to query the lawfully seized cell phone data because the extracted data has been retained in the government's possession for too long.

For reasons explained more fully below, this Court holds that protection of legitimate privacy and possessory concerns is the precise job of the Fourth Amendment warrant requirement. The Fourth Amendment does not operate as an arbiter of law enforcement retention policies for lawfully seized evidence, and supplementing warrant prerequisites to impose retention time limits would run the risk of arbitrarily creating undue burdens on law enforcement that frustrate legitimate and reasonable law enforcement interests.

Law enforcement here did exactly what the Fourth Amendment requires: for the purpose of uncovering evidence of criminal activity, the government presented before a neutral magistrate judge probable cause to believe that evidence relevant to specific criminal conduct is reasonably likely to be found in a particular location. The fact that this particular location happens to be in lawfully seized, previously lawfully searched extracted cell phone data already in the custody of law enforcement means merely that the search may be readily accomplished and does not necessitate examination of separate questions of whether law enforcement's continued custody of such evidence is justified by reasons other than compliance with evidence retention requirements, and whether a new search would unduly "impact . . . the device owner's possessory interests." *Id*.

To construe the Fourth Amendment warrant requirement to encompass these separate inquiries would expand the reach of what this constitutional mandate guarantees far beyond well-settled law and require judicial line-drawing about the time periods during which law enforcement may have continued need to retain and appropriately search anew lawfully seized, previously searched evidence, regardless of the broad range of multiple factors that may affect when further examination of such evidence occurs, such as investigative work load priorities, the type of evidence at issue, the availability of new or more effective forensic tools, data retention policies, or, as here, the emergence of new investigative leads providing probable cause to believe such evidence may reveal new criminal conduct. The Supreme Court has never so construed the Fourth Amendment.

The stakes are high. In creating *ex ante* restrictions on evidence retention and basing such restrictions in constitutional requirements under the Fourth Amendment, courts would compel law enforcement to ignore, destroy, or release lawfully seized evidence (or copies of

such evidence) at some arbitrary point, beyond which the evidence is unavailable for use in a subsequent investigation, thereby potentially forcing law enforcement to re-seize relevant evidence in person, with the concomitant intrusiveness associated with such a seizure, as well as the potential danger, risks of evidence destruction, and cumulative problems that entails, all for the sake of retrieving evidence law enforcement had already lawfully seized, searched, and reasonably retained for use in an earlier investigation and prosecution.

The issue here is not whether the government lawfully seized the cell phones. It did. Nor whether the government properly executed a search warrant to extract and search data from the cell phones. It did. Nor whether the government has probable cause to conduct a further search of the extracted data for evidence of additional criminal wrongdoing. It does. Nor whether the government has satisfied the particularity requirement for the new search requested. It has. The question at issue is whether the Fourth Amendment prohibits the government from executing a perfectly valid new search warrant to query retained data from execution of a prior search warrant because the closing of the criminal case for which the data was originally seized renders the retained data off-limits for further investigatory use. The answer is that the Fourth Amendment presents no such bar. Thus, for the reasons set forth below, the warrant is approved.

I. BACKGROUND

Summarized below is the relevant factual and procedural history.

A. Factual Background

Law enforcement agencies in the District of Columbia (the "District") have recently focused investigatory efforts on the proliferation of [REDACTED] firearms [REDACTED]. Gov't's Mot. at 5. [REDACTED]. *See* Aff. of Susan Wittrock in Supp. of Appl. for Search Warrant ("Wittrock Aff.") ¶¶ 8–12, 16, 30, ECF No. 5 (citing 18 U.S.C. § 922(a)(1) (Manufacturing or Dealing in Firearms Without a License); *see also* 18 U.S.C. § 922(d)

(prohibiting the sale or transfer of a firearm to any person if known or reasonably believed that such person is prohibited from possessing or receiving firearms); *id.* § 922(g) (prohibiting possession or receipt of firearms by any person whose status is enumerated under the statute). [REDACTED]. Wittrock Aff. ¶ 16.

The District has seen this trend play out, with exponential increases in the numbers of [REDACTED] being seized in connection with criminal investigations. [REDACTED]. These firearms were used in a variety of criminal activities including "unlawful firearm possession, homicide, assault with intent to kill, assault with a dangerous weapon, robbery, and destruction of property." *Id.* ¶ 18. The government has reason to believe that the bulk of these [REDACTED] entered the District through unlawful [REDACTED] trafficking. *Id.* ¶¶ 16, 30.

Beginning in about February 2021, a task force of law enforcements officers led by the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF") has been investigating the [REDACTED] trafficking, and possession of [REDACTED] guns. *Id.* ¶¶ 7, 18. As part of ATF's efforts to identify those responsible for committing possible violations of 18 U.S.C. § 922(a)(1)(A) (Manufacturing or Dealing in Firearms without a License), and 18 U.S.C. § 371 (Conspiracy) (hereinafter "the Target Offenses"), ATF has reviewed records in cases where arrested individuals possessed [REDACTED]. *Id.* ¶¶ 6–7.

Analysis of the [REDACTED]. *Id*. In approximately 47 of those 120 [REDACTED] recoveries, law enforcement also seized a cell phone in tandem with the [REDACTED]. *Id.* ¶¶ 26–27. Out of those 47 [REDACTED] recoveries that also involved a cell phone, 26 were identified with [REDACTED]. *Id.* ¶¶ 26, 28, 31. Put another way, law enforcement recovered

each cell phone near or on persons connected with unlawful possession of [REDACTED] that contained [REDACTED]. *Id.* ¶ 91.

B. Procedural Background

The government sought to further its investigation into the identities of individuals unlawfully [REDACTED] trafficking [REDACTED] by searching the 26 cell phones or digital copies of the data extracted by law enforcement from those phones (the "Target Devices"), for information related to the acquisition, [REDACTED] sale, or receipt of the [REDACTED] seized in tandem with the Target Devices. Appl. for Warrant by Tel. or Other Reliable Elec. Means ("Warrant Appl."), ECF No. 5; Warrant Appl. Attach. B, ECF No. 5. On July 22, 2021, the government first applied for the warrant to search all 26 Target Devices, *see* Gov't's Mot. at 9, and following the submission of supplemental briefing in support of the requested search warrant, *see* Gov't's Mem. Supp. Requested Search Warrant ("Gov't's Mem."), ECF No. 4, the magistrate judge granted the application as to four Target Devices (numbered 5, 6, 14, and 15), Mag. J. ("MJ") Order (Aug. 18, 2021) at 1, ECF No. 6. The magistrate judge explained that the warrant was granted as to these four Target Devices because the warrant application and supplemental briefing established that the devices were abandoned prior to their seizure by law enforcement "and thus the [owners] no longer have a possessory interest in the devices" and have forfeited any expectation of privacy for those devices, which removes the devices from the Fourth Amendment's protections. *Id.* at 4–6; *see also Redacted MJ Decision*, 2021 WL 5822583, at *2.[2]

[2] Three of these four Target Devices had been discarded by a fleeing person during a police chase and the fourth was found during a law enforcement canvass of an area where gunshots had recently been heard. MJ Order (Aug. 18, 2021) at 4–6. Under these circumstances, all four devices were deemed "abandoned" by the magistrate judge and thus outside any Fourth Amendment protection. *Id.* at 6; *Redacted MJ Decision*, 2021 WL 5822583, at *2.

As to the remaining 22 Target Devices, the magistrate judge requested additional briefing regarding "the basis and legitimacy of the government's initial seizure of the devices and/or device extractions, the length of and justification for their continued retention by the government, and the reasonableness of the government's request that it now be permitted to search them to benefit a subsequent criminal investigation." MJ Order (Aug. 18, 2021) at 12–13. The government thereafter withdrew the request to search half of the 22 Target Devices but continued to seek warrants to search the remaining eleven devices. Gov't's Resp. Court's Aug. 18, 2021 Order ("Gov't's Resp.") at 1–2, ECF No. 11.[3]

After submission of additional briefing and hearing the government's arguments on September 27, 2021, the magistrate judge issued, on November 30, 2021, a comprehensive written decision partially granting and denying the warrant application. Specifically, the magistrate judge granted the warrant to search seven more Target Devices (numbered 1, 2, 7, 13, 21, 22, and 23) because the government (1) initially seized each device pursuant to either a valid search warrant or a search incident to a lawful arrest based on probable cause, (2) exhibited reasonable diligence in pursuing the instant warrant based on a serious and legitimate subsequent investigation, and (3) presented "a compelling basis" for retaining the devices due to their status as evidence in a prosecution that was ongoing at the time of instant warrant application, all of which, the magistrate judge determined, outweighed the owners' "significant" possessory interest in the devices. *Redacted MJ Decision*, 2021 WL 5822583, at *15. At the same time, the application was denied as to four Target Devices (numbered 16–19) because the government

[3] The government did not provide a detailed explanation for withdrawal of its request to search eleven of the Target Devices, stating only that "[w]hile the government disagreed with the [magistrate judge]'s pre-warrant reasonableness inquiry as a matter of law . . . in light of the [magistrate judge]'s orders at the time, the government elected to seek warrants as to those devices it believed were in the best position to successfully address the concerns raised by the [magistrate judge]." Gov't's Mot. at 1 n.2.

failed to establish "the overall reasonableness of the government's requested search," *id.* at *4, as the government had not shown that its retention of the Target Devices after the conclusion of the prosecutions of the individuals from whom the devices were seized was supported by "a sufficient basis entitling it to possession of [the devices]" that would "justify its request to search those cell phones again in a subsequent investigation in the face of the defendant's significant, if somewhat diminished, possessory interests in those devices," *id.* at *24–25.

In assessing whether the government had "a sufficient basis" for continued retention of the cell phones, the magistrate judge focused on the stage of the investigation or prosecution of the individuals from whom the Target Devices were seized: if the prosecution was still ongoing, with outstanding charges against the defendant not resolved, a second search of the seized device was allowed, *id.* at *6 (noting, in approving the warrant to search Target Devices 1, 2, 7, 13, 21, 22, and 23, "that each device is itself being retained as evidence in those ongoing proceedings, a fact that weighs heavily in the Court's consideration of all of the factors"). Conversely, if the prosecution had been resolved and the defendant sentenced, a second search was not permitted. *Id.* at *15 (denying warrant application as to Target Devices 16–19 because they "are not associated with ongoing prosecutions"). The fact that the new investigative lead prompting the instant warrant application only arose after the conclusion of the prior prosecutions was immaterial to this analysis; such inopportune timing simply dooms the warrant.

After three extensions of the deadline to seek review of the partial denial of the warrant application, *see* Min. Orders (Dec. 13, 2021, Dec. 21, 2021, Jan. 5, 2022), the government filed the instant motion to review the magistrate judge's November 30, 2021 decision and renewed its application for issuance of the warrant for four Target Devices 16–19, Gov't's Mot. at 1–2; *see generally* Warrant Appl.

C. The Requested Warrant: Target Devices 16, 17, 18, and 19

On review, the government requests a warrant to search for relevant data from four cell phone extractions—Target Devices 16, 17, 18, and 19—currently in law enforcement custody and obtained from four cell phones that were (1) seized on or about [REDACTED] 2019, in connection with the arrests of two individuals for unlawful possession of firearms—[REDACTED], and (2) searched pursuant to search warrants issued by the D.C. Superior Court. *See* Wittrock Aff. ¶¶ 65–68; Warrant Appl., Attachs. A-16, A-17, A-18, A-19. The facts underlying the seizures of these four devices are described as follows by the magistrate judge: On [REDACTED] 2019, after seeing an Instagram live feed featuring three males holding firearms and smoking what appeared to be marijuana, law enforcement identified their location and, within twenty minutes of the live-streamed video, arrived at that building location and saw two individuals trying to run inside a particular apartment. *Redacted MJ Decision*, 2021 WL 5822583, at *15. During a consent search of that apartment, two individuals were arrested inside a bedroom, where "[a] number of firearms were recovered from the closet, each of which matched the appearance of guns seen on the live-streamed video." *Id*. Target Devices 16 and 17 were seized incident to the arrest of one of the two individuals and Target Devices 18 and 19 from the other individual. *Id*.

The prosecutions for both individuals have concluded, with each individual pleading guilty on March [REDACTED] 2020, and being sentenced on October [REDACTED] 2020, and December [REDACTED] 2020, respectively. Gov't's Mot. at 8. Although two of the cell phones were released back to their owner, no efforts have been made to retrieve the remaining two cell phones, and they remain in law enforcement's custody. *Id*. Nonetheless, the government retained copies of the extractions from all four phones, pursuant to its data retention policies. *See id.* at 8–9; *see also* U.S. Dep't Just., Just. Manual §§ 9-14.000–14.009.

According to the government, a search of Target Devices 16, 17, 18, and 19 "could yield evidence of the person's connection to the [REDACTED], as well as possible evidence of unidentified conspirators who were involv[ed] in acquiring the firearm [REDACTED]. Gov't's Mot. at 5; *see also* Wittrock Aff. ¶¶ 91, 94–95. The government reasons that because law enforcement recovered the Target Devices and [REDACTED] from individuals [REDACTED], there is probable cause to believe that the Target Devices contain the desired evidence as "[i]t is common for individuals engaged in the unlawful [REDACTED]trafficking/possession of firearms to use . . . telephonic communications . . . [and] social media . . . to further their criminal activities." Wittrock Aff. ¶ 94. For example, individuals engaging in the unlawful [REDACTED] trafficking, or possession of firearms often use their phones (1) "to communicate and remain in contact with sources, customers, or possessors of . . . firearms"; (2) "to exchange information with customers and/or sources of supply" through text messages, direct messages, telephone conversations, photographs, and videos; and (3) "to take video recordings and photographs of themselves or other[s] . . . engaging in illegal activities, such as the assembling of firearms, supply of firearms for sale, or brandishing of firearms." *Id*. Thus, a review of such evidence stored as electronic data in Target Devices 16, 17, 18, and 19 may enable ATF to identify the [REDACTED] traffickers, customers, associates, and co-conspirators involved in the Target Offenses as well as the methods by which the Target Offenses have been committed.

II. LEGAL STANDARD

Under 28 U.S.C. § 636(b)(3), "[a] magistrate judge may be assigned such additional duties as are not inconsistent with the Constitution and laws of the United States." As this matter was not "designate[d]" to a magistrate judge by a district court judge within the meaning of § 636(b)(1)(A) or (B), the order denying the government's application is an exercise of the

magistrate judge's "additional duties," pursuant to § 636(b)(3), in conjunction with this Court's Local Criminal Rule 57.17(a), under which magistrate judges are granted the "duty and the power" to "[i]ssue search warrants," as well as to "[i]ssue subpoenas . . . or other orders necessary to obtain the presence of parties or witnesses or evidence needed for court proceedings." D.D.C. LCrR 57.17(a)(3), (10).

Pursuant to Local Criminal Rule 59.3, a "magistrate judge's warrant or order for which review is requested" in a "criminal matter not assigned to a district judge, . . . may be accepted, modified, set aside, or recommitted to the magistrate judge with instructions, after de novo review by the Chief Judge." D.D.C. LCrR 59.3(a), (b); *see also In re Search of Info. Associated with [redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-757 (BAH), 2017 WL 3445634, at *5 (D.D.C. July 31, 2017) (noting that "because this case arises out of the Magistrate Judge's 'additional duties' jurisdiction pursuant to § 636(b)(3), the Magistrate Judge's order is subject to *de novo* review by the district court"). Accordingly, the magistrate judge's order is subject to *de novo* review.

III. DISCUSSION

As noted, despite finding that the warrant application adequately established probable cause to search the Target Devices at issue and sufficiently described with particularity the place to be searched and the things to be seized, *Redacted MJ Decision*, 2021 WL 5822583, at *3–4, the magistrate judge denied the application based on an assessment of the "overall reasonableness of the government's requested search," *id.* at *4. The government challenges the legal framework adopted by the magistrate judge to justify partial denial of the warrant application, Gov't's Mot. at 1–3, which framework would require, "in cases where the warrant arises as part of an investigation different from the investigation in which the device was seized,"

a "constitutional inquiry" involving "an assessment of . . . the reason for any delay in the search request, the sufficiency of the basis for the government's continued retention of the device thereby making it available for search in another investigation, and a consideration of the search's impact on the device owner's possessory interests," *Redacted MJ Decision*, 2021 WL 5822583, at *4.

As explained below, superimposing on the warrant requirement "an additional and freestanding reasonableness analysis," Gov't's Mot. at 2, focused on the timing of the government's request in relation to both the status (as closed or ongoing) of the original investigation for which the evidence was seized and initially searched, and the duration of the retained digital data in the government's custody, as well as the possessory or privacy interests of the data owner, is not required by the Fourth Amendment. Instead, because the government has demonstrated adequate probable cause, as required by the Fourth Amendment, in support of the application to search the four Target Devices, and the warrant is sufficiently particularized to pass constitutional muster, the warrant shall issue as to Target Devices 16, 17, 18, and 19.

After review of the current state of the law governing application of the Fourth Amendment to government requests for electronically stored information ("ESI") located on or derived from cell phones, the appropriateness of the proposed reasonableness inquiry for issuance of a search warrant is addressed.

A. Fourth Amendment Application to ESI Recovered from Cell Phones

The first clause of the Fourth Amendment safeguards "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. As the Supreme Court has stressed, "the text makes clear, 'the ultimate touchstone of the Fourth Amendment is "reasonableness."'" *Riley v. California*, 573 U.S. 373, 381 (2014) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)). The second clause of

the Fourth Amendment goes on to prescribe: "and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

In assessing whether a particular search meets the reasonableness standard, courts must balance the search's "intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests." *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652–53 (1995) (quoting *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 619 (1989)). The Supreme Court has explained that "[i]n most criminal cases, we strike this balance in favor of the procedures described by the Warrant Clause of the Fourth Amendment," with the result that, with some exceptions, "a search or seizure in such a case is not reasonable unless it is accomplished pursuant to a judicial warrant issued upon probable cause." *Skinner*, 489 U.S. at 619; *see also Riley*, 573 U.S. at 382 ("Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant." (omission in original) (quoting *Vernonia*, 515 U.S. at 653)).

The question addressed in *Riley* was "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who had been arrested." *Riley*, 573 U.S. at 378. The Court answered no, holding that "officers must generally secure a warrant before conducting such a search." *Id.* at 386. The reasoning underpinning this holding illuminates considerations relevant here. Relying on its prior caselaw concerning searches incident to arrest, the Supreme Court concluded that the concerns identified in that line of cases—fears about officer safety and evidence preservation—are not implicated by digital data stored on cell phones. *Id.* at 382–86. First, the Supreme Court aptly noted "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the

arrestee's escape," which eliminated the primary concern underlying the search-incident-to-arrest doctrine. *Id.* at 387–88. Second, the risk of evidence destruction is also mitigated by the officer's arrest of the individual and securing of the phone without any need to search the digital data until a warrant is secured. *Id.* at 388–90. In short, the rationales guiding the search-incident-to-arrest cases were found to have little relevance to digital data stored on a cell phone.

The Supreme Court also emphasized "[t]he search incident to arrest exception rests not only on the heightened government interests at stake in a volatile arrest situation, but also on an arrestee's reduced privacy interests upon being taken into police custody." *Id.* at 391. The Court, however, quickly noted that unlike the approved searches of physical items seized upon arrest, the search of a cell phone and its digital data "implicate privacy concerns far beyond those implicated by the search of [other personal items such as] a cigarette pack, a wallet, or a purse." *Id.* at 393. Cell phones, with their immense storage capacity, raise many heightened privacy concerns as their data includes "many distinct types of information . . . that reveal much more in combination than any isolated record." *Id.* at 394. Furthermore, the digital data held in a cell phone may allow law enforcement to reconstruct "[t]he sum of an individual's private life," as it can reveal private interests and concerns including such personal information as "someone's specific movements down to the minute," "detailed information about all aspects of a person's life," a person's political leanings, history of commercial transactions, romantic interests, addictions, personal health information, and so on. *Id.* at 394–96. In short, a search of a cell phone's ESI "would typically expose to the government far *more* than the most exhaustive search of a house," *id.* at 396 (emphasis in original), which the Court had already determined required a warrant to be searched incident to an arrest. Thus, despite the diminished privacy expectations of an arrestee, the Supreme Court concluded the weighty privacy-related concerns

engendered by a search of ESI in a cell phone required a warrant before searching a cell phone seized incident to an arrest. *Id.* at 403 ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."). The Court broadly held "information on a cell phone is [not] immune from search," but "instead . . . a warrant is generally required before such a search." *Id.* at 401.

Confronted with *Riley*'s straight-forward command, the government pursued probable cause warrants here at each juncture before searching the Target Devices, both after its initial seizure of the cell phones during a search incident to an arrest and in connection with the subsequent investigation of [REDACTED] into the District. The magistrate judge concluded, however, that compliance with *Riley*'s warrant command was not enough here. Drawing on *Riley*'s recognition of the volume of personal data and information held on cell phones, and the concomitant possessory interest an individual has in that information, *Redacted MJ Decision*, 2021 WL 5822583, at *12, the magistrate judge found that possessory interests extend to any such data retained by law enforcement, *id*. *12–15, *21–24, and that those interests simply may not be overcome, even with a valid warrant, when the government's initial evidentiary use of the data has been exhausted with completion of a prosecution, *id*. at *24. This is an extraordinary stretch of *Riley*'s holding.

Contrary to the magistrate judge's determinations, the government's approach, as discussed next, prudently comports with binding caselaw establishing the Fourth Amendment rules law enforcement must follow when investigatory steps may significantly intrude on possessory or privacy interests during the search of ESI on or derived from cell phones.

B. The Government's Conduct and Warrant Application Satisfy Fourth Amendment Requirements

"The 'basic purpose of [the Fourth] Amendment . . . is to safeguard the privacy and security of individuals against *arbitrary* invasions by governmental officials.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) (emphasis added) (quoting *Camara v. Mun. Ct. of San Francisco*, 387 U.S. 523, 528 (1967)). Accordingly, the Fourth Amendment's "'central requirement' is one of reasonableness." *Illinois v. McArthur*, 531 U.S. 326, 330 (2001). "In order to enforce that requirement, [the] Court has interpreted the Amendment as establishing rules and presumptions designed to control conduct of law enforcement officers that may significantly intrude upon privacy [or possessory] interests." *Id*. Generally, "those rules require warrants." *Id*.; *see also Elkins v. District of Columbia*, 690 F.3d 554, 564 (D.C. Cir. 2012) ("The warrant requirements of the Fourth Amendment are not mere formalities, but serve the high function of shielding citizens' private lives from all but necessary and fully justified governmental intrusion." (internal quotation and citation omitted)).

The Fourth Amendment warrant requirement "protect[s] two distinct interests": "First, the warrant requirement seeks to guarantee that any searches [or seizures] intruding upon an individual's privacy must be justified by probable cause, as determined by a 'neutral and detached magistrate,' [and] [s]econd, where probable cause is found and a warrant issues, the particularity requirement seeks to assure that those searches [and seizures] deemed necessary should be as limited as possible." *United States v. Heldt*, 668 F.2d 1238, 1256 (D.C. Cir. 1981) (internal quotation and citation omitted). The particularity requirement is intended to leave "nothing . . . to the discretion of the officer executing the warrant," *id.* (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)), and avoid "the specific evil [of] the 'general warrant' abhorred by the colonists" authorizing "a general, exploratory rummaging in a person's

belongings," *id.* (quoting *Coolidge v. New Hampshire*, 402 U.S. 443, 467 (1971) (plurality opinion)). Upon a showing by the government that its application to search Target Devices 16–19 demonstrates "a fair probability that . . . evidence of a crime will be found in a particular place," and satisfies the particularity requirement, a search warrant may issue. *Illinois v. Gates*, 462 U.S. 213, 238 (1983); *see also* FED. R. CRIM. P. 41(d) ("After receiving an affidavit or other information, a magistrate judge . . . must issue the warrant if there is probable cause to search for and seize a person or property . . . .").

In a careful review of the warrant and supporting application, the magistrate judge found that the government fulfilled the probable cause and particularity warrant requirements. *Redacted MJ Decision*, 2021 WL 5822583, at *3–4. This Court agrees and adopts that finding in full.

The warrant to search Target Devices 16–19 was nonetheless denied upon the magistrate judge's finding that the overall reasonableness of the government's requested search fell outside constitutional bounds because the requested warrant "arises as part of an investigation different from the investigation in which the device was seized," and therefore raises "questions regarding the reason for any delay in the search request, the sufficiency of the basis for the government's continued retention of the device thereby making it available for search in another investigation, and a consideration of the search's impact on the device owner's possessory interests." *Id.* at *4. This proposed reasonableness inquiry essentially adds to the wholly separate warrant requirements of probable cause and particularity three additional overlapping considerations: (1) the timing of the search in relation to the original purposes for which the evidence was seized; (2) the justification for the retention of the target data in the government's continued possession, beyond compliance with applicable evidence retention policies, which standing alone are

insufficient; and (3) any continuing privacy or possessory interests of the owner of the data. A legal framework requiring this additional three-pronged reasonableness inquiry to search previously lawfully seized and searched digital extractions for evidence of a separate crime suffers several legal and practical flaws, starting with being unnecessary to protect possessory or privacy interests.

1. *Satisfaction of the Warrant Requirement Sufficiently Safeguards Privacy Interests*

First, the imposition of a three-pronged reasonableness inquiry as a prerequisite to conduct a new search of lawfully seized and searched retained digital data for evidence of criminal activity disregards bedrock Fourth Amendment caselaw establishing that satisfaction of the warrant requirement is generally enough to safeguard the constitutional guarantee of privacy. *See Mitchell v. Wisconsin*, 139 S. Ct. 2525, 2550–51 (2019) (Sotomayor, J., dissenting) (quoting *Skinner*, 489 U.S. at 621–22); *see also Zurcher v. Stanford Daily*, 436 U.S. 547, 554 (1978) ("As the Fourth Amendment has been construed and applied by this Court, 'when the State's reason to believe incriminating evidence will be found becomes sufficiently great, the invasion of privacy becomes justified and a warrant to search and seize will issue.'" (quoting *Fisher v. United States*, 425 U.S. 391, 400 (1976))); *Camara*, 387 U.S. at 534 ("'[P]robable cause' is the standard by which a particular decision to search is tested against the constitutional mandate of reasonableness."). As the Supreme Court's admonishment in *Riley* reflects, the prevailing guidance in the subsequent search context is simple: get another warrant. *See United States v. Burgess*, 576 F.3d 1078, 1094–95 (10th Cir. 2009) (noting caselaw requires law enforcement to obtain a new warrant to search previously seized evidence for possible criminal violations outside the scope of the initial warrant); *United States v. Giberson*, 527 F.3d 882, 890–91 (9th Cir. 2008) (holding the government acted reasonably when it secured a separate warrant to

search for evidence of criminal activity not covered by a previously-issued warrant); *United States v. Keszthelyi*, 308 F.3d 557, 571 (6th Cir. 2002) (concluding that once the execution of a warrant is complete, law enforcement is "required to apply for a new warrant or identify a valid exception to the warrant requirement authorizing [a second search of previously searched evidence]"); *see also United States v. Nasher-Alneam*, 399 F. Supp. 3d 579, 592 (S.D. W. Va. 2019) ("Under the Fourth Amendment, when law enforcement personnel obtain a warrant to search for a specific crime but later, for whatever reason, seek to broaden their scope to search for evidence of another crime, a new warrant is required."); *id.* at 592–94 (collecting cases); *see generally Riley*, 573 U.S. at 401 (holding searches of cell phones seized incident to arrest require a warrant).

The government followed that prescription to the letter. Here, the government initially seized Target Devices 16–19 during their investigation and arrest of two individuals featured in a live video on Instagram brandishing firearms and smoking what appeared to be marijuana. *Redacted MJ Decision*, 2021 WL 5822583, at *15. After timely obtaining warrants to search the devices for evidence related to the defendants' unlawful possession of firearms, the government searched and extracted data from the four devices pursuant to the warrants. *Id.* at *17. The government's subsequent and separate investigation of [REDACTED] in the District led the government reasonably to believe that evidence of unlawful firearm [REDACTED] trafficking would also be found on the Target Devices. Realizing law enforcement retained the extracted data from the Target Devices pursuant to evidence retention polices, the government requested a search warrant authorizing a search of the retained data from the Target Devices for evidence of [REDACTED] firearms [REDACTED] trafficking offenses. Once the magistrate judge determined that the probable cause and particularity requirements had been met, the

warrant should have issued. *Cf. United States v. Hulscher*, No. 4:16-CR-40070-01-KES, 2017 WL 657436, at *2 (D.S.D. Feb. 17, 2017) (concluding that when law enforcement discovered, during subsequent investigation, the probability that a digital copy of a defendant's phone created pursuant to a lawful search warrant might contain evidence of a separate offense not detailed in the original search warrant, "[t]he conclusion [wa]s inescapable: [the agent] should have applied for and obtained a second warrant [that] would have authorized him to search [defendant's] cell phone data for evidence of [the new] offenses" (first and fourth alteration in original) (citation omitted)).

2. *Retention of Evidence Lawfully Seized and Searched Pursuant to a Search Warrant Does Not Implicate Fourth Amendment Concerns*

Second, the magistrate judge's assessment of the reasonableness of the government's proposed search is based on caselaw that is inapplicable to the factual circumstances underlying the warrant at issue. Relying on cases holding that a delay in securing a warrant may render a warrantless seizure unreasonable under the Fourth Amendment and prohibit any subsequent searches, the magistrate judge evaluated (1) "the lawfulness of the government's initial seizure," (2) the timing of the government's request to search the retained data, and (3) the government's justification for retaining the evidence, balanced against the owner's possessory interest in the Target Devices. *Redacted MJ Decision*, 2021 WL 5822583, at *4, *6 (citing *United States v. Wilkins*, 538 F. Supp. 3d 49, 89 (D.D.C. 2021); *United States v. Smith*, 967 F.3d 198, 205 (2d Cir. 2020); *United States v. Laist*, 702 F.3d 608, 612–13 (11th Cir. 2012); and *United States v. Burgard*, 675 F.3d 1029, 1032 (7th Cir. 2012)). The unreasonable delay line of caselaw utilizes these three factors to assess the reasonableness of the length of time the government seizes and retains evidence without securing a warrant to justify its intrusion on an owner's possessory interests. According to the magistrate judge, a finding of probable cause and particularity does

not address the reasonableness concerns raised by these cases because in each case, law enforcement later secured a warrant. *Id.* at *4 & n.4. This observation misses the mark, however.

The critical focus of the unreasonable delay cases is not on the reasonableness of any subsequent search conducted pursuant to a warrant but on the reasonableness of the *initial warrantless seizure*. The line of unreasonable delay cases highlights the link between the right of the people to be secure against "unreasonable searches and seizures" provided by the first clause of the Fourth Amendment and the importance of the safeguards guaranteed by the second clause—the warrant requirements. To enforce the first clause, the Supreme Court has generally interpreted the Fourth Amendment as demanding law enforcement meet the requirements of the second clause. *See McArthur*, 531 U.S. at 330 ("[I]n 'the ordinary case,' seizures of personal property are 'unreasonable within the meaning of the Fourth Amendment,' without more, 'unless . . . accomplished pursuant to a judicial warrant,' issued by a neutral magistrate after finding probable cause." (omission in original) (quoting *United States v. Place*, 462 U.S. 696, 701 (1983))); *Riley*, 573 U.S. at 382 ("Our cases have determined that '[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing . . . reasonableness generally requires the obtaining of a judicial warrant.'" (alteration and omission in original) (quoting *Vernonia Sch. Dist.*, 515 U.S. at 653)). "The presence of a search warrant serves a high function," that goes beyond a finding of particularity and probable cause. *McDonald v. United States*, 335 U.S. 451, 455 (1948). "[T]he Fourth Amendment has interposed a magistrate between the citizen and the police . . . so that an objective mind might weigh the need to invade that privacy in order to enforce the law." *Id*. Thus, the Supreme Court has held that the absence of a warrant will not be excused unless law enforcement shows that bypassing this constitutional mandate was "imperative." *Id.* at 456; *see also Smith*, 967 F.3d at

205 (noting that "[t]he Supreme Court . . . has never 'held unlawful a temporary seizure that was supported by probable cause and was designed to prevent the loss of evidence *while the police diligently obtained a warrant in a reasonable period of time*'" (emphasis in original) (quoting *McArthur*, 531 U.S. at 334)).

The unreasonable delay cases stand as assurance that law enforcement must adequately justify their intrusions on an individual's privacy and possessory interests without the protection of a warrant. An unreasonable initial seizure—including by excessive delay in obtaining a warrant—cannot be cured by the later securing of a warrant because the government's actions have already violated the Fourth Amendment. If, however, the initial warrantless seizure is reasonable and the government subsequently obtains a valid warrant in a reasonable time period to conduct a search, the government, under the Fourth Amendment, has satisfactorily justified its interest in retaining an individual's property over any possessory or privacy interests a property owner might raise.

As the government aptly points out, this unreasonable delay line of caselaw is inapposite to the factual circumstances here, where the government's initial seizure of the Target Devices has not been challenged and the government has already searched, seized, and retained evidence pursuant to a validly issued search warrant. Gov't's Mot. at 26–29. Put another way, in the unreasonable delay cases, the issue is that the government has held onto seized property without a neutral magistrate assessing the reasonableness of the seizure, whereas here the seized property has already been found by a neutral magistrate to be both lawfully seized and lawfully extracted and searched under a valid warrant. This key factual distinction makes all the difference under the Fourth Amendment.[4]

[4] This is not to say that consideration of the timing and location of the property to be searched finds no anchor in Fourth Amendment jurisprudence outside the context of delays in seeking warrants post-seizure, but only to the

The magistrate judge's decision to conduct a Fourth Amendment reasonableness inquiry into the government's interest in retaining copies of the lawfully seized digital data versus its owner's ongoing possessory interest prior to the issuance of a warrant finds no support in binding circuit precedent. *See United States v. Hubbard*, 650 F.2d 293, 302–03 (D.C. Cir. 1980) (refusing to ground an owner's protectible interests in lawfully seized items "in the Constitution's provisions" but mandating "some procedural mechanism by which those interests can be presented contemporaneously to [a] court" under the court's supervisory powers). Indeed, the majority of circuits to consider the issue have held that "[e]valuating the legitimacy of [law enforcement's] interests [in retaining lawfully seized property] and weighing them against an individual's competing interest in *regaining* his property *is not, and never has been*, a concern of the Fourth Amendment," even when the underlying investigation or prosecution has been completed. *Lee v. City of Chicago*, 330 F.3d 456, 465 (7th Cir. 2003) (emphasis added); *id.* ("[A] government's decision regarding how and when to return once lawfully obtained property

---

extent that both factors affect the probable cause and particularity requirements for a warrant. Thus, for example, probable cause might dissipate or become stale if the item to be searched is perishable, easily transferable, or not typically maintained over long periods of time or if the specified location is unreliable or shifts due to the nature of the criminal activity under investigation. *See United States v. Matthews*, 753 F.3d 1321, 1324 (D.C. Cir. 2014) ("The likelihood that the evidence sought is still in place is a function not simply of watch and calendar but of variables . . . [such as]: the character of the crime . . ., of the criminal . . ., of the thing to be seized (perishable and easily transferable or of enduring utility to its holder?), of the place to be searched (mere criminal forum of convenience or secure operational base?), etc." (quoting *United States v. Bruner*, 657 F.2d 1278, 1298 (D.C. Cir. 1981))); *United States v. Scurry*, 821 F.3d 1, 15 (D.C. Cir. 2016) ("[T]o satisfy the search component of the particularity requirement, a warrant must enable the executing officer to locate and identify the place to be searched and ensure — to a reasonable probability — that the officer will not mistakenly search the wrong place."). Courts, however, have routinely held that such timing and location concerns are not implicated "[w]here the records or documents in question are digital," *United States v. Ali*, 870 F. Supp. 2d 10, 33–34 (D.D.C. 2012), because ESI does not "rapidly dissipate[] or degrade[]" and "can be retained almost indefinitely," *United States v. Vosburgh*, 602 F.3d 512, 529 (3d Cir. 2010). Consequently, the location of the digital evidence or the delay between the initial criminal activity and when the digital evidence is to be searched rarely, if ever, affects the likelihood of whether the digital records may still contain evidence of the offense specified in the warrant. Accordingly, as the magistrate judge determined, and this Court concluded, the probable cause determination is not affected by the location of the digital evidence or the timing of the investigation at issue in this case.

'raises different issues, which the text, history, and judicial interpretations of the Fourth Amendment do not illuminate.'" (quoting *Wilkins v. May*, 872 F.2d 190, 194 (7th Cir. 1989))); *Shaul v. Cherry Valley-Springfield Cent. Sch. Dist.*, 363 F.3d 177, 187 (2d Cir. 2004) ("Where, as in this case, an initial seizure of property was reasonable, [the government's] failure to return the items does not, by itself, state a separate Fourth Amendment claim of unreasonable seizure . . . . To the extent the Constitution affords [an owner] any right with respect to a government agency's retention of lawfully seized property, it would appear to be procedural due process."); *Case v. Eslinger*, 555 F.3d 1317, 1330–31 (11th Cir. 2009) (same); *Denault v. Ahern*, 857 F.3d 76, 83–84 (1st Cir. 2017) (same); *Fox v. Van Oosterum*, 176 F.3d 342, 349–52 (6th Cir. 1999) (same); *see also* FED. RED. CRIM P. 41(g) advisory committee notes to 1989 amendments (noting that "[a]s long as the government has a law enforcement purpose in copying records, there is no reason why it should be saddled with a heavy burden of justifying the copying" although "[i]n some circumstances . . . *equitable* considerations might justify an order requiring the government to return or destroy all copies of records that it has seized" (emphasis added)); *cf. Springer v. Albin*, 398 F. App'x 427, 433–34 (10th Cir. 2010) (declining to decide whether the alleged theft by law enforcement of currency seized during the execution of a valid search warrant violated the Fourth Amendment); *but see Mom's Inc. v. Willman*, 109 F. App'x 629, 636–37 (4th Cir. 2004) (per curiam) (holding the government's failure to return a watch seized pursuant to a valid search warrant and then stolen by a police officer constituted an unreasonable seizure "beyond its lawful duration," which violated the Fourth Amendment).[5]

[5] Certainly, statutory or regulatory regimes may constrain the government's retention of lawfully seized evidence. *See e.g.*, 18 U.S.C. § 2518(8)(a) (requiring retention of intercepted wire, oral, or electronic communications authorized under this chapter "for ten years"); *United States v. Jacobetz*, 955 F.2d 786, 802 (2d Cir. 1992) (noting that the government's failure to return lawfully obtained property might violate an owner's *statutory* right under state law but did not constitute a *constitutional* violation); U.S. Dep't Just., Just. Manual §§ 9-14.000–14.009 (setting out the Department of Justice's retention policies for evidence in closed prosecutions). The courts,

In so holding, the Court does not suggest that the government may indefinitely retain lawfully seized items once a prosecution or investigation has ended without *any* justification. *See, e.g.*, *Lee*, 330 F.3d at 466 ("It is axiomatic that property once seized, but no longer needed, should at some point be returned to its rightful owner. Equitable principles would dictate as much." (citation omitted)). Indeed, the Federal Rules of Criminal Procedure provide a statutory mechanism through which an owner may seek the return of lawfully seized and retained property. *See* FED. RED. CRIM P. 41(g) advisory committee notes to 1989 amendments ("[A] person whose property has been lawfully seized may seek return of property when aggrieved by the government's continued possession of it."). Instead, as several of the circuits have held, judicial scrutiny of law enforcement's retention policies for evidence seized lawfully pursuant to a search warrant simply falls outside the purview of the Fourth Amendment.

Here, the initial search warrants for Target Devices 16–19 authorized "the copying and extraction" of the devices' digital data, Gov't's Mot. at 7, and the government has asserted the Department of Justice's evidence retention policy as the basis for its continued retention of the copies, *see id.* at 8–9. Accordingly, the government's retention of copies of the digital data lawfully extracted from Target Devices 16–19 does not affect the reasonableness of any subsequent search of such data.

3. *Concerns about "Overseizure" of ESI Are Adequately Addressed by the Warrant Requirements*

Third and relatedly, the type of evidence that the government seeks to search—ESI derived from an extraction of a cell phone—does not by itself trigger the need for any additional protections prior to the issuance of a warrant. As the magistrate judge noted, several courts, *in*

however, have reasonably refused to enlist the Fourth Amendment to serve as the constitutional guardian of such concerns.

dicta, have expressed concern about the government's retention of ESI because the practicalities of searching for ESI often lead to "overseizure" during the execution of a search warrant, allowing the government to seize and retain evidence beyond the scope of the initial warrant. *See Redacted MJ Decision*, 2021 WL 5822583, at *5–6, *17 n.10; *see also United States v. Schesso*, 730 F.3d 1040, 1042 (9th Cir. 2013) (noting "searches of electronic records" inherently raise a risk of overseizing data "[b]ecause electronic devices contain vast quantities of intermingled information"). Courts have characterized this concern as a fear that "[i]f the Government could seize and retain non-responsive electronic records indefinitely, so it could search them whenever it later developed probable cause, every warrant to search for particular electronic data would become in essence, a general warrant," which the Fourth Amendment's protections were fashioned expressly to preclude. *United States v. Ganias*, 755 F.3d 125, 139–40 (2d Cir. 2014), *rev. en banc*, 824 F.3d 199 (2d Cir. 2016) (citing *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1171 (9th Cir. 2010) (en banc)). In response, several courts, like the magistrate judge here, have attempted to set restrictions on what can be done with copies of ESI extracted from cell phones and other electronic storage media. *See id.* at 137–40 (holding the Fourth Amendment prohibited the government's retention and use of a mirror image of a hard drive created pursuant to a valid search warrant, where the copy contained responsive and non-responsive files and the government secured a subsequent search warrant to query both the responsive and non-responsive files); *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1178–80 (Kozinski, C.J., concurring) (proposing several restrictions on the execution of search warrants for ESI, including a requirement that the government must destroy, or return all copies of non-responsive data).[6]

[6] Notably, *Ganias* and former Chief Judge Kozinski's concurrence in *Comprehensive Drug Testing* are the only two circuit decisions to ever propose such restrictions, and no other circuit has yet to adopt these search

To the extent the "overseizure" of ESI in executing warrants on digital devices raises Fourth Amendment privacy concerns, the Supreme Court and Congress, in amending Rule 41, already signaled their understanding that in order adequately to conduct a search and seizure of ESI, the government is authorized to copy and retain ESI from the seized electronic storage medium, which will inevitably include non-responsive data. *See* FED. R. CRIM. P. 41(e)(B) (permitting a warrant to "authorize the seizure of electronic storage media or the seizure or copying of electronically stored information" in order for law enforcement to conduct "a later review of the media or information consistent with the warrant"); *id.* 41(f)(1)(B) (noting that "[i]n a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information . . . the officer may retain a copy of the electronically stored information that was seized or copied"). In short, Rule 41 recognizes that data stored in cell phones or other electronic storage media is a cohesive unit, in which responsive and non-responsive data are intermingled, and likely must be preserved in its entirety to be forensically sound. *See also Ganias*, 824 F.3d at 215 ("[T]he extraction of specific data files to some other medium can alter, omit, or even destroy portions of the information contained in the original storage medium. Preservation of the original medium or a complete mirror may therefore be necessary in order to safeguard the integrity of evidence that has been lawfully obtained or to

protocols or restrictions on retained copies of ESI. In fact, the Second Circuit's position in the original *Ganias* panel decision was not adopted by the full en banc court, *see United States v. Ganias*, 824 F.3d 199, 200 (2d Cir. 2016) (en banc) (declining to decide whether the retention of the forensic mirrors violated the Fourth Amendment and instead finding law enforcement's subsequent search of the retained mirrors pursuant to a second search warrant was objectively reasonable and thus not subject to suppression), and the Ninth Circuit, although initially having Chief Judge Kozinki's opinion serve as the majority opinion, subsequently reissued its decision and moved his guidance to a non-binding concurrence, *compare United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (en banc), *with United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010) (en banc). In short, these concerns have not gained much traction. *See Tlapanco v. Elges*, 969 F.3d 638, 657 (6th Cir. 2020) (noting that no circuit has held the government's practice of retaining forensic mirrors of electronic files unlawful under the Fourth Amendment).

authenticate it at trial."); *id.* ("Retention of the original storage medium or its mirror may also be necessary to afford criminal defendants access to that medium or its forensic copy so that, relying on forensic experts of their own, they may challenge the authenticity or reliability of evidence allegedly retrieved."); *see also United States v. Aboshady*, 951 F.3d 1, 6–8 (1st Cir. 2020) (rejecting an overbreadth challenge to government's retention of a copy of all the ESI stored in defendant's email account until defendant's criminal appeals were completed because "[n]othing . . . in the warrant . . . set[] forth a time limit on the retention of the data that [the warrant] plainly authorized the government to acquire" and it was reasonable "to interpret the warrant to permit the government to retain that data until the appeals [were] completed").

Once seized and copied, the Fourth Amendment's particularity requirement kicks in, restricting the scope of the search and the government's use of the data in a criminal proceeding only to the data particularly described in the warrant as evidence of the target offenses. Although a significant amount of information is seized, the particularity requirement, as it always has, bars the government from conducting a general unrestricted rummaging through the immense trove of information stored on the electronic device.

To be sure, the reasonableness requirement of the Fourth Amendment may come into play in the manner of execution of a warrant, but that overlay of reasonableness has been restricted to ensuring strict adherence to the warrant's particularity terms. As the D. C. Circuit has explained: "[o]f course, even when the search warrant meets both the probable cause and particularity requirements, the search itself must be conducted in a reasonable manner, appropriately limited to the scope and intensity called for by the warrant." *Heldt*, 668 F.2d at 1256 (citing *Terry v. Ohio*, 392 U.S. 1, 17–18 (1968) ("This Court has held in the past that a search which is reasonable at its inception may violate the Fourth Amendment by virtue of

its intolerable intensity and scope.")). This is because "[w]hen investigators fail to limit themselves to the particulars in the warrant, both the particularity requirement and the probable cause requirement are drained of all significance as restraining mechanisms, and the warrant limitation becomes a practical nullity," and, thus, "[o]bedience to the particularity requirement both in drafting and executing a search warrant is therefore essential to protect against the centuries-old fear of general searches and seizures." *Id.* at 1257.[7]

The manner of execution of the warrant therefore may require, for example, special training of law enforcement agents conducting a search to segregate targeted relevant records from innocuous ones in a large data collection, *see, e.g.*, *id.* at 1261 (cautioning that "proper execution of a search warrant for numerous documents requires . . . adequate preparation"), or a privilege review team to segregate privileged information from seizure if the location of the search is reasonably believed to contain such information outside the legitimate purview of a warrant. Due to the nature of the location to be searched and information particularly targeted by a warrant, the execution of a warrant may, at times, necessarily entail the search (and seizure) of non-responsive information—and that has not been held to be unreasonable, absent "a flagrant disregard for the limitations in a warrant." *Id.* at 1259–60 (finding document search to be reasonable, despite seizure of some documents outside the warrant's scope, since "[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized"); *see also, e.g.*, 18 U.S.C. § 2518(5) (authorizing interception, under statutory requirements, of oral,

[7] These conclusions comport with settled Fourth Amendment caselaw, which, rather than prohibiting warrants based on the nature or location of the items to be searched or imposing additional requirements to protect privacy or other constitutionally-protected interests, has required only "that the courts apply the warrant requirements with particular exactitude when [certain constitutionally-protected] interests would be endangered by the search." *Zurcher*, 436 U.S. at 565 (holding that searches implicating First Amendment concerns did not call for imposing additional requirements outside of the Fourth Amendment's warrant requirements to issue a warrant).

wire, and electronic communications "in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter," but allowing such minimization to "be accomplished as soon as practicable after such interception" when the communications are "in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period"). Ensuring that a search is reasonably executed within the strict bounds of the warrant's terms is generally a judicial task on review of a suppression motion, rather than an *ex ante* consideration injecting judicial management on law enforcement's execution and subsequent handling of any information or items seized and retained as a result of the search. *See Dalia v. United States*, 441 U.S. 238, 257 (1979) ("[I]t is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant . . . ."); *United States v. Burgess*, 576 F.3d 1078, 1092–94 (10th Cir. 2009) (explaining the rationale for the court's reluctance to "limit computer searches" in advance); *see also United States v. Khanani*, 502 F.3d 1281, 1290–91 (11th Cir. 2007) (holding that a warrant's "lack of a written 'search protocol'" did not render a search for digital evidence unreasonable where the protocols utilized by the government in executing the warrant reasonably cabined the search to the warrant's scope).

Ultimately, the inherent risk of overseizure in the digital context does not present obstacles that the Fourth Amendment has not been called on to address before. Courts have recognized the certain searches, like document searches, eavesdropping and bugging searches, and now ESI searches, "tend to involve broad disclosures of the intimacies of private lives, thoughts, and transactions" presenting "acute constitutional hazards." *Heldt*, 668 F.2d at 1260 (citing *Andersen v. Maryland*, 427 U.S. 463, 482 n.11 (1976)). Nonetheless, searches of this

nature have never been held impermissible. Instead, they demand "a heightened sensitivity to the particularity requirement," coextensive with the heightened degree of intrusiveness that may result from the search. *United States v. Galpin*, 720 F.3d 436 at 446–47 (2d Cir. 2013). The Fourth Amendment asks only that a magistrate judge, in issuing a warrant, consider that heightened sensitivity and that judges, in their *ex post* review of the search warrant and its execution, do the same. Thus, where the government has lawfully obtained a copy of ESI pursuant to a search warrant and retained such a copy for law enforcement purposes, the Fourth Amendment presents no obstacle to the issuance of a search warrant authorizing the subsequent search of this lawfully held evidence, so long as the subsequent search satisfactorily meets the warrant requirements.

In sum, not only does the proposed three-pronged reasonableness inquiry add little to the Fourth Amendment's already adequate protections of an individual's privacy and possessory interests, it also stymies legitimate and serious law enforcement interests recognized by the Fourth Amendment. Nothing has been gained, but time, efficacy, and adequate protection of the public's safety has been lost.

Despite the magistrate's legitimate concerns, prior caselaw has already addressed how to set "reasonable limit[s] on the government's power" to "search a mobile device—or data extracted from such a device—that the government has retained for months or years after its seizure as part of an earlier investigation and prosecution." *Redacted MJ Decision*, 2021 WL 5822583, at *5. As the Supreme Court previously instructed in *Riley*, in order for the government to search a cell phone's digital data the government must get a probable cause warrant. It has requested one here. As the body of caselaw governing expanded investigations dictates, once the government's investigation unearths the likelihood that evidence of offenses

not covered by the initial warrant exists, the government must set forth adequate probable cause and particularity to secure a warrant expanding the scope of its search of previously seized evidence. It has done so here. Fourth Amendment jurisprudence has not, to date, required the government to justify retention of evidence lawfully seized pursuant to a valid search warrant before being permitted to execute a new valid search warrant, and this Court rejects such an innovation here.

This is not a case of the government attempting surreptitiously and unrestrictedly to mine an individual's private data or to use a previously issued warrant "to rummage through [cell phones] in an unrestrained search for evidence of criminal activity." *Riley*, 573 U.S. at 403. Nor has the government "seize[d] and indefinitely [held without a warrant] . . . property merely on the Government's word that the property owner is a person of interest in some uncharged, unrelated crime at the time of the seizure." *Wilkins*, 538 F. Supp. 3d at 94. Instead, at all times, from the prior search and seizure, pursuant to a warrant, and continuing to the requested search at issue now, the government has acted within the constraints of the Fourth Amendment. It has now set forth before a neutral magistrate judge its "probable cause to believe 'that the evidence sought will aid in a particular apprehension or conviction' for a particular offense," *Dalia*, 441 U.S. at 255 (quoting *Warden v. Hayden*, 387 U.S. 294, 307 (1967)), and "'particularly describe[d] the "things to be seized,"' as well as the place to be searched," *id.* (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Having meet those three requirements, "[n]othing in the language of the Constitution or in [the Supreme Court's] decisions interpreting [the Warrant requirement of the Fourth Amendment] suggests that" the government must meet additional requirements concerning its justification to retain evidence lawfully seized pursuant to a valid

search warrant. *United States v. Grubbs*, 547 U.S. 90, 98 (2006) (quoting *Dalia*, 441 U.S. at 255). Accordingly, the requested warrant shall issue as to Target Devices 16, 17, 18, and 19.

IV. CONCLUSION AND ORDER

For the reasons stated above, the portion of the magistrate judge's Opinion and Order denying the government's application for search warrant as to Target Devices 16, 17, 18, and 19 is **REVERSED,** and that application is **GRANTED**.

The government is **DIRECTED** to submit an amended warrant application with respect to Target Devices 16, 17, 18, and 19.

Further, the government is **DIRECTED** to review this Memorandum Opinion and Order, and other filings on the Court's docket in this matter, and advise which filings may be unsealed, in whole or in part, with proposed redactions as necessary to protect any ongoing criminal investigations, by March 24, 2022, unless these filings have been unsealed before then.

SO ORDERED.

Date: March 14, 2022

BERYL A. HOWELL
Chief Judge