brownrudnick

MICHAEL J. BOWE
MBowe@brownrudnick.com

E. PATRICK GILMAN
PGilman@brownrudnick.com

September 13, 2021

BY EMAIL/ECF

The Honorable J. Paul Oetken
United States District Judge
Southern District of New York
Thurgood Marshall U.S. Courthouse
40 Foley Square
New York, New York 10007

RE: *In re Search Warrant dated April 28, 2021*, 21-MC-425 (JPO)

Dear Judge Oetken:

Victoria Toensing, through counsel, writes in reply to the Government's September 3, 2021 letter (the "Letter") concerning the Special Master review process and temporal limitations of the above referenced search warrant (the "Warrant"). The Government has persistently sought to push the bounds of reasonableness under the Fourth Amendment. To make matters worse, it has now become apparent from discussions with the Government that it badly bungled the data collection process and is seeking an unlimited review of all electronic data on Ms. Toensing's phone because the Government corrupted the metadata from which the typical date range searches are regularly conducted in federal courts across the country. Rather than inform the Court of this significant data collection/management blunder and commit to fix it, the Government attempts to mask it behind a self-righteous canard that it is graciously offering to compromise even though it (incorrectly) claims that it is entitled to review all the data collected from Ms. Toensing's phone. The Government has no such right. Its attempt to do so is Unconstitutional. And that Constitutional limitation is not excused simply because the Government's own errors now make it impossible or more difficult to conduct a Constitutional search.

A. The Fourth Amendment's particularity requirement limits which files are eligible for review.

To be clear, Ms. Toensing has not claimed, and is not now claiming, that the Government's seizure of her iPhone was Unconstitutional. To be sure, Ms. Toensing questions the basis of probable cause, but reserves that argument for another day. However, how her iPhone is searched and what is searched pursuant to the Warrant is fully at issue today.

"The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one 'particularly describing the place to be searched and the persons or things to be seized.'" *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (quoting U.S. Const. amend. IV) ("Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase." (*id.* at 84–85 (citation omitted))). For instance, "[p]robable cause to

believe that a container placed in the trunk of a taxi contains contraband or evidence does not justify a search of the entire cab." *United States v. Ross*, 456 U.S. 798, 824 (1982). Thus, reasonable limitations on how and what the Government may search serves "[t]he manifest purpose of this particularity requirement"—"to prevent general searches." *Garrison*, 480 U.S. at 84.

Broadly speaking, the April 22, 2021 seizure warrant described the iPhone which the Government seized, and the April 28, 2021 Warrant defines the scope of what may be permissibly searched. *See In re 650 Fifth Ave. & Related Properties*, 934 F.3d 147, 163 (2d Cir. 2019) (a "warrant is facially deficient" without "a temporal scope for the items to be seized"); *see also United States v. Hanna*, 661 F.3d 271, 286 (6th Cir. 2011) (upholding a search because the Government's review of electronic files complied with "'temporal limits,' 'subject matter limits,' and 'categorical limits' on the items that could be searched and seized"). What the Government did not do, and has not done, however, is establish with any particularity how it intended to cull data that falls outside the temporal and content scopes of the Warrant *See generally Matter of the Search of Apple iPhone, IMEI 013888003738427*, 31 F. Supp. 3d 159, 166 (D.D.C. 2014) (Imaging devices create "a complete copy of all its data—including the data for which there is no probable cause to seize—that must be accounted for and which ultimately must be purged of data outside the scope of the warrant."). As a practical matter, counsel cannot imagine that an image would not be created, so the Government must clarify this aspect and make clear in its applications that the non-relevant data will be deleted from any system images.").

Every day in prosecutions and litigations across this country, parties effectively identify and review electronic data based on temporal and relevant search protocols, often dictated by the courts. The Government has these same capabilities. *Id.* at 167 (Indeed, the "digital world . . . is entirely different" because "search tools exist [that] allow the [G]overnment to find specific data without having to examine every file on a hard drive or flash drive.").[1] Because the data responsive to the Warrant can readily be identified, the Government is Constitutionally required to do so. *Id.* (requiring the Government to "explain to the Court how the [G]overnment intends to determine where it will search (which 'parts'—or blocks—of the iPhone's NAND flash drive)").

To ensure it does so Constitutionally requires transparency and the application of now well-established processes—including, an identified search protocol—*i.e.* "an explanation of the scientific methodology the [G]overnment will use to separate what is permitted to be seized from what is not," which necessarily limits "where it is going to search." *Id.* at 166. The protocol must further explain "how those decisions with respect to how the search will be conducted will help limit the possibility that locations containing data outside the scope of the warrant will be searched." *Id.* at 167. Otherwise, the Government's intentional and wholesale review of areas or files that fall outside the scope of the Warrant violates the Fourth Amendment.[2] *See United States v. Sears*, 411 F.3d 1124, 1131 (9th Cir. 2005) (The

[1] In fact, an iPhone's memory "could allow storage of up to around two million text documents." *Matter of the Search of Apple iPhone, IMEI 013888003738427*, 31 F. Supp. 3d at 166 (referencing an iPhone 4 with even less storage capacity than Ms. Toensing's iPhone 7). So, "it is inconceivable that the [G]overnment would go file by file to determine whether each one is within the scope of the warrant." *Id.* To that end, "[w]hen searching electronic devices to seize the data, the potential for abuse has never been greater: it is easy to copy them and store thousands or millions of documents with relative ease." *Id.* at 167 (requiring the Government to use "search tools . . . so that they are more likely to find only the material within the scope of the warrant").

[2] Courts routinely confine the review of seized files to those falling within the temporal limitations of a warrant. *See, e.g., United States v. Evaschuck*, 65 F. Supp. 2d 1360, 1365 (M.D. Fla. 1999) (granting a motion to suppress because the "search and seizure of logbooks containing only documents that were beyond the scope of the search

Fourth Amendment forbids the Government from "transform[ing] the search into an impermissible general search by ignoring the terms of the warrant and engaging in indiscriminate fishing").

B. The Government, not Respondents, conflated relevance and privilege.

Contrary to the Government's assertion, Ms. Toensing's August 30, 2021 letter and Rudolph Giuliani's August 27, 2021 letter do not conflate the privilege and relevance issues under the Warrant. The Government conflated these issues when it requested and secured a Special Master and now wants that Special Master to review all data seized for privilege regardless of its date or subject matter. By definition, this position means the Government intends to review all data seized even if it is unquestionably outside the temporal and subject scope of the Warrant or not clearly within that scope. The Government rationalizes this position as one taken for "the sake of efficiency," but nothing could be less efficient because it necessarily entails multiple participants reviewing wholesale vast amounts of data that easily could be culled as temporally non-responsive or apparently not temporally responsive. *See* Letter at 1. Those documents are by definition not relevant either, but, in addition, the Government's position would create the same inefficiencies with respect to dates within the date range because its proposal would necessarily entail multiple reviews of even temporally responsive data that nevertheless plainly are not relevant to the Warrant's enumerated subject matter scope.

C. The Government's Data Mismanagement Is Not a License to Avoid the Constitution.

While the Government represents to the Court that its proposal is grounded in efficiency and a gracious effort to compromise, what it has not disclosed is that, as a practical matter, a proper process to identify all relevant data is no longer possible because the Government mismanaged and corrupted the data it seized. For example, thousands of Ms. Toensing's files the Government provided for this purported review now contain associated metadata with a date stamp in July 2021. *See* Letter at 2 (acknowledging that "the Special Master has informed the parties that over 25,000 emails, text messages, chats, and voicemails have timestamps in July 2021" from Mr. Giuliani's and Ms. Toensing's files). Yet, the phone was seized in April 2021. Moreover, these files no longer contain the original metadata indicating when they were created, edited, or otherwise acted upon. Beyond rendering these files inauthentic by definition, this corruption is an undisclosed (and perhaps the only) reason the Government now claims that the review of files with dates outside the scope of the Warrant may be "necessary" if the electronic date stamps fail to reflect the true date a file was created, modified, or deleted. *See id.* at 2 (claiming that "the Government cannot rely on automated time stamping to identify temporally responsive documents, because such timestamps can often err."). It is neither candid nor genuine for the Government to make this claim without

---

warrant was not reasonably required to locate the items described in the search warrant"); *see also United States v. Nordlicht*, No. 16-CR-00640 (BMC), 2018 WL 705548, at *8 (E.D.N.Y. Feb. 2, 2018) (placing the Government "on notice that when it collects a business's electronic data, it must execute the warrant by setting aside any materials not within the scope of the warrant within a reasonable time following the seizure").

Likewise, the Government routinely agrees to filter out documents that fall outside the temporal limitations of a warrant. *See, e.g.*, *United States v. Wilson*, No. CR 19-10080-NMG-17, 2020 WL 6945939, at *5 (D. Mass. Nov. 25, 2020) ("First, the U.S. Attorney's Office had its Technology Support Team filter out any 'user-generated data stored' from [the defendant's] email account that fell outside of the identified date range"); *United States v. Taylor*, No. 17-CR-00191-JST-1, 2019 WL 281457, at *3 (N.D. Cal. Jan. 22, 2019) (the Government agreed that it would "not use, and will delete" all "emails dated prior to the date restriction in the Search Warrant" because "these documents [were] outside the scope of the search warrant"); *United States v. Lustyik*, 57 F. Supp. 3d 213, 219 (S.D.N.Y. 2014) (reviewers specifically excluded "emails that were removed from the Relativity database either because they were privileged or fell outside the Warrant's date range").

disclosing its role in the problem and then use that problem as the justification for the wholesale review of all data seized irrespective of temporal or subject matter limitations.

The Government created the situation in which it now finds itself. The only reasonable explanation for how mountains of data show creation dates that post-date when the Government seized Ms. Toensing's device—and indeed Mr. Giuliani's device as well—is that the Government bungled the collection, retrieval, and management process. The Government can blame no one but itself (and its chosen vendor) for any alleged errors. Despite requests from Ms. Toensing's counsel, the Government has yet to provide an explanation as to what happened to the data or how pervasive is the problem.

Instead, it represented to the Court only that the July 2021 metadata date possibly "reflects a 'last modified' date based on when the Government's vendor extracted the data from the searched devices." *See* Letter at 2. This possibility is no answer at all and, even if true, ignores the indisputable fact that these files would only contain a new "modified" date if they, in fact, had been modified. As a minimum threshold condition of proceeding further in this process, the Government must be required to provide a complete and candid account of what happened to the seized files.

Regardless of that answer, however, the Government's corruption of the data cannot be used as a basis for avoiding the location and identification of data that is temporally and subjectively within the scope of the Warrant and limiting the review to that data. The law does not permit the Government to gain access to a trove of data, to which it is otherwise not entitled, simply because the Government's own collection and processing was problematic. *See United States v. Morgan*, 493 F. Supp. 3d 171, 200 (W.D.N.Y. 2020) (finding that "an evidentiary hearing was needed to resolve factual disputes concerning whether the [G]overnment's electronic productions complied with the [document production protocol]" due to corrupted metadata, including questions concerning when the defendant sent electronic messages seized by the Government).

D. The Government's proposed January 1, 2018 cutoff date is arbitrary and capricious.

Moreover, the Government proposes that data pre-dating "January 1, 2018 should thus simply be put aside, and not reviewed by the Special Master or the Government." Letter at 4. However, the Government fails to justify its arbitrary selection of the proposed January 2018 cutoff date. What makes January 2018 any different from July 2018 or December 2018? Rather, the temporal limitations that the Government requested when it obtained the Warrant to search through files contained on Ms. Toensing's device are from January 2019 to December 2019. Search Warrant, 21 Mag. 4591. The Fourth Amendment does not allow executive agents to review files other than those which fall within the specifically delineated scope of the Warrant, either ***before or after*** those dates. *See supra* Part A.

Ms. Toensing trusts that the Special Master is capable of making a determination regarding the relevance of files under the temporal limitations imposed by the Warrant, along with her determination of whether those documents are privileged. If any disagreements arise concerning whether a specific document or file falls within the temporal scope of the Warrant, like the privilege review, Ms. Toensing's counsel is happy to discuss and provide those documents as required under the Warrant. The Fourth Amendment requires nothing more and nothing less.[3]

[3] The only two cases the Government cites purportedly in support of its Fourth Amendment position regarding the review of files outside the scope of the Warrant are entirely inapposite. The first challenged the probable cause determination behind a warrant—as the Court's previous rulings have made clear, an issue not yet ripe in this

Respectfully submitted,

BROWN RUDNICK LLP

Michael J. Bowe
E. Patrick Gilman

Cc: Honorable Barbara Jones (Retired), Special Master (Bracewell LLP)
Audrey Strauss, Esq. (United States Attorney for the Southern District of New York)
Rebekah Donaleski, Esq. (Assistant United States Attorney)
Nicolas Roos, Esq. (Assistant United States Attorney)
Aline Flodr (Assistant United States Attorney)

---

matter—which permitted the Government to search all files on a seized cell phone that fell *within* the scope of the warrant. Letter at 2 (citing *United States v. Gatto*, 313 F. Supp. 3d 551, 561 (S.D.N.Y. 2018) (rejecting an *alternative* argument regarding the overbreadth of a warrant that expressly permitted the Government "to examine *all* of the seized data to evaluate its contents and determine whether the data is responsive to the warrant" without imposing any temporal limitation in the warrant (emphasis added))). That decision specifically noted that "[h]ere, in particular, it would have been difficult for the search warrants to specify *ex ante* those areas of data in which law enforcement was likely to find evidence responsive to the warrants because, among other reasons, it was not clear in advance whether the government would be able to sort through the various data categories in some automatic or mechanical way." *Gatto*, 313 F. Supp. 3d at 561. That is not the case here where the Government could easily, mechanically filter out unresponsive files by date in accordance with the Warrant, which provides a clear temporal scope. *See Matter of the Search of Apple iPhone, IMEI 013888003738427*, 31 F. Supp. 3d at 166.

Second, the Government attempts to rely upon a case that specifically declined to decide the substantive Fourth Amendment question concerning whether the Government violated the Fourth Amendment by retaining a person's full hard drive when the original warrant authorized the Government's search of something less. Letter at 3 (citing *United States v. Ganias*, 824 F.3d 199, 200 (2d Cir. 2016) ("[W]e need not and do not decide whether the Government violated the Fourth Amendment" by retaining the full hard drives obtained pursuant to a warrant authorizes the search of only certain types of files)). Even so, the Second Circuit expressed concerns surrounding the retention of wide-ranging data. *See Ganias*, 824 F.3d at 219 ("Since we resolve this case on other grounds, we need not address whether [the defendant's] failure to make such a motion forfeited any Fourth Amendment objection he might otherwise have had to the Government's retention of the mirrors," but "we agree with the district court that, as a pragmatic matter, such a motion would have given a court the opportunity to consider whether the government's interest could be served by an alternative to retaining the property, and perhaps to order the mirrors returned to [the defendant]"). Similar concerns regarding the Government's access to files it is not authorized to review weigh in favor of enforcing the temporal limitations at issue today, without any review of files outside the scope of the Warrant by any executive agent.