

Ashwin J. Ram (SBN 227513)
aram@steptoe.com
Michael A. Keough (SBN 327037)
mkeough@steptoe.com
Meghan L. Newcomer (*pro hac vice*)
mnewcomer@steptoe.com
Nicholas P. Silverman (*pro hac vice*)
nsilverman@steptoe.com
STEPTOE & JOHNSON LLP
633 West Fifth Street, Suite 1900
Los Angeles, CA 90071
Telephone: (213) 439-9400
Facsimile: (213) 439-9599

Counsel for Defendant Richard Ayvazyan

Fred G. Minassian (SBN 170974)
fgminassian@yahoo.com
**LAW OFFICES OF FRED G.
MINASSIAN, INC.**
101 N. Brand Ave, Suite 1970
Glendale, CA 91203
Telephone: (818) 240-2444

Counsel for Defendant Tamara Dadyan

John L. Littrell (SBN 221601)
jlittrell@bklwlaw.com
Ryan V. Fraser (SBN 272196)
rfraser@bklwlaw.com
**BIENERT KATZMAN LITRELL
WILLIAMS, LLP**
601 W. 5th Street, Suite 720
Los Angeles, CA 90071
Telephone: (213) 528-3400
Facsimile: (949) 369-3701

Counsel for Defendant Marietta Terabelian

Thomas A. Mesereau Jr. (SBN 91182)
mesereau@mesereaulaw.com
MESEREAU LAW GROUP, P.C.
10100 Santa Monica Blvd., Suite 300
Los Angeles, CA 90067
Telephone: (310) 651-9960

Jennifer J. Wirsching (SBN 263141)
wirschinglaw@outlook.com
ATTORNEY AT LAW
1935 Alpha Rd, Suite 216
Glendale, CA 91208
Telephone: (424) 902-9280

Counsel for Defendant Artur Ayvazyan

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

UNITED STATES OF AMERICA,

Plaintiff,

v.

RICHARD AYVAZYAN,
MARIETTA TERABELIAN,
ARTUR AYVAZYAN,
TAMARA DADYAN,

Defendants.

Case No. 20-cr-579 (SVW)

**JOINT NOTICE OF MOTION AND
MOTION TO EXCLUDE DIGITAL
DEVICE FILES FROM DEVICES
OBTAINED ON NOVEMBER 5,
2020**

Hon. Stephen V. Wilson

Current Hearing Date: June 21, 2021
Requested Hearing Date: June 14, 2021
Time: 11:00 a.m.

NOTICE OF MOTION TO SUPPRESS ELECTRONIC FILES

TO THE COURT, ALL PARTIES, AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on Monday, June 14, 2021; Monday, June 21, 2021; or as soon as this counsel may be heard in Courtroom 10A of this Court at 350 W. 1st Street, 10th Floor, Los Angeles, CA 90012, Defendants Richard Ayvazyan, Marietta Terabelian, Artur Ayvazyan, and Tamara Dadyan, through undersigned counsel, will move the Court to exclude the digital device files contained in devices that were obtained on November 5, 2020 and not subject to a timely responsiveness review.

This motion is based on this notice, the accompanying memorandum of points and authorities, the declaration of Ashwin J. Ram in support, any reply that the defendants may make, such other evidence and arguments as may be presented at or prior to the hearing, and all records and files in this action.

Dated: May 24, 2021

Respectfully submitted,

STEPTOE & JOHNSON LLP

/s/ Ashwin J. Ram

Ashwin J. Ram (SBN 227513)

aram@steptoe.com

Michael A. Keough (SBN 327037)

mkeough@steptoe.com

Meghan L. Newcomer (*pro hac vice*)

mnewcomer@steptoe.com

Nicholas P. Silverman (*pro hac vice*)

nsilverman@steptoe.com

STEPTOE & JOHNSON LLP

633 West Fifth Street, Suite 1900

Los Angeles, CA 90071

Telephone: (213) 439-9400

Facsimile: (213) 439-9599

Counsel for Defendant Richard Ayvazyan

/s/ John L. Littrell

John L. Littrell (SBN 221601)

jlittrell@bklwlaw.com

Ryan V. Fraser (SBN 272196)

rfraser@bklwlaw.com

BIENERT KATZMAN LITRELL

WILLIAMS, LLP

601 W. 5th Street, Suite 720

Los Angeles, CA 90071

Telephone: (213) 528-3400

Facsimile: (949) 369-3701

Counsel for Defendant Marietta Terabelian

/s/ Thomas A. Mesereau

Thomas A. Mesereau Jr. (SBN 91182)

mesereau@mesereaulaw.com

MESEREAU LAW GROUP, P.C.

10100 Santa Monica Blvd., Suite 300

Los Angeles, CA 90067

Telephone: (310) 651-9960

Jennifer J. Wirsching (SBN 263141)

wirschinglaw@outlook.com

ATTORNEY AT LAW

1935 Alpha Rd, Suite 216

Glendale, CA 91208

Telephone: (424) 902-9280

Counsel for Defendant Artur Ayvazyan

/s/ Fred G. Minassian

Fred G. Minassian (SBN 170974)

fgminassian@yahoo.com

LAW OFFICES OF FRED G. MINASSIAN, INC.

101 N. Brand Ave, Suite 1970

Glendale, CA 91203

Telephone: (818) 240-2444

Counsel for Defendant Tamara Dadyan

TABLE OF CONTENTS

I.	LEGAL STANDARD	2
II.	ARGUMENT	3
A.	THE GOVERNMENT’S SEARCH WARRANT EXECUTION VIOLATED THE TERMS OF THE WARRANTS AND THE FOURTH AMENDMENT	4
1.	The Government Failed to Complete a Responsiveness Review as Soon as Practicable and Failed to Secure a Valid Extension	5
2.	The Government Violated the Warrant’s Requirement that the Responsiveness Review Be Conducted By a Law Enforcement Officer Search Team Utilizing Search Protocols	9
B.	THE GOVERNMENT’S SEARCH WARRANT EXECUTION WAS UNREASONABLE BECAUSE IT AMOUNTS TO A GENERAL WARRANT	11
C.	EXCLUSION IS PROPER UNDER RULE 16 AND THE DISCOVERY CUT-OFF ORDER	13
D.	THE ELECTRONIC FILES SHOULD BE EXCLUDED DUE TO <i>KASTIGAR</i> TAIN T INFECTING THE REVIEW PROCESS	16
III.	CONCLUSION	16

TABLE OF AUTHORITIES

	Cases	Page(s)
1		
2		
3		
4	<i>Andresen v. Maryland</i> ,	
5	427 U.S. 463 (1976).....	3
6	<i>In re App'n for Warrant (Cunnius)</i> ,	
7	770 F. Supp. 2d 1138 (W.D. Wash. 2011)	9
8	<i>In re Apple iPhone</i> ,	
9	31 F. Supp. 3d 159 (D.D.C. 2014).....	3, 9, 10
10	<i>Armstrong v. Manzo</i> ,	
11	380 U.S. 545 (1965).....	8
12	<i>Coolidge v. New Hampshire</i> ,	
13	403 U.S. 443 (1971).....	10
14	<i>Entick v. Carrington</i> ,	
15	19 How. St. Tr. 1029 (1765).....	2
16	<i>Franklin v. Foxworth</i> ,	
17	31 F.3d 873 (9th Cir. 1994)	12
18	<i>Go-Bart Importing Co. v. United States</i> ,	
19	282 U.S. 344 (1931).....	3
20	<i>Matthews v. Eldridge</i> ,	
21	424 U.S. 319 (1976).....	8
22	<i>In re Odys Loox Plus Tablet</i> ,	
23	28 F. Supp. 3d 40 (D.D.C. 2014).....	10
24	<i>Payton v. New York</i> ,	
25	445 U.S. 573 (1980).....	3
26	<i>Purbeck v. Wilkinson</i> ,	
27	No. 21-cv-47, 2021 WL 1550563 (D. Idaho Apr. 20, 2021).....	8
28	<i>Riley v. California</i> ,	
	573 U.S. 373 (2014).....	11
	<i>In re Search Warrant</i> ,	
	No. 00-cr-138, 2000 WL 1196327 (D.D.C. July 24, 2000).....	8

1	<i>In re Search Warrants Issued Aug. 29, 1994,</i>	
2	889 F. Supp. 296 (S.D. Ohio 1995)	8
3	<i>Stanford v. State of Texas,</i>	
4	379 U.S. 476 (1965)	2
5	<i>United States v. Adjani,</i>	
6	452 F.3d 1140 (9th Cir. 2006)	12
7	<i>United States v. Bonner,</i>	
8	No. 12-cr-3429, 2013 WL 3829404 (S.D. Cal. July 23, 2013)	10
9	<i>United States v. Bridges,</i>	
10	344 F.3d 1010 (9th Cir. 2003)	3
11	<i>United States v. Comprehensive Drug Testing, Inc.,</i>	
12	621 F.3d 1162 (9th Cir. 2010)	2, 9
13	<i>United States v. Davis,</i>	
14	244 F.3d 666 (8th Cir. 2001)	15
15	<i>United States v. Garcia,</i>	
16	730 F. Supp. 2d 1159 (C.D. Cal. 2010)	14
17	<i>United States v. Garcia,</i>	
18	No. 2:10-cr-595 (C.D. Cal. July 13, 2010)	14
19	<i>United States v. Huntoon,</i>	
20	No. 16-cr-46, 2018 WL 1755788 (D. Ariz. Apr. 12, 2018)	11
21	<i>United States v. Kirschenblatt,</i>	
22	16 F.2d 202 (2d Cir. 1926)	2, 11
23	<i>United States v. Mason,</i>	
24	No. 06-cr-80, 2008 WL 281970 (S.D.N.Y. Jan. 25, 2008)	15
25	<i>United States v. Ornelas,</i>	
26	906 F.3d 1138 (9th Cir. 2018)	14
27	<i>United States v. Ramirez,</i>	
28	523 U.S. 65 (1998)	3
	<i>United States v. Roybal,</i>	
	566 F.2d 1109 (9th Cir. 1977)	14

1	<i>United States v. Sadr,</i>	
2	No. 18-cr-224 (S.D.N.Y. Oct. 10, 2019)	15
3	<i>United States v. Schesso,</i>	
4	730 F.3d 1040 (9th Cir. 2013)	3, 9
5	<i>United States v. Schwartz,</i>	
6	857 F.2d 655 (9th Cir. 1988)	14
7	<i>United States v. Tamura,</i>	
8	694 F.2d 591 (9th Cir. 1982)	2, 12
9	<i>United States v. W.R. Grace,</i>	
10	526 F.3d 499 (9th Cir. 2008)	14
11	Other Authorities	
12	Fed. R. Crim. P. 16(a)(1)(E)	1, 4, 13, 15
13	Fed. R. Crim. P. 41	<i>passim</i>
14	Michael Lesk, How Much Information Is There In the World?,	
15	https://chnm.gmu.edu/digitalhistory/links/pdf/introduction/0.6a.pdf	13

1 **MEMORANDUM OF POINTS AND AUTHORITIES**

2 The government executed broad search warrants at each of the moving
3 defendant's homes on November 5, 2020, choosing to seize dozens of digital devices
4 containing private information. In the last two weeks, the government has disclosed
5 that (1) government agents or attorneys are currently selecting their exhibits from four
6 raw, complete devices belonging to each of the moving defendants, (2) the government
7 did not even begin to review any of these devices¹ for responsiveness until after the
8 Warrant's deadline passed, and (3) the government's only argument for using the
9 totality of defendants' digital lives without a Rule 41 responsiveness review is that it
10 obtained a post-indictment, *ex parte*, sealed extension permitting it to continue
11 reviewing the entire device and seizing files until after trial. There was no justification
12 for the government's four-month delay in beginning a responsiveness review and no
13 need to deprive the defendants of their right to be heard on an extended deprivation of
14 property. The government hid the proceedings from the defendants because it knew
15 that if the presiding judge knew that the discovery cut-off was eleven days away, that
16 trial was two months away, and that the government had failed to diligently execute the
17 warrant, then the presiding judge would not grant an extension at all—much less allow
18 the prosecutors unrestricted access to select trial exhibits from raw digital device data.

19 It simply cannot be the case that the Fourth Amendment's prohibition on general
20 searches is circumvented this easily such that law enforcement can seize massive digital
21 devices and obtain extensions until after a discovery cut-off and after trial that enable it
22 to fish through the entire digital devices for evidence to use against the devices'
23 owners. Were the government's position correct, the exception would consume the rule
24 and functional general searches of digital devices would become permissible.

25
26 ¹ The government provided notice on April 26, 2021 that it intends to use four digital devices, one
27 belonging to each of the moving defendants. The government *did not disclose* that it had not
28 conducted a responsiveness review. Indeed, it is oxymoronic for the government to have decided
which devices it would use *before conducting a responsiveness review* to determine which devices and
files the government could seize.

1 The government's delayed responsiveness review strategy violates the terms of
2 the warrant, the Court's discovery order mandating production of all Rule 16 discovery
3 by March 15, the Fourth Amendment's prohibition on unreasonable execution, and the
4 prohibition of *Kastigar v. United States* and its progeny against using tainted
5 information to interpret evidence or select exhibits. The evidence from each of the
6 digital devices seized on November 5, 2020 should therefore be excluded.

7 **I. LEGAL STANDARD**

8 The Fourth Amendment was enacted to prohibit the equivalent of "general
9 warrants known as writs of assistance," which "had given customs officials blanket
10 authority to search where they pleased for goods imported in violation of the British tax
11 laws." *Stanford v. State of Texas*, 379 U.S. 476, 481 (1965) (unanimous). In *Entick v.*
12 *Carrington*, the "wellspring" of the right now protected by the Fourth Amendment, the
13 court had declared a warrant unlawful because it authorized seizure of "all the party's
14 papers, in the first instance." *Id.* (quoting 19 How. St. Tr. 1029, 1064 (1765)) (noting
15 that the British House of Commons responded by passing a resolution condemning the
16 use of general warrants). Just as *Entick* found a general seizure of books and papers to
17 be unlawful, the Fourth Amendment sought to prohibit such general warrants from
18 being executed in the future. *Stanford*, 379 U.S. at 486 (holding unconstitutional a
19 search warrant that authorized broad seizure of a suspect's books and papers); *see also*
20 *United States v. Kirschenblatt*, 16 F.2d 202, 204 (2d Cir. 1926) (Hand, J.) ("[T]o
21 rummage at will among his papers in search of whatever will convict him, appears to us
22 to be indistinguishable from what might be done under a general warrant.").

23 In tension with the prohibition on general searches is the fact that "over-seizing is
24 an inherent part of the electronic search process." *United States v. Comprehensive*
25 *Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc). The Ninth Circuit
26 has therefore urged judicial officers to exercise "greater vigilance ... in striking the
27 right balance between the government's interest in law enforcement and the right of
28 individuals to be free from unreasonable searches and seizures." *Id.* "In the

1 comparatively rare instances where documents are so intermingled that they cannot
2 feasibly be sorted on site,” officers “may apply for specific authorization for large-scale
3 removal of material, which should be granted by the magistrate issuing the warrant only
4 where on-site sorting is infeasible and no other practical alternative exists.” *United*
5 *States v. Tamura*, 694 F.2d 591, 595-96 (9th Cir. 1982) (noting that the Fourth
6 Amendment requires executing warrants “in a manner that minimizes unwarranted
7 intrusions upon privacy.” (quoting *Andresen v. Maryland*, 427 U.S. 463, 482 n.11
8 (1976))).

9 “As the Ninth Circuit has made clear, ‘the reality that overseizing is an inherent
10 part of the electronic search process’ requires [courts] to ‘exercise greater vigilance in
11 protecting against the danger that the process of identifying seizable electronic evidence
12 could become a vehicle for the government to gain access to a larger pool of data that it
13 has no probable cause to collect.’” *In re Apple iPhone*, 31 F. Supp. 3d 159, 168
14 (D.D.C. 2014) (quoting *Schesso*, 730 F.3d at 1042). In search warrant execution as in
15 all Fourth Amendment analysis, the Fourth Amendment’s purpose to prevent general
16 warrants is paramount and the protections are “to be liberally construed” in favor of
17 individual rights. *See United States v. Bridges*, 344 F.3d 1010, 1014 & n.1 (9th Cir.
18 2003) (quoting *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931)); *see*
19 *also United States v. Ramirez*, 523 U.S. 65, 71 (1998); *Payton v. New York*, 445 U.S.
20 573, 583 (1980). Any attempt to exploit Fed. R. Crim. P. 41 to turn a temporary
21 overseizure into a general warrant must therefore be rejected.

22 **II. ARGUMENT**

23 The government seized the digital devices at issue almost seven months ago.
24 During Friday’s hearing, the government revealed that it *still* has not conducted the
25 responsiveness reviews required by Fed. R. Crim. P. 41 and the Fourth Amendment to
26 determine which files are responsive to the warrant and subject to seizure. Instead of
27 having a search team conduct a responsiveness review pursuant to a search protocol and
28 seizing only a portion of each device (as the Warrant requires), in this case, the

1 government—apparently including attorneys who are not part of the search team as
2 defined by the Warrants—is selecting its trial exhibits from the *entirety of massive*
3 *digital devices and announced that it intends to deem the files it selects as exhibits*
4 *“seized.”* That is contrary to the letter and spirit of the Fourth Amendment, Federal
5 Rules of Criminal Procedure 16 and 41, and this Court’s discovery cut-off, which
6 required production of all discovery by March 15, 2020—precisely to avoid this sort of
7 last-minute addition of evidence.

8 The government’s search warrant execution strategy in this case was to exploit
9 the off-site responsiveness review permitted by Fed. R. Crim. P. 41 to seize entire
10 digital devices (i.e., execute a general warrant seizing all of one’s papers), then delay
11 that responsiveness review until after the government had selected which of the files on
12 those devices it wanted to introduce into evidence. The government flouted this
13 Court’s discovery order, ignored the prosecution’s Rule 16 obligation to produce the
14 portion of the device that had been seized by March 15, 2021, and undermined the
15 Fourth Amendment by seeking to accomplish exactly what it was designed to prohibit:
16 a general warrant in which the government is free to peruse at its leisure the entirety of
17 a person’s life use any digital file in a person’s possession against them. Exclusion of
18 the files—none of which were timely seized in a responsiveness review—is therefore
19 proper under Rule 16 and the discovery cut-off order and under the Fourth Amendment.

20 **A. The Government’s Search Warrant Execution Violated the Terms of**
21 **the Warrants and the Fourth Amendment**

22 The Warrants (Ram Decl. Ex. A, Ex. B) imposed two important limitations on
23 the government’s review of seized digital devices. First, the Warrants required a
24 responsiveness review be completed “as soon as is practicable” and no later than March
25 5, 2021. Warrants Attach. B ¶ 4.a. Second, the Warrants required that a “search team
26 will conduct the search only by using search protocols specifically chosen to identify
27 only the specific items to be seized under this warrant.” *Id.* ¶ 4.b; *see also id.* ¶ 5
28 (noting that after law enforcement officials conducted the responsiveness review,

1 government attorneys could review the resulting “seized or copied” data). Rather than
2 execute a responsiveness review using search protocols, the government sought an
3 unlawful extension that would give the prosecutors unfettered access to the raw data
4 throughout trial. Because the government failed to complete a responsiveness review
5 as soon as practicable, failed to secure a valid extension, and failed to utilize proper
6 search protocols, exclusion is appropriate.

7 **1. The Government Failed to Complete a Responsiveness Review**
8 **as Soon as Practicable and Failed to Secure a Valid Extension**

9 The Fourth Amendment and Fed. R. Crim. P. 41 permit the *temporary*
10 overseizure of electronic data to identify the limited files within that data that fall
11 within the scope of the warrant’s probable cause. Fed. R. Crim. P. 41(e)(2)(B). In
12 order to avoid “frequent petitions to the court for additional time,” Rule 41 does not
13 impose a one-size-fits-all deadline and instead permits “a judge [to] impos[e] a deadline
14 ... at the time the warrant is issued.” Fed. R. Crim. P. 41 adv. comm. note (2009). In
15 this case, the Warrant instructed that “[t]he search team shall complete the search of
16 [digital devices or forensic copies thereof] as soon as is practicable but not to exceed
17 120 days from the date of execution of the warrant.” Warrant Attach. B ¶ 4.a. The
18 120-day period expired on March 5, 2020.

19 The government failed to complete its review as soon as practicable. When the
20 120-day period expired, the government had not even *begun* a responsiveness review of
21 the digital devices at issue. *See Sealed Ex Parte App’n for Extension* ¶ 8.a (Mar. 4,
22 2021) (DOJ_PROD_0000162873) (Ram Decl. Ex. C) (“Extension App’n”) (claiming
23 that the only devices that had begun a responsiveness review were tainted devices from
24 the Miami airport stop and that the remaining devices were “still being imaged and
25 process by the lab and reviewed by the filter team”).² This “backlog in the imaging and

26 ² This application was produced to the defendants on May 13, 2021 along with the government’s
27 motion to file its ex parte application under seal. *See Ram Decl. Ex. D* (DOJ_PROD_0000162894)
28 (“Sealing App’n”). A substantially identical application was filed with respect to each of the devices
at issue.

1 review process” was the government’s own doing; it was “caused” by the decision to
2 seize approximately 50 devices during the ransacking of the defendants’ houses. *Id.*
3 ¶ 8.d. Although the government blamed the FBI forensic team’s resources being
4 “stretched” due to important “investigations arising out of the January 6, 2021
5 insurrection at the U.S. Capitol,” *id.* this was (at best) a red herring. The relevant
6 devices were seized on November 5, 2020. Although the government has not produced
7 the FD-302 memoranda for these devices, the memoranda for other devices show that
8 CART was able to process the data within one week but that the government waited
9 multiple months to submit a request.³ In any event, all of the relevant devices had been
10 processed by February 1, 2020 at the latest,⁴ leaving the government with over one
11 month to complete its responsiveness review.⁵

12 At Friday’s hearing, the government attempted to argue that it had obtained an
13 extension and had until July to finish its responsiveness review, but that extension is
14 invalid. The government obtained a post-indictment extension on an *ex parte* and
15 *sealed* basis to prevent the defendants from being heard on an additional deprivation of
16 property. The government’s extension was obtained by deceiving the Court,
17 withholding material facts, and seeking relief that is not authorized by any statute. To
18 prevent the defendants from challenging its unlawful warrant execution, the
19 government wrongfully applied for and received permission to seal its extension
20 request even though the underlying warrant had already been disclosed and the
21

22 ³ See Ram Decl. Ex. E (DOJ_PROD_0000153655; DOJ_PROD_0000153807;
23 DOJ_PROD_0000153808) (Dec. 16, 2020 request to process 7 devices completed by Dec. 21, 2020;
24 Jan. 4, 2021 request to process 6 devices completed by Jan. 7, 2021; Jan. 4, 2021 request to re-process
25 7 devices completed by Jan. 7, 2021).

26 ⁴ See Ram Decl. Ex. F (Feb. 1, 2021 discovery letter).

27 ⁵ The government also claimed to have utilized a filter review. Extension App’n ¶ 8.b. It is unclear
28 whether this is true. The government never asked for a filter term list and the resulting productions
included both attorney-client privileged materials and privileged confidential marital communications.
Regardless of whether the government’s claim is false, the government knew a filter review was
necessary when it secured the Warrant and any such review would therefore have been accounted for
in the 120-day limit.

1 indictment on the underlying warrant had already been returned. The government
2 falsely informed the Court that it needed the application to be sealed—four months
3 after the devices were seized from their owners and the owners were given a copy of
4 the underlying search warrant and affidavits—“to maintain the integrity of the
5 government’s ongoing investigation.” Sealing App’n at 3-4 (Ram Decl. Ex. D). In
6 support, the government cited cases about “pre-indictment disclosure of a search
7 warrant affidavit,” but they do not appear to have cited a single case or statute that
8 permits post-indictment sealing. *Cf.* Fed. R. Crim. P. 41(f)(3) (noting that notice may
9 only be delayed “if the delay is authorized by statute”). The government further
10 misrepresented that “[t]he search warrants in this case remain under seal,” only
11 disclosing that the affidavits had been produced to the defendants. Sealing App’n at 5.

12 The government did not disclose that all of the devices were seized from the four
13 existing defendants; that the government had been ordered to produce all outstanding
14 discovery to those four defendants by March 15, 2020; and that those four defendants
15 had a May 4, 2020 trial date. The government did not disclose these facts because it
16 knew that they would be material to denying the government’s application. Instead, the
17 government falsely assured the Court—five days before obtaining the superseding
18 indictment—that if the property owners were informed “before any additional charging
19 decisions can be made, there is a significant risk that the case would be jeopardized by,
20 among other reasons, potentially alerting additional subjects that the investigation is
21 ongoing.” *Id.*

22 The government’s stated justification to prevent the defendants from being heard
23 was utterly false for two reasons. First, as the government has trumpeted to this Court
24 it had told the defendants that the investigation was ongoing months earlier. *See, e.g.,*
25 Gov’t’s Opp’n to Mot. to Dismiss at 1, Dkt. 278 (Apr. 12, 2021) (“[In a January 2021
26 email,] [t]he government put defendant on notice that he was subject to an ongoing
27 investigation”). The government is not free to assure one judge that its
28 investigation is so secret that property owners cannot be permitted their constitutional

1 right to notice and an opportunity to be heard while simultaneously assuring another
2 judge that the same people are fully informed of the ongoing investigation. Second,
3 knowledge of the ongoing investigation had nothing to do with the government's
4 sealing. Indeed, the superseding indictment was unveiled less than one week later, and
5 yet the government refused to produce the Extension Application and Sealing
6 Application for *over two months thereafter*. The Extension Application revealed no
7 privileged trial strategy or investigatory details, and there was no valid reason to seal.
8 The government did not want the defendants to object to the unlawful bases for seizing
9 their property, so it lied to the Court to keep them in the dark.

10 The defense has twice asked the government for its legal authority for proceeding
11 on an ex parte, sealed basis after an indictment of the owners or possessors of the
12 digital devices. The government has not responded. That is because no authority
13 exists. *Cf. Purbeck v. Wilkinson*, No. 21-cv-47, 2021 WL 1550563, at *5 (noting that
14 even property owners who have not yet been indicted can have a Fourth Amendment
15 right of access); *In re Search Warrant*, No. 00-cr-138, 2000 WL 1196327, at *1
16 (D.D.C. July 24, 2000) (noting that the general right to unsealing affidavits derives
17 from a defendant's constitutional right to move to suppress and therefore attaches after
18 indictment); *In re Search Warrants Issued Aug. 29, 1994*, 889 F. Supp. 296, 299 & n.4
19 (S.D. Ohio 1995) (holding that the Fourth Amendment includes the right to examine the
20 affidavit supporting a warrant and holding that fears of jeopardizing a continuing
21 criminal investigation were insufficient because the government demonstrate "no less
22 restrictive means, such as redaction" would satisfy that interest). The defendants were
23 entitled to object to the seizure of their property for an additional 120 days, *see*
24 *Matthews v. Eldridge*, 424 U.S. 319, 333 (1976) ("The fundamental requirement of due
25 process is the opportunity to be heard "at a meaningful time and in a meaningful
26 manner." (quoting *Armstrong v. Manzo*, 380 U.S. 545, 552 (1965))), but they were
27 wrongfully deprived of that right by the government's misrepresentations to the Court.

1 The resulting extension violated the defendants' rights under Rule 41 and the
2 Constitution and is without force or effect.

3 **2. The Government Violated the Warrant's Requirement that the**
4 **Responsiveness Review Be Conducted By a Law Enforcement**
5 **Officer Search Team Utilizing Search Protocols**

6 The Warrants require that the "[t]he search team will conduct the search only by
7 using search protocols specifically chosen to identify only the specific items to be
8 seized under the warrant." Warrant ¶ 4.b. The search team (defined as "law
9 enforcement personnel or other[s] assisting law enforcement personnel") is supposed to
10 use these search protocols to identify specific files, copy the specific files (¶ 4.e),
11 produce the resulting seized or copied files to the prosecutors (¶ 5).

12 The government appears to be violating the Warrants in two ways. First, the
13 government is not using search protocols to identify specific responsive files. A search
14 protocol is "an explanation of the scientific methodology the government will use to
15 separate what is permitted to be seized from what is not, will explain to the Court how
16 the government will decide where it is going to search." *In re Apple iPhone, IMEI*
17 *013888003738427*, 31 F. Supp. 3d 159, 166 (D.D.C. 2014); *CDT III*, 621 F.3d at 1179
18 (Kozinski, C.J., concurring) (equating search protocol with "[t]he process of sorting,
19 segregating, decoding and otherwise separating seizable data (as defined by the
20 warrant) from all other data"). Ideally, search protocols will ensure that those
21 prosecuting the case are not exposed to raw data until after an independent
22 responsiveness review has deemed it within the scope of the warrant. *See In re App'n*
23 *for Warrant (Cunnius)*, 770 F. Supp. 2d 1138, 1150 (W.D. Wash. 2011) (endorsing
24 *CDT* concurrence protocols and emphasizing the importance of releasing only
25 responsive data to investigating agents); *see also CDT III*, 621 F.3d at 1179 (Kozinski,
26 C.J., concurring) (urging courts to require a protocol that prevented agents involved in
27 the investigation from seeing data until the responsive data has been segregated); *cf.*
28 *United States v. Schesso*, 730 F.3d 1040, 1049 (9th Cir. 2013) (explaining that "The
seized electronic data was reviewed by Investigator Holbrook, a specialized computer

1 expert, rather than Detective Kennedy, the case agent, and Schesso does not assert that
2 Holbrook disclosed to Kennedy ‘any information other than that which [was] the target
3 of the warrant.’”).

4 In *United States v. Bonner*, a court in the Southern District of California
5 explained that search protocols must be “reasonably directed to identify data within the
6 scope of the warrant in order to meet the particularity requirement.” No. 12-cr-3429,
7 2013 WL 3829404, at *19 (S.D. Cal. July 23, 2013). Without such a protocol in place,
8 “the search of the electronic data becomes general exploratory rummaging in a person's
9 belongings.” *Id.* Because the government’s protocol “expanded the search to data
10 which the Government had no probable cause to collect,” the *Bonner* court concluded
11 that the search protocol was “not directed to identify data within the scope of the
12 warrant and violated the Defendant’s rights under the Fourth Amendment.

13 So too here. The government has jettisoned the search protocol requirement
14 altogether. In its March 4 extension request, the government revealed that its protocols
15 contain no restrictions on search methodology mistakenly defining the protocol as
16 imaging and processing devices, conducting a filter review, and producing the devices
17 to the case agents for a responsiveness review pursuant to the warrant. Extension
18 App’n ¶ 7. Search protocols are supposed to provide a detailed “explanation of how the
19 government intends to conduct the search so that the Court may conclude that the
20 government is making a genuine effort to limit itself to a particularized search.” *Apple*
21 *iPhone*, 31 F. Supp. 3d at 168; *see also In re Odys Loox Plus Tablet*, 28 F. Supp. 3d 40,
22 46 (D.D.C. 2014) (holding that no search protocol would be deemed adequate without
23 an explanation of how the search would be done to ensure it was not a “general,
24 exploratory rummaging in a person’s belongings” (quoting *Coolidge v. New*
25 *Hampshire*, 403 U.S. 443, 467 (1971))). The government’s protocol does not explain
26 how it will limit its responsiveness review at all, and indeed it has not. Implicit in the
27 government’s in-court representations on Friday is the conclusion that the
28 government—including its attorneys who are not authorized members of the search

1 team—are selecting trial exhibits directly from the raw phones with no protocol or
2 restrictions in place. That is the essence of a “general, exploratory rummaging in a
3 person’s belongings” and is anathema to the Fourth Amendment and the Warrant.

4 Because government attorneys are accessing data that has not already been seized
5 and because they are doing so without a valid search protocol in place, the government
6 is violating the Warrant’s terms and the Fourth Amendment.

7 **B. The Government’s Search Warrant Execution Was Unreasonable**
8 **Because It Amounts to a General Warrant**

9 An individual’s liberty is not protected from general warrants if the government
10 remains free to seize “a digital record of nearly every aspect of [individuals’] lives” and
11 avoid narrowing that digital record until after trial. *See Riley v. California*, 573 U.S.
12 373, 395 (2014). In *Riley*, the Supreme Court stated with approval: “In 1926, Learned
13 Hand observed (in an opinion later quoted in *Chimel*) that it is ‘a totally different thing
14 to search a man’s pockets and use against him what they contain, from ransacking his
15 house for everything which may incriminate him.’” *Id.* (quoting *United States v.*
16 *Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926)). In another portion of Judge Hand’s
17 quoted opinion, he noted that while “a thorough search of all that the offender has” may
18 be necessary to ensure that the government finds every piece of evidence, that is
19 “exactly what the [Fourth] amendment was designed to prevent.” *Kirschenblatt*, 16
20 F.2d at 204. Here, the government seeks not just to ransack defendants’ houses for a
21 thorough search of all that the defendants have, but to be able to continue doing so
22 through trial. The government has an executed a strategy in this case that would allow
23 it to do just that: pushing out its responsiveness review deadline to ensure that it
24 maintains the whole of each defendant’s digital record for use at trial.

25 That strategy, particularly in light of the discovery cut-off, violated the Fourth
26 Amendment’s prohibition of unreasonable search warrant execution. “[B]oth the scope
27 of a seizure permitted by a warrant, and the reasonableness of government conduct in
28 executing a valid warrant, can present Fourth Amendment issues.” *United States v.*

1 *Huntoon*, No. 16-cr-46, 2018 WL 1755788, at *2 (D. Ariz. Apr. 12, 2018); *see also*
2 *Tamura*, 694 F.2d at 596 (“The government’s unnecessary delay in returning the [non-
3 responsive property] appears to be an unreasonable and therefore unconstitutional
4 manner of executing the warrant.”). “The reasonableness of a search or seizure
5 depends not only on when it is made, but also on how it is carried out.” *Franklin v.*
6 *Foxworth*, 31 F.3d 873, 875 (9th Cir. 1994); *see also United States v. Adjani*, 452 F.3d
7 1140, 1149 (9th Cir. 2006) (“We understand the heightened specificity concerns in the
8 computer context, given the vast amount of data they can store.”).

9 Fed. R. Crim. P. 41’s authorization of off-site review was meant as a substitute
10 for on-site review, not a substantive expansion of the federal government’s authority to
11 search private property. *See* Fed. R. Crim. P. 41 adv. comm. note (2009) (noting that
12 the reason for permitting off-site review is “[p]ractical[ity]” and “the need for a two-
13 step process,” not a desire to afford a new substantive power to law enforcement and
14 that property owners should retain “an expectation of the timing for return of the
15 property”); *cf.* Warrants Attach. B ¶ 4.a (“The search team shall complete the search as
16 soon as is practicable”). The government’s strategy in this case attempts to use that
17 authorization as a loop hole that would provide precisely that: a substantive expansion
18 of its power to search and seize items to be used against their owners. Here, the
19 government chose to execute a mass seizure of devices, chose to indict the case two
20 weeks later, chose to wait approximately one month before it started processing the
21 devices, made no effort to complete its responsiveness review (or even start it) was
22 aware that it was subject to a discovery cut-off, and submitted a misleading extension
23 request that it kept from the defendants in order to hide material information from the
24 reviewing judge. The government’s strategy was designed to ensure that it had the full
25 forensic device at its disposal when picking trial evidence, which is precisely the type
26 of general warrant that the Fourth Amendment was designed to prevent. The strategy
27 should result in exclusion.

C. Exclusion is Proper Under Rule 16 and the Discovery Cut-Off Order

The government's failure to complete its discovery has violated this Court's Discovery Order. The government was required to comply with *all of its discovery obligations*—including disclosure of items material to preparing the defense and items that the government intends to use in its case-in-chief at trial—by March 15, 2021. In Chambers Order, Dkt. 105 (Dec. 22, 2020).

The government's argument at Friday's hearing was that disclosing a forensic copy of the devices containing terabytes of data was sufficient to meet its obligations, but the government is wrong. Rule 16 applies to each "portion[] of any of these items" that is material to preparing the defense, that the government intends to use in its case in chief, or that was obtained from the defendant. Fed. R. Crim. P. 16(a)(1)(E). By producing the entire item, the government does not obviate its duty to produce the "portion" of the item that it intends to use particularly where knowing that subset is material to preparing the defense. The government claims that the devices hold so much data that it could not complete a cursory responsiveness review—meant to be a substitute for paging through a bookcase while on site—in the *four months* provided by the initial warrant. How can the defendants (without the resources of the federal government) possibly be expected to complete an in-depth substantive content review and prepare a defense while simultaneously processing the other information the government has amassed? The defendants pushed for disclosure and a discovery cut-off because the government used the grand jury's powers to secure over 20 terabytes of data, more than the Library of Congress and its 20 million books.⁶ The simple answer is that the defendants cannot possibly process the government's addition of newly seized data⁷ within two weeks.

⁶ See Michael Lesk, How Much Information Is There In the World?, <https://chnm.gmu.edu/digitalhistory/links/pdf/introduction/0.6a.pdf>.

⁷ To be clear, the entire devices were obtained from the defendants in November 2020. Only the portion marked responsive can lawfully be seized. Thus, the government has produced the data obtained from the defendants, but it has not produced the portion that was seized.

1 Based on the government's failure to produce the portion of the phones that it
2 was seizing in time for the discovery cut-off, the Court has discretion to exclude the
3 proposed seized data to enforce its order. *See United States v. W.R. Grace*, 526 F.3d
4 499, 514 (9th Cir. 2008) (en banc) (upholding exclusion of government evidence not
5 disclosed by discovery deadline); *United States v. Ornelas*, 906 F.3d 1138, 1150-51
6 (9th Cir. 2018) (affirming exclusion of testimony disclosed shortly before trial as
7 enforcement of discovery order); *United States v. Roybal*, 566 F.2d 1109, 1110-11 (9th
8 Cir. 1977) (reversing conviction, emphasizing that the provision of late discovery in
9 violation of a specific order resulted in "unfairness and potential prejudice to the
10 defendant" as well as "unfairness and discourtesy to the trial judge"); *United States v.*
11 *Schwartz*, 857 F.2d 655, 659 (9th Cir. 1988) (reaffirming that "the district court may
12 exclude documents or witnesses" where the government "fail[s] to comply with the
13 court's pretrial or discovery orders."). Although no showing of prejudice is necessary,
14 *see W.R. Grace*, 526 F.3d at 515, prejudice will occur in this case because the addition
15 of the seized data to the government's already large pool of seizures, with only two
16 weeks until trial, would make it potentially impossible for the defendants to adequately
17 prepare.

18 In *United States v. Garcia*, a defendant moved to exclude evidence of a prior
19 conviction because it was not produced to her in discovery before the discovery
20 deadline of June 30, 2010. 730 F. Supp. 2d 1159 (C.D. Cal. 2010). The government
21 argued that by producing Garcia's entire criminal record, it had satisfied its discovery
22 deadline. Opp'n to Def't's Mot. in *Limine* to Exclude Evidence of Garcia's Prior
23 Offense, *United States v. Garcia*, 2:10-cr-595, Dkt. 32 (C.D. Cal. July 13, 2010). The
24 court, expressing doubt that the production actually contained the did not rule on that
25 basis. Instead, it ruled that due the government's failure to produce the evidence that it
26 sought to admit prior to the discovery cut-off, enforcement of the discovery cut-off and
27 exclusion of evidence was appropriate. *Garcia*, 730 F. Supp. 2d at 1168-69.

1 In *United States v. Sadr*, the government produced both a forensic copy of the
2 defendant's email account in April 2018 and the portion of that email account
3 (approximately 358 documents) marked "responsive" or "pertinent" in May 2018. The
4 discovery cut-off in that case passed in July 2018. See Mem. of Law Supp. Mot. to
5 Exclude at 2-6, *United States v. Sadr*, No. 18-cr-224, Dkt. 149 (S.D.N.Y. Oct. 10,
6 2019). Later in the litigation, after the discovery deadline had passed, the government
7 proposed to add 1,775 documents to the pool of responsive documents, arguing (as the
8 government does here) that the forensic copy of the defendant's email account was
9 sufficient to comply with its discovery obligations. See Sept. 17, 2019 Letter from U.S.
10 Attorney's Office for the Southern District of New York, *United States v. Sadr*, No. 18-
11 cr-224, Dkt. 149-3 (S.D.N.Y. Oct. 10, 2019). The defendant moved to exclude
12 pursuant to Rule 16 arguing that the court should exercise its discretion to enforce the
13 discovery deadline or to sanction the government's discovery failures and that the
14 prejudice to the defense from expanding the pool of potential evidence exceeded the
15 prejudice to the government, who had already indicted the case based on the more
16 limited pool. After initially opposing the motion, the government ultimately agreed not
17 to use the documents despite the earlier production of a forensic copy, and the
18 documents were properly excluded.⁸

19 In cases like this, courts frequently look to the reason for the delay. See, e.g.,
20 *United States v. Davis*, 244 F.3d 666, 671 (8th Cir. 2001) (chastising the government
21 for not seeking a continuance or otherwise challenging the discovery deadline and
22 affirming exclusion of evidence); *United States v. Mason*, No. 06-cr-80, 2008 WL
23 281970, at *3, *4 (S.D.N.Y. Jan. 25, 2008) ("Here, the government concedes that there
24 were 'shortfalls . . . ,' but offers no excuse or explanation, acceptable or otherwise, for
25 the failure to timely disclose evidence" that defendant had specifically sought for
26 eleven months). Here, there is no good reason for the government's delay. It was
27

28 ⁸ See Nov. 25, 2019 Hr'g Tr. at 36-39.

1 given three months' warning of the March 15, 2021 discovery cut-off and yet it treated
2 that cut-off as a mere suggestion. It exhibited no interest in protecting the rights of the
3 defendants either to discovery or to exclusive possession of their property. The
4 government's delay merits exclusion and under the Court's discovery cut-off order, it
5 has that authority.

6 **D. The Electronic Files Should Be Excluded Due to *Kastigar* Taint**
7 **Infecting the Review Process**

8 Based on the government's description at Friday's hearing, the same government
9 team members are reviewing the phones that previously reviewed, received, or used
10 tainted information. *Kastigar* prohibits using tainted information as an investigatory
11 lead or to uncover evidence, to interpret evidence, to build a case, or to make trial
12 decisions like selecting exhibits. *See* Joint Mot. for *Kastigar* Hearing, to Disqualify the
13 Prosecution Team, and to Dismiss at 8-9, Dkt. 338 (May 17, 2021). The ongoing
14 responsiveness review is therefore tainted.

15 **III. CONCLUSION**

16 The Fourth Amendment's purpose is to prohibit general warrants. If the
17 government's strategy in this case—seizing masses of digital device data and refusing
18 to perform the required responsiveness review until after it figures out which evidence
19 to mark as trial exhibits against the device's owner—is tantamount to a declaration that
20 the Fourth Amendment's restrictions do not apply to digital devices. That declaration
21 can and should be emphatically rejected. The government's failure to promptly
22 perform a responsiveness review, unlawful extension request, and unconstitutional
23 strategy merits exclusion of the digital device evidence the government proposes to use.

24 //

25 //

26 //

27 //

28 //

1 Dated: May 24, 2021

Respectfully submitted,

2 /s/ Ashwin J. Ram

3 Ashwin J. Ram (SBN 227513)

4 *aram@steptoe.com*

5 Michael A. Keough (SBN 327037)

6 *mkeough@steptoe.com*

7 Meghan L. Newcomer (*pro hac vice*)

8 *mnewcomer@steptoe.com*

9 Nicholas P. Silverman (*pro hac vice*)

10 *nsilverman@steptoe.com*

11 **STEPTOE & JOHNSON LLP**

633 West Fifth Street, Suite 1900

12 Los Angeles, CA 90071

13 Telephone: (213) 439-9400

14 Facsimile: (213) 439-9599

15 *Counsel for Defendant Richard Ayvazyan*

16 /s/ John L. Littrell

17 John L. Littrell (SBN 221601)

18 *jlittrell@bklwlaw.com*

19 Ryan V. Fraser (SBN 272196)

20 *rfraser@bklwlaw.com*

21 **BIENERT KATZMAN LITRELL**

22 **WILLIAMS, LLP**

23 601 W. 5th Street, Suite 720

24 Los Angeles, CA 90071

25 Telephone: (213) 528-3400

26 Facsimile: (949) 369-3701

27 *Counsel for Defendant Marietta Terabelian*

28 [SIGNATURES CONTINUE ON NEXT PAGE]

/s/ Thomas A. Mesereau Jr.

Thomas A. Mesereau Jr. (SBN 91182)

mesereau@mesereaulaw.com

MESEREAU LAW GROUP, P.C.

10100 Santa Monica Blvd., Suite 300

Los Angeles, CA 90067

Telephone: (310) 651-9960

Jennifer J. Wirsching (SBN 263141)

wirschinglaw@outlook.com

ATTORNEY AT LAW

1935 Alpha Rd, Suite 216

Glendale, CA 91208

Telephone: (424) 902-9280

Counsel for Defendant Artur Ayyazyan

/s/ Fred G. Minassian

Fred G. Minassian (SBN 170974)

fgminassian@yahoo.com

LAW OFFICES OF FRED G. MINASSIAN, INC.

101 N. Brand Ave, Suite 1970

Glendale, CA 91203

Telephone: (818) 240-2444

Counsel for Defendant Tamara Dadyan

SIGNATURE ATTESTATION

Pursuant to Local Rule 5-4.3.4(a)(i), the filer attests that all signatories listed, and on whose behalf the filing is submitted, concur in the filing's content and have authorized the filing.