

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 REPLY IN SUPPORT OF
MOTION TO EXCLUDE DIGITAL
DEVICE FILES FROM DEVICES
OBTAINED ON NOVEMBER 5,
2020**

Hon. Stephen V. Wilson

Hearing Date: June 14, 2021
Time: 1:30 p.m.

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	ARGUMENT	3
A.	THE GOVERNMENT VIOLATED THE WARRANTS’ REQUIREMENT THAT “THE SEARCH TEAM SHALL COMPLETE THE SEARCH AS SOON AS PRACTICABLE BUT NOT TO EXCEED 120 DAYS FROM THE DATE OF EXECUTION OF THE WARRANT.”	3
1.	The Government Failed to Complete a Responsiveness Review “as soon as practicable but not to exceed 120 days from the date of execution of the warrant” and Failed to Secure a Valid Extension	4
a.	The Extension Was Unlawfully Obtained and Therefore Invalid.....	6
b.	Regardless of Any Extension, the Government Failed to Complete Its Review “as soon as practicable”	9
2.	The Government Violated the Warrants’ Search Protocol Requirement.....	14
3.	The Government Utilized Prosecutors Who Were Not Part of the “Search Team” as Defined in ¶ 4.a of the Warrants	16
B.	THE GOVERNMENT’S SEARCH WARRANT EXECUTION WAS UNREASONABLE BECAUSE IT AMOUNTS TO A GENERAL WARRANT	18
C.	EXCLUSION IS PROPER UNDER RULE 16 AND THE DISCOVERY CUT-OFF ORDER.....	20
D.	THE ELECTRONIC FILES SHOULD BE EXCLUDED DUE TO <i>KASTIGAR</i> TAIN T INFECTING THE REVIEW PROCESS	21
III.	CONCLUSION.....	22

TABLE OF AUTHORITIES

	Cases	Page(s)
1		
2		
3		
4	<i>Andresen v. Maryland</i> ,	
5	427 U.S. 463 (1976).....	9
6	<i>In re Apple iPhone, IMEI 013888003738427</i> ,	
7	31 F. Supp. 3d 159 (D.D.C. 2014).....	14
8	<i>Brock v. Roadway Express</i> ,	
9	481 U.S. 252 (1987).....	6
10	<i>Durham v. Prudential Ins. Co.</i> ,	
11	No. 16-cv-8202 (ODW), 2017 WL 7661482 (C.D. Cal. Apr. 26, 2017)	7
12	<i>M.A.C. ex rel Garcia v. City of Los Angeles</i> ,	
13	No. 16-cv-4477 (DMG) 2017 WL 10574306 (C.D. Cal. Dec. 8, 2017)	7
14	<i>Giever v. City of Las Cruces</i> ,	
15	No. 08-cv-155, 2010 WL 11626776 (D.N.M. Jan. 12, 2010)	16
16	<i>Hall v. Tudbury</i> ,	
17	35 F. App'x 428 (9th Cir. 2002)	3
18	<i>Horton v. California</i> ,	
19	496 U.S. 128 (1990).....	3
20	<i>Joint Anti-Fascist Refugee Comm'n v. McGrath</i> ,	
21	341 U.S. 123 (1951).....	6
22	<i>Mathews v. Eldridge</i> ,	
23	424 U.S. 319 (1976).....	6
24	<i>Plummer v. Camarillo</i> ,	
25	No. 19-cv-7489 (PSG), 2019 WL 8226106 (C.D. Cal. Dec. 23, 2019)	7
26	<i>In re Search Warrant (Cunnius)</i> ,	
27	770 F. Supp. 2d 1138 (W.D. Wash. 2011)	13
28	<i>Simon v. City of New York</i> ,	
	893 F.3d 83 (2d Cir. 2018).....	3
	<i>In re Taylor</i> ,	
	567 F.2d 1183 (2d Cir. 1977)	6

1	<i>United States v. Aboshady,</i>	
2	951 F.3d 1 (1st Cir. 2020).....	15
3	<i>United States v. Bonner,</i>	
4	No. 12-cr-3429, 2013 WL 3829404 (S.D. Cal. July 23, 2013)	15
5	<i>United States v. Comprehensive Drug Testing, Inc.,</i>	
6	579 F.3d 989 (9th Cir. 2009)	8, 14
7	<i>United States v. Comprehensive Drug Testing, Inc.,</i>	
8	621 F.3d 1162 (9th Cir. 2010)	<i>passim</i>
9	<i>United States v. Galpin,</i>	
10	720 F.3d 436 (2d Cir. 2013)	2
11	<i>United States v. Ganas,</i>	
12	755 F.3d 125 (2d Cir. 2014)	6
13	<i>United States v. Harris,</i>	
14	973 F.2d 333 (4th Cir. 1992)	21
15	<i>United States v. Kirschenblatt,</i>	
16	16 F.2d 202 (2d Cir. 1926).....	5
17	<i>United States v. Mapes,</i>	
18	59 M.J. 60 (C.A.A.F. 2003)	21
19	<i>United States v. McDaniel,</i>	
20	482 F.2d 305 (8th Cir. 1973)	21
21	<i>United States v. Microsoft,</i>	
22	56 F.3d 1448 (D.C. Cir. 1995).....	6
23	<i>United States v. Penn,</i>	
24	647 F.2d 876 (9th Cir. 1980)	3
25	<i>United States v. Phua,</i>	
26	No. 14-cr-249, 2015 WL 1281603 (D. Nev. Mar. 20, 2015)	14
27	<i>United States v. Powell,</i>	
28	No. 19-cr-216, 2020 WL 2199758 (N.D. Ohio May 6, 2020).....	16
	<i>United States v. Rice,</i>	
	421 F. Supp. 871 (E.D. Ill. 1976)	21

1 *United States v. Tamura*,
2 694 F.2d 591 (9th Cir. 1982) 5, 9, 19

3 **Statutes**

4 Cal. Penal Code § 830.1 16

5 **Other Authorities**

6 Fed. R. Crim. P. 16..... 20

7
8 Fed. R. Crim. P. 16(a)(1)(E) 20

9 Fed. R. Crim. P. 41 4, 5, 7

10 Fed. R. Crim. P. 41(f)(3) 7

1
2 **I. INTRODUCTION**

3 The government’s opposition advocates for government authority to execute a
4 general warrant of digital devices. The government seized smartphones containing “the
5 entirety of a person’s digital life,” then—rather than executing the responsiveness
6 review required by the warrants and seizing only items identified as responsive during
7 that review—held the devices for trial to ensure that any item it wanted to use as an
8 exhibit would be seized even if it was not immediately identified as responsive. *See*
9 May 21, 2021 Hr’g Tr. at 37 (Ram Decl. Ex. A) (prosecutors “now are in the process of
10 identifying which piece of information we’ll seize and use as exhibits at trial”). The
11 government’s approach—if permitted—would undermine the purpose of
12 responsiveness reviews to mimic on-site searches and enable the twenty-first century
13 version of the general warrants the Fourth Amendment was intended to prohibit. *See*
14 Mot. to Exclude Digital Device Files at 2-3, Dkt. 363 (describing cases forming the
15 “wellspring” of the Fourth Amendment).

16 But the search warrants in this case required more. The warrants followed Ninth
17 Circuit guidance by requiring that the government conduct a responsiveness review as
18 soon as practicable, implement a search protocol, and shield the prosecutors from
19 exposure to the data before it was seized. The government violated each of those
20 search warrant requirements, and its search is therefore effectively warrantless.
21 Because no exception is advocated by the government (and none applies), the
22 warrantless search is unconstitutional. The cases cited by the government’s
23 opposition—involving warrants that did not include the restrictions at issue in this
24 case—miss the point entirely. When government authority to search and seize is
25 conditioned on restrictions, the government is obligated to follow those conditions.
26 Enforcement of the restrictions is all the more important when dealing with vast and
27 purportedly probative electronic data. *See United States v. Comprehensive Drug*
28 *Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (*CDT III*) (emphasizing the

1 need for “greater vigilance” in cases of oversteering electronic data); *United States v.*
2 *Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (emphasizing the need for “heightened
3 sensitivity” to Fourth Amendment requirements in the electronic context).

4 The government failed to follow and flagrantly disregarded the warrant
5 requirements. Bound to execute the search warrant by completing a responsiveness
6 review “as soon as is practicable,” the government had not even begun that
7 responsiveness review for any of the 49 devices seized when the 120-day deadline
8 came and went (or one and a half months later when the government identified the four
9 devices it now seeks to use). The government has no defense to the “as soon as is
10 practicable” clause. As to the 120-day deadline, the government relies on an
11 unlawfully obtained extension, which was heard on an *ex parte*, *sealed* basis without
12 any statutory permission and in violation of the defendants’ right to be heard on being
13 deprived of their property interests for an additional 120 days. The government’s
14 submission misrepresented the dangers of informing the magistrate judge, claiming that
15 knowledge that their phone search remained ongoing would somehow imperil the
16 government’s ability to seek a superseding indictment even though (1) the government
17 had already informed the defendants of its intent to supersede; and (2) after the
18 superseding indictment was returned, the government still refused to disclose the
19 extension and sealing filings, keeping them hidden for another two months.

20 The government likewise failed to comply with the warrant requirements for a
21 responsiveness review conducted with a search protocol and conducted by a “search
22 team” composed of law enforcement personnel, not government attorneys. Both of
23 these requirements came from Ninth Circuit guidance and the government provides no
24 excuse for failing to meet them.

25 The government seized 49 electronic devices. It should be held to a high
26 standard based on the degree of intrusiveness inherent in that seizure. The gross failure
27 to minimize that intrusiveness encompassing the failed responsiveness review, the *ex*
28

1 *parte* extension, the failure to meet the discovery deadline, and the use of tainted
2 prosecutors to conduct a sham responsiveness review confirm the need for exclusion.

3 **II. ARGUMENT**

4 **A. The Government Violated the Warrants’ Requirement that “The** 5 **search team shall complete the search as soon as practicable but not to** 6 **exceed 120 days from the date of execution of the warrant.”**

7 The opening motion argued that exclusion of the digital device evidence was
8 proper because the government “violate[d] the terms of the warrant[s]” and therefore
9 conducted a warrantless search in violation of the Fourth Amendment. *See* Mot. to
10 Exclude Digital Device Files § II.A, Dkt. 363; *id.* at 2 (“The government’s delayed
11 responsiveness review strategy violates the terms of the warrant....”); *id.* at 4-5 (laying
12 out the terms of the warrant and concluding that exclusion is merited by the
13 government’s failure to adhere to the limitations in the warrant).

14 It is black letter law that “If the scope of the search exceeds that permitted by the
15 terms of a validly issued warrant or the character of the relevant exception from the
16 warrant requirement, the subsequent seizure is unconstitutional without more.” *Horton*
17 *v. California*, 496 U.S. 128, 140 (1990); *Hall v. Tudbury*, 35 F. App’x 428, 431 (9th
18 Cir. 2002) (“Because the officers exceeded the scope of the warrants when then entered
19 Hall’s motel room, [they] caus[ed] a warrantless entry into Hall’s private dwelling, [and
20 therefore] violated Hall’s Fourth Amendment rights.”). This is because “[s]earches and
21 seizures that exceed the scope of the warrant are considered warrantless....” *Simon v.*
22 *City of New York*, 893 F.3d 83, 94 (2d Cir. 2018) (“Together, these principles yield the
23 commonsense rule that police officers must abide by the limitations set forth on the face
24 of a warrant they are executing.”); *accord United States v. Penn*, 647 F.2d 876, 882 n.7
25 (9th Cir. 1980) (en banc) (“The portion of a search that exceeds the scope of a warrant
26 is, of course, unwarranted.”).

27 The defense’s § II.A argument is therefore simple: the government violated the
28 warrants’ limitations, rendering their search “warrantless” and “unconstitutional

1 without more.” Rather than respond to the argument about the warrants’ limitations,
2 the government responded to the argument that it wished the defendants had made:
3 whether the duration of the government’s search would have been reasonable in the
4 *absence of an explicit search warrant restriction*, and whether a search warrant
5 protocol is required under First Circuit law regarding *cases that did not involve a*
6 *search warrant requiring such a protocol*. With the exception of a dispute regarding
7 the Paragraph 4.a’s definition of “search team,” the government disregards that it
8 violated the terms of the warrants and effectively argues that if the warrants did not
9 contain these terms, then the government’s actions would be constitutional.

10 Search warrant restrictions are uniquely important in cases involving the mass
11 seizure of approximately 49 digital devices from family homes. The en banc Ninth
12 Circuit has encouraged judicial officers to exercise “greater vigilance ... in striking the
13 right balance between the government’s interest in law enforcement and the right of
14 individuals to be free from unreasonable searches and seizures.” *CDT III*, 621 F.3d at
15 1177. This is because temporary overseizures—while arguably necessary to search
16 electronic files—“create[] a serious risk that every warrant for electronic information
17 will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.”
18 *Id.* at 1176. The search warrants in this case exercised vigilance by incorporating
19 limitations on the government’s execution. The problem is that the government did not
20 adhere to those limitations.

21 **1. The Government Failed to Complete a Responsiveness Review**
22 **“as soon as is practicable but not to exceed 120 days from the**
23 **date of execution of the warrant” and Failed to Secure a Valid**
Extension

24 Rule 41 sets up a two-step process by which the government—instead of sitting
25 in a defendant’s home while it searches digital devices or bookcases for responsive
26 items—may temporarily overseize items to identify the portions that fall within the
27 scope of the warrant’s probable cause. Joint Mot. to Exclude Digital Device Files at 5,
28 Dkt. 363. This authorization does not guarantee that the government will find every

1 single piece of evidence, *cf. United States v. Kirschenblatt*, 16 F.2d 202, 204 (2d Cir.
2 1926) (Hand, J.) (some evidence “cannot be reached, except by a thorough search of all
3 that the offender has, to allow which would be to countenance exactly what the [Fourth
4 A]mendment was designed to prevent”); it merely substitutes for an on-site execution
5 procedure in order to protect individual property owners. *See CDT III*, 621 F.3d at
6 1171 (“The point of the *Tamura* procedures is to maintain the privacy of materials that
7 are intermingled with seizable materials, and to avoid turning a limited search for
8 particular information into a general search of office file systems and computer
9 databases.”). Judges are therefore explicitly empowered to impose deadlines. Fed. R.
10 Crim. P. 41 adv. comm. note (2009) (noting also the desire to avoid frequent requests
11 for additional time).

12 Whether or not those deadlines are constitutionally required is not the issue—at
13 least not in Argument II.A.1—and every case cited by the government is therefore
14 inapposite because each of them concerns only the reasonableness of search warrant
15 executions in cases that did not involve deadlines. The government proposed a
16 deadline of “as soon as is practicable but not to exceed 120 days from the date of
17 execution of the warrant.” The magistrate judge signed a warrant commanding the
18 government to obey that deadline. The government failed to even *begin* its review
19 process by the deadline and therefore seized zero (0) documents by the deadline.¹ The
20 post-deadline seizures were therefore warrantless and should not be admitted at trial.

21
22
23 ¹ Indeed, as of a month and a half after the deadline, on April 26, 2021, the government had not begun
24 a responsiveness review of any of the four devices it proposed to use at trial. *See* Dkt. 391-5 (noting
25 that these devices were still in the filter team’s possession and had not yet gone through the
26 responsiveness review we now know to have been conducted by the prosecution team). The fact that
27 the government determined these were the four devices it wished to use *before conducting a*
28 *responsiveness review to see what if anything could be seized from the devices* implies that the
government was accessing the devices beyond the bounds of the warrant. It was not that the
government chose these devices because they were the only ones owned by the defendants; they were
a subset out of dozens of devices owned by the defendants in their own names chosen specifically
because of their contents. The government could not have known their contents without violating the
warrants and conducting a substantive evidentiary review before any responsiveness review.

1 The determinative questions before the Court are therefore (a) whether the
2 government's post-indictment, *ex parte*, sealed extension is valid; and (b) if so, whether
3 the government completed its responsiveness review "as soon as [wa]s practicable." If
4 the answer to either question is "No," then the government violated the terms of the
5 warrants and the resulting warrantless seizures should be suppressed and excluded from
6 evidence.

7 **a. The Extension Was Unlawfully Obtained and Therefore**
8 **Invalid**

9 "Traditions of fairness that have long been honored in American jurisprudence
10 support the strongest possible presumption against *ex parte* proceedings." *Brock v.*
11 *Roadway Express*, 481 U.S. 252, 278 (1987). *Ex parte* proceedings are disfavored both
12 because they are fundamentally unfair,² and because they create the risk of erroneous
13 fact finding.³ For that reason, "Whenever the legal rights of individuals are to be
14 adjudicated, the presumption is against the use of secret proceedings." *Taylor*, 567
15 F.2d at 1188.

16 The government effectively concedes that it cannot rebut the presumption against
17 using secret proceedings. The government's extension application was a request to
18 deprive the litigants of a property interest: their right to exclude others from their
19 property.⁴ The initial warrant authorized a deprivation of 120 days, and the government

21 ² *In re Taylor*, 567 F.2d 1183, 1187-88 (2d Cir. 1977) ("In camera proceedings are extraordinary
22 events in the constitutional framework because they deprive the parties against whom they are directed
23 of the root requirements of due process," i.e., notice and a hearing); *accord United States v. Microsoft*,
24 56 F.3d 1448, 1464 (D.C. Cir. 1995) ("Ex parte communications generally are disfavored because
they conflict with a fundamental precept of justice: a fair hearing requires a reasonable opportunity to
know the claims of the opposing party and to meet them.") (citation omitted).

25 ³ *See, e.g., Mathews v. Eldridge*, 424 U.S. 319 (1976); *Joint Anti-Fascist Refugee Comm'n v.*
McGrath, 341 U.S. 123, 171 (1951) (Frankfurter, J., concurring) ("Secrecy is not congenial to truth-
26 seeking.").

27 ⁴ *See, e.g., United States v. Ganius*, 755 F.3d 125, 137 (2d Cir. 2014) (government's continued
possession of defendant's data "was a meaningful interference with Ganius's possessory rights in
those files and constituted a seizure within the meaning of the Fourth Amendment"), *rev'd en banc on*
28 *other grounds*, 824 F.3d 199 (2d Cir. 2016).

sought to institute a further deprivation. The Due Process Clause and fundamental fairness therefore entitled the defendants to an opportunity to be heard, which, under the presumption against ex parte proceedings was presumed to be a *pre-deprivation* opportunity to be heard. “When, as here, the government comes into possession of evidence by circumventing or willfully disregarding limitations in a search warrant, it must not be allowed to benefit from its own wrongdoing by retaining the wrongfully obtained evidence or any fruits thereof.” *CDT III*, 621 F.3d at 1174.

As the defendants’ opening brief pointed out, the legal underpinning of the government’s sealing request was fundamentally flawed. The sealing request cited only pre-indictment authority and did not reference a single statute under which it was entitled to delay notice. *See* Fed. R. Crim. P. 41(f)(3) (limiting delayed notice to delays authorized by statute).⁵ The Opposition does not respond to, and therefore concedes,⁶ this argument that there is no legal authority for depriving an indicted defendant of notice and the opportunity to be heard in this context.

The Opposition relies on the sealing application for its argument, cutting and pasting the very text that misled the reviewing magistrate. The government urged the magistrate to permit an extended seizure of property without notice or an opportunity to be heard because making the application public would supposedly jeopardize the

⁵ The government argues that violations of Rule 41 do not require suppression unless there was prejudice or deliberate disregard of the rule. Mem. Opp’n to Mot. to Exclude Digital Device Files at 11 n.2, Dkt. 391 (“Opp’n”). To be clear, the defense’s initial motion was to exclude based on violations of the search warrant’s terms and consequent Fourth Amendment violations, not Rule 41 violations. The government, however, raises a good point: Suppression is independently merited on the basis that the government violated rule 41, and the defendants hereby move for suppression on that basis. Even though either would suffice, there was both prejudice and deliberate disregard for Rule 41’s terms. The prejudice is an extension and set of searches that would not have occurred but for the government’s Rule 41 violations. The deliberate disregard is the government’s deliberate disregard of Rule 41’s limitation on when notice can be withheld from property holders.

⁶ *Plummer v. Camarillo*, No. 19-cv-7489 (PSG), 2019 WL 8226106, at *6 (C.D. Cal. Dec. 23, 2019) (“Arguments to which no response is supplied are deemed conceded.”); *M.A.C. ex rel Garcia v. City of Los Angeles*, No. 16-cv-4477 (DMG) 2017 WL 10574306, at *5 (C.D. Cal. Dec. 8, 2017) (“Plaintiffs do not respond to this point and have thereby conceded it.”); *Durham v. Prudential Ins. Co.*, No. 16-cv-8202 (ODW), 2017 WL 7661482, at *2 (C.D. Cal. Apr. 26, 2017) (“Plaintiff does not respond to this argument, and therefore concedes it.”).

1 forthcoming indictment because disclosing the application requesting more time to
2 conduct the responsiveness review could “alert[] additional subjects that the
3 investigation is ongoing.” Opp’n at 6 (quoting Dkt. 353 Ex. D). This representation
4 was nonsensical and the government withheld the information necessary for the
5 magistrate judge to understand why it was so:

- 6 • The government withheld the fact that the “ongoing investigation” and intent to
7 add additional defendants had already been disclosed to the defendants.
- 8 • The government withheld the fact that the defendants had already received not
9 just the search warrant but the underlying search warrant affidavits, which
10 contained far more information about the government’s investigation than the
11 application for additional time.
- 12 • The government’s application had nothing to do with the additional subjects. It
13 concerned only extended time to search devices seized from the original four
14 defendants.
- 15 • If the protective order was sufficient to ensure that the defendants did not share
16 the above information with the additional subjects—including the government’s
17 own statement that the investigation was ongoing—then it would, *a fortiori*, be
18 sufficient here, where the application had nothing to do with and did not indicate
19 a forthcoming indictment.

20 The government’s omissions and misrepresentations should not be allowed to accrue to
21 their advantage. To the contrary, in *CDT II*, the en banc Ninth Circuit instructed that
22 “omitting such highly relevant information altogether is inconsistent with the
23 government’s duty of candor in presenting a warrant application. A lack of candor in
24 this or any other aspect of the warrant application shall bear heavily against the
25 government in the calculus of any subsequent motion to return or suppress the seized
26 data.” *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 998-99 (9th
27 Cir. 2009) (en banc) (*CDT II*), opinion revised and superseded, *CDT III*. So too here.
28 The government engaged in disfavored *ex parte*, *sealed* litigation to deprive individual

1 litigants of their property without due process or fundamental fairness. The
2 government should be held to the highest of standards and under any objective reading,
3 its submission failed to meet those standards.

4 But even if all of those points were not present, the government's argument is
5 *directly contradicted* by the fact that it continued to hide its extension application and
6 sealing application for *months after the superseding indictment was returned* on March
7 9, 2021.⁷ If the justification for proceeding without notice or an opportunity to be heard
8 was the risk of endangering the superseding indictment—a dubious proposition for the
9 bulleted reasons above—then that justification was gone on March 9, 2021. Why did
10 the government continue to withhold the submissions from the property owners for 65
11 more days until May 13, 2021? There was never a need for the government to be heard
12 without notice to the property holders. The government just went ahead and did it
13 anyways because it had ceased thinking about the property holders' rights.

14 **b. Regardless of Any Extension, the Government Failed to**
15 **Complete Its Review “as soon as practicable”**

16 The requirement to complete a responsiveness review “as soon as practicable”
17 was consistent with the laudatory requirement to execute warrants “in a manner that
18 minimizes unwarranted intrusions upon privacy.” *United States v. Tamura*, 694 F.2d
19 591, 595-96 (9th Cir. 1982) (quoting *Andresen v. Maryland*, 427 U.S. 463, 482 n.11

20 ⁷ The government repeatedly chastises the defendants for not making a motion until the government
21 stopped obstinately withholding the core evidence for the motion: a description of the responsiveness
22 review and the submissions made to the Court. Prior to May 2020, the defendants attempted to inject
23 this issue into the Motion to Suppress Search Warrant Evidence, but the government refused to
24 disclose the status of its responsiveness review or its extension-related submissions. The defendants,
25 thinking that the responsiveness review had already been completed, asked the government for the
26 results of that review repeatedly. During the Friday May 21 hearing, the government finally admitted
27 on the record that it had not yet conducted a responsiveness review. May 21 Hrg Tr. at 29-30, 37-38
28 (attached hereto as Ram Decl. Ex. A) (“[We] now are in the process of identifying which pieces of
information we'll seize and use as exhibits at trial. ... we're in the process of making final decisions
about which ones we will use at trial.”).

during the Friday May 21 hearing, the defendants committed to filing by Monday May 24 and they
did so.

1 (1976))). The government was required to move forward as quickly as possible, and in
2 that respect, it utterly failed. The government chose to seize approximately 49 digital
3 devices under the warrants at issue. The government did not begin a responsiveness
4 review—the review that is designed to mimic an on-site review of an item in a person’s
5 house—*of any of the 49 devices within the 120-day period in the warrant*. The
6 government concedes this fact; while the Opposition deceptively states that “only three
7 devices” had been subjected to the responsiveness review, Opp’n at 3, each of those
8 three devices were from the October 19, 2020 tainted Miami airport stop, not the
9 November 5 search warrant execution.⁸ This is not a case where a litigant exercised
10 best efforts but came up short; this is a case where—despite an explicit warrant
11 condition to the contrary—the government showed no sense of urgency and made no
12 effort to minimize the duration of its property seizure by completing its responsiveness
13 review as soon as practicable.

14 In their opening motion, the defendants explained how the government waited
15 two months after seizing the devices before even sending them to CART lab (the
16 government’s technical team), which violated the warrant provision requiring a
17 responsiveness review as soon as practicable. Since that motion was filed, the
18 government has produced additional documents revealing (at best) lethargy and the
19 utter misrepresentation that the January 6, 2021 Capitol fallout (months after the search
20 warrants were executed) had any effect on CART’s work, which was completed within
21 three weeks. To put it simply, the delay was the government trial team and FBI agents’
22 fault. When CART began receiving requests from the FBI agents and prosecutors in
23 January 2021, it promptly fulfilled those requests.

24
25
26 ⁸ The three devices are identified as “black iPhone (model number A1660), barcode E6701411; yellow
27 iPhone, barcode E6701408; and mint green iPhone, barcode E4973575.” Dkt. 363 Ex. C ¶ 8.a (under
28 seal). Each of these three devices is listed in the table of the six digital devices seized at the Miami
airport on October 19, for which the government obtained a warrant on November 12, 2020. *Id.* ¶ 5
(table rows 5-7).

1 The government does not defend its failure to begin reviewing the devices,
2 instead pointing to the extension submission and conclusively stating “[the d]efendants
3 do not seriously challenge” the extension’s rationale. To be clear, the government is
4 wrong. The extension’s rationales do not stand up to any level of scrutiny, particularly
5 in a case in which the government was given 120 days instead of the more typical
6 60-day review period. *See, e.g., CDT III*, 621 F.3d at 1168-69 (noting that warrant gave
7 government computer personnel “a reasonable period of time not to exceed 60 days” to
8 complete responsiveness review of data seized from lab servers). The extension blames
9 two factors for its failure to complete (or even begin) the responsiveness reviews:
10 (1) CART and forensic processing; and (2) the filter review.

11 With respect to CART, the government’s March 4, 2021 submission complained
12 that CART’s forensic review “is time consuming. Agents cannot simply turn on
13 computers and review their contents because merely turning on a computer and
14 reviewing its contents changes the data on the computer. ... The review also must be
15 conducted by agents who have received specialized training to ensure that the review is
16 done thoroughly and in a forensically sound fashion. This process takes substantial
17 time.” Dkt. 363 Ex. C ¶ 8.b. As a result, there was “a backlog in the imaging and
18 review process” that was exacerbated by the CART forensic team’s resources being
19 “stretched due to the huge influx of devices that were seized during investigations
20 arising out of the January 6, 2021 insurrection at the U.S. Capitol in Washington, D.C.”
21 *Id.* ¶ 8.d. Those were the government’s sealed, ex parte representations. But here are
22 the actual facts:

- 23 • The government chose to execute search warrants at six homes on November 5,
24 2020 with the knowledge that an indictment had to be returned by November 17,
25 2020.
- 26 • The government chose to use a dragnet approach during those November 5, 2020
27 search warrant executions, seizing approximately 49 devices over objection.

- For the rest of November 2020, the government made no effort to process the November 5 devices.
- For all of December 2020, the government made no effort to process the November 5 devices, instead processing only the October 19 Miami devices from December 16-21, 2020 (Dkt. 363-7 at 2).
- The first request to process the November 5 devices produced in discovery occurred on January 4, 2021, two months after the warrants were executed. The majority of the November 5 devices appear to be processed in two days (January 11 and 27, 2021).
- The “four digital devices” highlighted by the government⁹ were processed and ready for review by January 27, 2021:

Device	Facts from Discovery
1B17	The request was not submitted until January 8, 2021. Ram Decl. Ex. B (DOJ_PROD_0000164355). The device was not delivered to CART until Jan. 14, 2021. Ram Decl. Ex. C (DOJ_PROD_0000163721). Processing took 163 minutes; completed on Jan. 27, 2021. Ram Decl. Ex. D (DOJ_PROD_0000163719).
1B21	No passcode; processing completed as part of the Jan. 11, 2021 batch. Ram Decl. Ex. E at 1-4 (DOJ_PROD_0000163697).
1B81	Processing took 69 minutes; completed on Jan. 27, 2021. Ram Decl. Ex. F (DOJ_PROD_0000163680).
1B85	Processing took 14 minutes; completed on Jan. 27, 2021. Ram Decl. Ex. G (DOJ_PROD_0000163663)

⁹ Opp’n at 3. The government focuses on “four digital devices” instead of the 49 digital devices it seized because at the end of April 2021, the government stated that it did not intend to use the remaining 45 digital devices.

- 1 • As of April 26, 2021, the government had not *begun* the responsiveness review
- 2 of any of these four devices. *See* Dkt. 391-5 (noting that the filter team had the
- 3 devices).
- 4 • Sometime between April 26, 2021 and May 26, 2021, the government’s trial
- 5 team lawyers conducted a responsiveness review.

6 The CART processing of these four devices was not requested until approximately
7 January 8, 2021 and it was completed by January 27, 2021. Yet somehow, the
8 responsiveness review had not even begun by April 26, 2021.

9 With respect to the government’s filter review excuse, that can be dismissed out
10 of hand. Ninth Circuit precedent has endorsed the practice of using a filter team to
11 conduct the responsiveness review, thereby obviating the need for a filter review. *See,*
12 *e.g., CDT III*, 621 F.3d at 1171-72 (noting that warrant required personnel uninvolved
13 in case to engage in responsiveness review and that this was an “important procedure”
14 “obviously designed to reassure the issuing magistrate that the government wouldn’t
15 sweep up large quantities of data”); *In re Search Warrant (Cunnius)*, 770 F. Supp. 2d
16 1138, 1149-50 (W.D. Wash. 2011) (denying search warrant application in large part for
17 failure to utilize independent filter team). The government chose to ignore the Ninth
18 Circuit’s advice as to best practices and it must live with the consequences. Moreover,
19 the government has failed to demonstrate that any filter review actually caused the
20 months-long delay in this case. From January 27 through April 26, the defendants
21 received no communications about a filter review of the devices, no requests for a list
22 of filter terms or lawyers, and no indications that certain devices were clearing filter
23 and being rolled to the responsiveness review team.¹⁰ The proposition of delay due to a
24 filter review makes no sense in light of the facts, which demonstrate that the

25
26 ¹⁰ Indeed, it would have been impossible for the trial team to select these four devices on April 26,
27 2021—which were not the only devices owned by the defendants and registered in their names—
28 unless they had already had access to the four devices’ contents. The trial team must have accessed
the four devices sometime before April 26 even though the filter team did not finish its purported
review until after that date.

1 government had pre-filter access to the devices' contents. Even if a filter review had
2 caused delay, however, it would be the government's fault for injecting an additional
3 layer of review that could otherwise be conducted simultaneously with the
4 responsiveness review consistent with Ninth Circuit's guidance. The government
5 decided to disregard Ninth Circuit guidance and did so contrary to the warrant's "as
6 soon as practicable" requirement. Now the government must live with the
7 consequences of its decision.

8 **2. The Government Violated the Warrants' Search Protocol** 9 **Requirement**

10 The Ninth Circuit has repeatedly encouraged judges to issue warrants requiring
11 search protocols designed to identify responsive documents without general rummaging
12 through electronic data. *CDT III*, 621 F.3d at 1179 (Kozinski, C.J., concurring); *accord*
13 *CDT II*, 579 F.3d at 999; *United States v. Phua*, No. 14-cr-249 et al., 2015 WL 1281603
14 (D. Nev. Mar. 20, 2015) ("The court will not approve a search warrant for
15 electronically stored information that does not contain an appropriate protocol
16 delineating what procedures will be followed to address these Fourth Amendment
17 issues."). The practice of engaging in a general review of the device's files "should not
18 be used without specific authorization in the warrant" *CDT III*, 621 F.3d at 1179.
19 A search protocol is "an explanation of the scientific methodology the government will
20 use to separate what is permitted to be seized from what is not, will explain to the Court
21 how the government will decide where it is going to search." *In re Apple iPhone, IMEI*
22 *013888003738427*, 31 F. Supp. 3d 159, 166 (D.D.C. 2014).

23 The search warrant in this case contained a search protocol requirement: a
24 defined search team was required to "conduct the search only by using search protocols
25 specifically chosen to identify only the specific items to be seized under the warrant."
26 Warrants Attach. B ¶ 4.b. Thus, the government did not need ongoing court-approval
27 for its protocol, but it did need to have a protocol and the protocol had to be geared
28 towards separating files and identifying only responsive files. In *United States v.*

1 *Bonner*, the court imposed a similar restriction, explaining that search protocols must be
2 “reasonably directed to identify data within the scope of the warrant” No. 12-cr-
3 3429, 2013 WL 3829404, at *19 (S.D. Cal. July 23, 2013). Because the government’s
4 protocols amounted to exploratory rummaging, the court held that the government
5 failed to adhere to the warrant and violated the Fourth Amendment. *Id.*

6 In this case, the government has not followed the search protocol requirement at
7 all. The government’s March 4 extension request misconstrued the search protocol
8 requirement to affect only the pre-responsiveness review activities. Extension App’n
9 ¶ 7, Dkt. 363 Ex. C (under seal). The government’s May 31 opposition ignored the
10 need for a search protocol requirement altogether, stating only “The government
11 reviewed the devices for documents that fall within the scope of the warrant.” Opp’n at
12 14. The government has effectively conceded that it failed to comply with the search
13 protocol requirement in the warrants. Suppression is therefore appropriate.

14 The government argues that its lack of a working search protocol does not
15 require suppression, relying on the First Circuit’s opinion in *United States v. Aboshady*,
16 951 F.3d 1 (1st Cir. 2020), a case in which no responsiveness review ever occurred and
17 the warrant imposed no search protocol requirement. Setting aside whether *Aboshady*
18 was correctly decided, it is completely inapplicable, because here the warrant *did*
19 *require a responsiveness review and a search protocol*.¹¹ Every seizure the government
20 made violated the warrants’ search protocol requirement because there was no search
21 protocol. Therefore, under the government’s own tortured logic, suppression is
22 merited.

23
24
25
26
27 ¹¹ The Ninth Circuit has not endorsed—and would never endorse—the warrant or law enforcement
28 practice in *Aboshady*, which permits permanent seizures of entire email accounts without a
responsiveness review. *See CDT III*, 621 F.3d at 1179 (noting that such rummaging is prohibited
absent specific authorization in the warrant).

1 **3. The Government Utilized Prosecutors Who Were Not Part of**
2 **the “Search Team” as Defined in ¶ 4.a of the Warrants**

3 The government concedes that prosecutors have conducted the responsiveness
4 review. *See* Opp’n at 14. The sole dispute is, therefore, whether the warrants’
5 definition of “the search team” (¶ 4.a) included the prosecutors.

6 The warrants are clear that only “the search team” will conduct the
7 responsiveness review: “In searching [t]he search team will conduct the search only
8 by using search protocols specifically chosen to identify only specific items to be seized
9 under this warrant. [¶]The search team may [list of permitted methods of executing
10 responsiveness review].” Warrants Attach. B ¶¶ 4, 4.b, 4.b.i-.iii. “The ‘search team’”
11 is a defined term meaning “law enforcement personnel” and “individuals assisting law
12 enforcement personnel.” *Id.* ¶ 4.a. If the search team determines that the device
13 contains data falling within the scope of the items to be seized, “the government” may
14 retain the entire device but may only access those items that have been seized. *Id.* ¶ 4.f.
15 “The review of the electronic data obtained pursuant to this warrant may include, *in*
16 *addition to law enforcement officers and agents* [i.e., the search team], attorneys for the
17 government,” including the prosecutors. *Id.* ¶ 5 (emphasis and bracketed text added);
18 *see also Giever v. City of Las Cruces*, No. 08-cv-155, 2010 WL 11626776, at *14
19 (D.N.M. Jan. 12, 2010) (prosecutor not considered a “law enforcement officer” under
20 state law); *United States v. Powell*, No. 19-cr-216, 2020 WL 2199758, at *2 (N.D. Ohio
21 May 6, 2020) (state law definition of “law enforcement officer” for warrant execution
22 purposes described as an officer or employee of an agency or subdivision with authority
23 to arrest individuals who violate the law); *cf.* Cal. Penal Code § 830.1 (defining “peace
24 officers” to include investigators in district attorneys’ offices and attorney general but
25 not the line prosecutors). The only constitutional option for an “independent review”
26 from the compulsory responsiveness review would be if it is a review of the *results* of
27 the responsiveness review, meaning a review of the data seized or obtained through the
28 responsiveness review. In essence, paragraph four mandates a responsiveness review

1 conducted by the search team (which does not include attorneys for the government)
2 and paragraph five says that the results may be given as a whole (unremarkably) to the
3 attorneys for the government. Neither paragraph says that the search team includes
4 attorneys for the government.

5 The warrants' exclusion of government attorneys from the responsiveness review
6 is consistent with Ninth Circuit guidance. In *CDT III*, two district court judges held
7 that the government had failed to adhere to an "important procedure in the warrant,
8 namely that 'computer personnel' conduct the initial review of the seized data and
9 segregate materials not the object of the warrant for return" 621 F.3d at 1171. The
10 *en banc* Court described this restriction with approval, noting that the use of a case
11 agent instead of a forensic specialist to conduct the responsiveness review "supports the
12 suspicion that representations in the warrant about the necessity for broad authority to
13 seize materials were designed to give the government access to the full list of
14 professional baseball players and their confidential drug testing records." *Id.* at 1172.

15 As here, the government in *CDT* argued that it did not violate the warrant
16 "because the warrant didn't specify that only computer personnel could examine the
17 seized files, and the case agent was therefore entitled to view them alongside the
18 computer specialist." *Id.* The Court rejected this argument as "sophistry," stating "[i]t
19 would make no sense to represent that computer personnel would be used to segregate
20 data if investigatory personnel were also going to access all the data seized. What
21 would be the point? ... the representation in the warrant that computer personnel would
22 be used to examine and segregate the data was obviously designed to reassure the
23 issuing magistrate that the government wouldn't sweep up large quantities of data in the
24 hope of dredging up information it could not otherwise lawfully seize. ... This was an
25 obvious case of deliberate overreaching by the government in an effort to seize data as
26 to which it lacked probable cause." *Id.*

27 Paragraph 4 of the warrants here spent twelve subparagraphs describing a
28 "search" executed by a defined "search team." Paragraph 5 provides that after the

1 investigating agency delivers a copy of all of the seized or copied data to the attorneys
2 for the government, government attorneys and others not contained within the
3 definition of the search team may engage in “independent review.” The government
4 argues that Paragraph 5 should be read as authorizing a second, independent
5 responsiveness review, separate and apart from the “search” conducted by the “search
6 team” in Paragraph 4. The government’s proposed reading of the warrant would
7 eviscerate that definition and implicitly expand the search team—without using the
8 word “search team” or even “search”—to include any government personnel assisting
9 in the investigation regardless of role. *Cf. CDT III*, 621 F.3d at 1171 (“One phrase in
10 the warrant cannot be read as eviscerating the other parts...”). A more logical reading
11 of the warrant is that—consistent with Ninth Circuit guidance—the warrant shields the
12 government attorneys from the raw, unfiltered devices and permits them to conduct an
13 “independent review” of the data that was “obtained pursuant to th[e] warrant,” i.e.,
14 obtained through the responsiveness review. *Id.* ¶ 5. As in *CDT III*, if the attorneys
15 were included in the search team executing the search warrant pursuant to ¶ 4.a, then it
16 would be pure sophistry to withhold them from the definition of “search team” and wait
17 until after ¶ 4.h dictates what occurs “[a]fter the completion of the search.”

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

20 The government does not argue that its conduct is distinct from the execution of
21 a general warrant. Instead, it argues that it is allowed to delay responsiveness reviews
22 until trial because “because the act of copying devices essentially “freezes” the
23 evidence in time.” Opp’n at 11. The government’s argument, if accepted, would mean
24 that law enforcement is free to execute general warrants.

25 The government’s argument begins with a flawed premise: “the objective of a
26 search warrant is to provide prosecutors with evidence to use at trial.” Opp’n at 14. It
27 is not. The objective of a search warrant is to make lawful the otherwise unlawful
28 seizure of private property for the purpose of an authorized investigation. More to the

1 point, the objective of a responsiveness review has nothing to do with trial evidence and
2 everything to do with protecting individual liberty. The objective of a responsiveness
3 review is to ensure that where Fourth Amendment rights are greatest—mass seizures of
4 private digital information—the government interests in things like trial evidence are
5 *not* paramount and are instead balanced against individual interests in privacy and
6 limiting government intrusions.

7 The en banc Ninth Circuit in *CDT III* provided on-point direction regarding the
8 purpose of responsiveness reviews: “The point of the *Tamura* procedures is to maintain
9 the privacy of materials that are intermingled with seizable materials, and to avoid
10 turning a limited search for particular information into a general search of office file
11 systems and computer databases.” 621 F.3d at 1170. The Ninth Circuit was
12 particularly concerned with the idea that the lack of stringent responsiveness review
13 rules would “create a powerful incentive for [law enforcement] to seize more rather
14 than less ... Let’s take everything back to the lab, have a good look around and see
15 what we might stumble upon. This would make a mockery of *Tamura* and render the
16 carefully crafted [warrant] safeguards in the Central District warrant a nullity. All three
17 judges below rejected this construction, and with good reason.” *CDT III*, 621 F.3d at
18 1170 (en banc).

19 The government’s requests for broad authorization “creates a serious risk that
20 every warrant for electronic information will become, in effect, a general warrant,
21 rendering the Fourth Amendment irrelevant.” *CDT III*, 621 F.3d at 1176. If the
22 government can seize whole digital devices and retain them until it has finished
23 selecting its trial evidence, then the government can execute general warrants on digital
24 devices. The wrongfulness of a general warrant is not that the government *gains*
25 *possession* of a broad swath of information; it is that the government can use *whatever*
26 *it wants from that broad swath* against the information’s owner. That wrongfulness is
27 baked into the government’s search warrant execution strategy in this case and merits
28 suppression.

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

The discovery dispute comes down to a sleight of hand by the government. During the May 21, 2021 hearing, the government argued to the Court that “the defendants have all of this information, because we made available the report of the phones ... a searchable report.”¹² This argument, however, rests on the government’s faulty premise that the request for the portions of those phones seized from the defendants is “essentially [a request to] identif[y] which documents we’re going to use at trial.” *Id.* at 39. The government is wrong. The production of 49 entire digital devices—terabytes worth of data without identification or individualized load files enabling file-specific review, more than any non-government counsel could possibly review—does not carry the government’s discovery obligation to produce the portions of those devices obtained by the trial team.

Rule 16’s plain text requires not just that the government produce whole items but that the government produce the “portions” of any items in the government’s possession, custody, or control that the government has “obtained from” the defendant or that are material to preparing the defense. Fed. R. Crim. P. 16(a)(1)(E)(i), (iii). The government cites to no precedent stating that it can produce 49 digital devices—even though it only seized (and thereby obtained) a “portion[]” of those files. *See* Mot. to Exclude at 15 (summarizing proceedings in *United States v. Sadr* that culminated in government’s agreement to forgo similarly late-identified portions based on Rule 16).

While no prejudice is necessary to enforce the Court’s Discovery Order, *see* Mot. to Exclude at 14-15 (collecting cases), the prejudice here is severe. The purpose of the Court’s discovery order was to ensure that the defense would have time to

¹² The reports are not functionally searchable. Due to the size of the reports (up to 60,000 pages), word searches cause computer crashes. The reports have therefore required linear review to the extent they have been reviewable at all. Regardless, the reports were produced as unlabeled needles in a haystack of 49 digital devices that were not identified by code, telephone number, or similar device-specific information. *See, e.g.*, Feb. 1, 2021 Discovery Ltr. (production of 20 digital devices without identifying information) (attached hereto as Ram Decl. Ex. H).

1 prepare for trial involving over 20 TB of discovery. The defense has spent months
2 preparing and just over two weeks before trial, the government dumps what it claims is
3 “overwhelming evidence” (Opp’n at 1) that was neither present in the indictment, used
4 in the grand jury, or cited in early descriptions of the case. The defense must therefore
5 pivot all of its resources at the last second and struggle to prepare for what has
6 effectively become a trial by ambush. The Court has discretion to prevent this and hold
7 the government to the evidence that it produced by the discovery deadline.

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

10 The government’s responsiveness review was conducted by the same lawyers
11 who were tainted by information derived from compelled statements months earlier.
12 *Kastigar* taint is like ink. It does not dissipate with time; it only spreads. The
13 government claims that it was not influenced in any way by its tainted impressions of
14 the case. Opp’n at 18. *Kastigar* is a “heavy burden” particularly because the
15 government must prove that the tainted information was effectively “obliterated from
16 the prosecutor’s mind,” and barring such proof, the prosecutor’s actions are tainted.
17 *United States v. McDaniel*, 482 F.2d 305, 312 (8th Cir. 1973); *United States v. Rice*,
18 421 F. Supp. 871, 876 (E.D. Ill. 1976) (noting that “even an unconscious reaction is not
19 permitted in cases of this nature”); *see also United States v. Harris*, 973 F.2d 333, 338
20 (4th Cir. 1992) (noting that even if total obliteration is not required, dismissal was
21 proper because tainted information “may have played some part” in the selection of
22 which files to review,” may have made the government “more likely to find [a
23 probative] file,” or may have aided the government in understanding the file); *United*
24 *States v. Mapes*, 59 M.J. 60, 70 (C.A.A.F. 2003) (noting need to scrutinize witness’s
25 “motives and state of mind in cooperation” due to potential effects from tainted
26 information). The government’s responsiveness review—conducted between April 26,
27 2021 and May 26, 2021 was irreparably tainted by months of exposure to tainted
28 information.

1 **III. CONCLUSION**

2 The Fourth Amendment's purpose is to prohibit general warrants. The Ninth
3 Circuit has warned of the "serious risk that every warrant for electronic information
4 will be come, in effect, a general warrant, rendering the Fourth Amendment irrelevant."
5 *CDT III*, 621 F.3d at 1176. The warrants in this case contained provisions meant to
6 mitigate that serious risk. The government failed to adhere to some provisions and
7 deceived the Court to evade other provisions while boxing the defendants out of the
8 process altogether. Exclusion of the seized evidence is the only remedy that will
9 impress upon the government that it must adhere to the terms of the warrants it secures.

10 Dated: June 7, 2021

Respectfully submitted,

11 /s/ Ashwin J. Ram

12 Ashwin J. Ram (SBN 227513)

13 *aram@steptoe.com*

14 Michael A. Keough (SBN 327037)

15 *mkeough@steptoe.com*

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

17 *mnewcomer@steptoe.com*

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

19 *nsilverman@steptoe.com*

20 **STEPTOE & JOHNSON LLP**

21 633 West Fifth Street, Suite 1900

22 Los Angeles, CA 90071

23 Telephone: (213) 439-9400

24 Facsimile: (213) 439-9599

25 *Counsel for Defendant Richard Ayvazyan*

26 [SIGNATURES CONTINUE
27 ON NEXT PAGE]
28

/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 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 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

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.