

1 TRACY L. WILKISON
Acting United States Attorney
2 SCOTT M. GARRINGER
Assistant United States Attorney
3 Chief, Criminal Division
SCOTT PAETTY (Cal. Bar No. 274719)
4 CATHERINE AHN (Cal. Bar No. 248286)
BRIAN FAERSTEIN (Cal. Bar No. 274850)
5 Assistant United States Attorneys
Major Frauds/Environmental and Community Safety Crimes Sections
6 1100/1300 United States Courthouse
312 North Spring Street
7 Los Angeles, California 90012
Telephone: (213) 894-6527/2424/3819
8 Facsimile: (213) 894-6269/0141
E-mail: Scott.Paetty@usdoj.gov
9 Catherine.S.Ahn@usdoj.gov
Brian.Faerstein@usdoj.gov

10 DANIEL S. KAHN
Acting Chief, Fraud Section
11 Criminal Division, U.S. Department of Justice
CHRISTOPHER FENTON
12 Trial Attorney, Fraud Section
Criminal Division, U.S. Department of Justice
13 1400 New York Avenue NW, 3rd Floor
Washington, DC 20530
14 Telephone: (202) 320-0539
Facsimile: (202) 514-0152
15 E-mail: Christopher.Fenton@usdoj.gov

16 Attorneys for Plaintiff
17 UNITED STATES OF AMERICA

18 UNITED STATES DISTRICT COURT

19 FOR THE CENTRAL DISTRICT OF CALIFORNIA

20 UNITED STATES OF AMERICA,

21 Plaintiff,

22 v.

23 RICHARD AYVAZYAN,
aka "Richard Avazian" and
24 "Iuliia Zhadko,"
MARIETTA TERABELIAN,
25 aka "Marietta Abelian" and
"Viktorika Kauichko,"
26 ARTUR AYVAZYAN,
aka "Arthur Ayvazyan," and
27 TAMARA DADYAN,
MANUK GRIGORYAN,
28 aka "Mike Grigoryan," and

No. CR 20-579(A)-SVW

GOVERNMENT'S MEMORANDUM IN
OPPOSITION TO MOTION TO EXCLUDE
DIGITAL DEVICE FILES FROM DEVICES
OBTAINED ON NOVEMBER 5, 2020
(ECF 363)

1 "Anton Kudiumov,"
2 ARMAN HAYRAPETYAN,
3 EDVARD PARONYAN,
4 aka "Edvard Paronian" and
5 "Edward Paronyan," and
6 VAHE DADYAN,
7
8 Defendants.

9 Plaintiff United States of America, by and through its counsel
10 of record, the Acting United States Attorney for the Central District
11 of California, Assistant United States Attorneys Scott Paetty,
12 Catherine S. Ahn, and Brian Faerstein, and Department of Justice
13 Trial Attorney Christopher Fenton, hereby files this memorandum in
14 opposition to defendants Richard Ayvazyan, Marietta Terabelian, Artur
15 Ayvazyan, and Tamara Dadyan's "motion to exclude digital device files
16 from devices obtained on November 5, 2020." (ECF 363.)

17 //

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

1 This opposition is based upon the attached memorandum of points
2 and authorities and exhibits, the files and records in this case, and
3 such further evidence and argument as the Court may permit.

4 Dated: May 31, 2021

Respectfully submitted,

5 TRACY L. WILKISON
6 Acting United States Attorney

7 SCOTT M. GARRINGER
8 Assistant United States Attorney
9 Chief, Criminal Division

10 /s/

11 SCOTT PAETTY
12 CATHERINE S. AHN
13 BRIAN FAERSTEIN
14 Assistant United States Attorneys

15 CHRISTOPHER FENTON
16 Trial Attorney, Department of
17 Justice

18 Attorneys for Plaintiff
19 UNITED STATES OF AMERICA
20
21
22
23
24
25
26
27
28

TABLE OF CONTENTS

<u>DESCRIPTION</u>	<u>PAGE</u>
TABLE OF AUTHORITIES.....	ii
MEMORANDUM OF POINTS AND AUTHORITIES.....	1
I. Introduction.....	1
II. Statement of Facts.....	2
A. The Search Warrants.....	2
B. The Government's Review and Production of Evidence from Digital Devices, Including the Four Digital Devices Subject to Defendants' Motion.....	3
C. Defendants' Prior Motions to Exclude Digital Evidence.....	7
III. Argument.....	7
A. The Length of the Government's Examination of the Digital Devices Was "Reasonable" under the Fourth Amendment.....	8
B. The Defendants' Process Argument Fails Because the Warrant Authorized Prosecutors to Participate in the Search of the Digital Devices.....	13
C. Defendants' Request for Exclusion Based on Rule 16 and the Court's Orders Is Frivolous.....	15
D. The Court has Already Ordered a Post-trial Kastigar Hearing.....	18
IV. Conclusion.....	18

TABLE OF AUTHORITIES

DESCRIPTION PAGE

CASES

<u>United States v. Aboshady</u> , 951 F.3d 1 (1st Cir. 2020).....	14, 15
<u>United States v. Burns</u> , No. 07 CR 556, 2008 WL 4542990 (N.D. Ill. Apr. 29, 2008).....	9, 11, 12
<u>United States v. Gorrell</u> , 360 F. Supp. 2d 48 (D.D.C. 2004).....	9
<u>United States v. Mutschelknaus</u> , 564 F. Supp. 2d 1072 (D.N.D. 2008).....	10
<u>United States v. Nepstead</u> , 424 F.2d 269 (9th Cir. 1970).....	10
<u>United States v. Stefanson</u> , 648 F.2d 1231 (9th Cir. 1981).....	11
<u>United States v. Syphers</u> , 426 F.3d 461 (1st Cir. 2005).....	10
<u>United States v. Triumph Capital Group, Inc.</u> , 211 F.R.D. 31 (D. Conn. 2002).....	10, 11, 12

STATUTES

Fed R. Crim. P. 41.....	11
-------------------------	----

MEMORANDUM OF POINTS AND AUTHORITIES

I. Introduction

There is overwhelming evidence of defendants' guilt contained in four smartphones that were lawfully seized from defendants' residences pursuant to warrants that this Court has already found to be constitutionally valid. The evidence includes digital photographs of fake identification documents and fraudulently obtained credit cards in the names of synthetic identities used to commit fraud; digital photographs of fraudulently submitted COVID-19 disaster relief loan applications; text messages between certain of the defendants detailing the manner and means of the charged conspiracies and schemes; and digital photographs of the templates used by defendants to create the fake identification documents, payroll reports, and tax forms used in furtherance of the fraud. (See, e.g., Declaration of Christopher Fenton ("Fenton Decl.") ¶¶ 1-4, Exs. 1-7 (examples of digital photographs seized from defendants' smartphones).)

The government produced a complete forensic copy of the four smartphones to the four defendants approximately four and a half months prior to the current trial so that the four defendants and their counsel could conduct their own examination of the smartphones. The government has also produced to all eight defendants summary reports of the contents that are searchable and organize the data by file type. The government has now completed its responsiveness review, approximately five weeks early, and produced to all eight defendants a follow-up report, showing which of the previously-disclosed discovery materials the government seized from these four smartphones. Tomorrow the government is producing to defendants, two

1 weeks before trial, a copy of the trial exhibits that the government
2 created using the evidence from the four smartphones belonging to
3 these four defendants, which are a subset of the materials that they
4 received in discovery months ago.

5 Facing overwhelming evidence and decades of imprisonment,
6 defendants resort to their now familiar tactic of demanding the Court
7 impose the drastic sanction of exclusion based on frivolous
8 allegations of prosecutorial misconduct. Defendants also ask the
9 Court to reconsider its prior opinions and orders finding that the
10 search warrants for the smartphones were constitutionally valid (ECF
11 296, 297), without providing a legitimate basis for the request or a
12 compelling reason for the Court to reconsider and reverse itself.
13 Defendants' motion is frivolous and meritless and should be denied.

14 **II. Statement of Facts**

15 **A. The Search Warrants**

16 On November 3, 2020, the United States obtained warrants to
17 search defendants' respective residences in Tarzana and Encino. (See
18 ECF 363, Ex. A, 2:20-MJ-05282, Ex. B, 2:20-MJ-05286.) Attachment B
19 to the warrants set forth detailed categories of items authorized to
20 be seized, including digital devices. The "search procedure" laid
21 out in the fourth paragraph of Attachment B authorized executing
22 parties to either search the digital devices on-site or "seize and
23 transport the device(s) and/or forensic image(s) thereof to an
24 appropriate law enforcement laboratory or similar facility to be
25 searched at that location." The "search procedure" also stipulated
26 that "[t]he search team shall complete the search as soon as is
27 practicable but not to exceed 120 days from the date of execution of
28 the warrant. The government will not search the digital device(s)

1 and/or forensic image(s) thereof beyond this 120-day period without
2 obtaining an extension of time order from the Court."

3 Of particular relevance to the defendants' motion, paragraph 5
4 of Attachment B specifically authorized prosecutors to participate in
5 the search of the electronic devices: "[t]he review of the electronic
6 data obtained pursuant to this warrant may be conducted by any
7 government personnel assisting in the investigation, who may include,
8 in addition to law enforcement officers and agents, attorneys for the
9 government, attorney support staff, and technical experts."
10 (emphasis added).

11 On November 5, 2020, federal agents executed the warrant and
12 recovered, among other things, dozens of digital devices, including
13 the four cellular telephones that are the subject of this motion
14 (hereinafter "the Four Digital Devices"). Rather than reviewing the
15 electronic materials on the premises, agents seized the devices, and
16 the FBI's Computer Analysis and Response Team ("CART") made digital
17 copies, which the warrants authorized.

18 **B. The Government's Review and Production of Evidence from**
19 **Digital Devices, Including the Four Digital Devices Subject**
20 **to Defendants' Motion.**

21 The government produced a complete forensic copy of each of the
22 digital devices to these four defendants so that their respective
23 counsel had timely access to all of the data on the devices and could
24 conduct their own review and examination. At the time the government
25 began producing these complete forensic copies to defendants, counsel
26 asked if the government had generated "reports" (e.g., using software
27 called Cellebrite) of the data contained on the devices. On January
28 4, 2021, the government explained that, after it produced to
defendants a copy of the complete forensic image, it would follow up

1 with a copy of any such Cellebrite reports if the government
2 generated such information: "We have not yet produced any of these
3 types of reports because the government has prioritized providing the
4 defense with complete forensic copies of the devices and therefore
5 has not yet completed its own review of the devices. We will produce
6 any discoverable reports generated as part of the government's review
7 of the devices once the government's review is complete and such
8 reports are generated." (Fenton Decl. ¶ 5, Ex. 8.) Defendants did
9 not seek any relief from this Court at that time.

10 When, in February 2021, the government began to produce these
11 Cellebrite reports to defendants (as the government said it would),
12 it explained that it had asked an independent filter team to review
13 the Cellebrite reports first for potentially privileged material
14 before they were made available to the prosecution team. (Fenton
15 Decl. ¶ 6, Ex. 9 (Feb. 26, 2021 Letter).) The government used an
16 independent filter team to review certain of the defendants' digital
17 devices, including the Four Digital Devices, both in an abundance of
18 caution and in recognition of defendant Richard Ayvazyan's claim
19 following the execution of a search warrant at his residence that he
20 possessed potentially privileged information. Because some of the
21 potentially privileged communications might have been in Armenian,
22 the independent filter team used an Armenian speaker to conduct the
23 review. Again, defendants did not seek any relief from this Court at
24 that time.

25 On March 4, 2021 the government sought and received its first
26 and only request for an extension of time to complete its search,
27 which allowed the government to continue searching up to and
28 including July 3, 2021. (See ECF 363, Ex. C, 2:20-MJ-05282.) The

1 government sought the extension using the same method it had used to
2 obtain the search warrants, namely by submitting an ex parte
3 application to the magistrate judge. In its submission, the
4 government explained that it had seized dozens of digital devices and
5 that more time was needed to complete its responsiveness review
6 because:

- 7 • as of that time, only three devices had been completely
8 processed and filter reviewed for privilege, and the
9 remaining digital devices were still being imaged and
10 processed by CART and reviewed by the filter team;
- 11 • the forensic review of digital devices was time consuming and
12 required specialized computer software and training, and, in
13 some cases, required additional time to decrypt encrypted
14 devices;
- 15 • the filter review process involved a thorough review of the
16 data contained on the devices to ensure that the
17 responsiveness review team was not tainted by the release of
18 privileged material; and
- 19 • the FBI CART team's resources had been stretched due to the
20 huge influx of devices that were seized during investigations
21 arising out of the January 6, 2021 insurrection at the U.S.
22 Capitol in Washington, D.C.

23 (See id.)

24 The government submitted its ex parte application under seal.
25 In its application to seal, the government explained to the
26 magistrate judge that its investigation had so far yielded an
27 indictment of four individuals in United States v. Ayvazyan, CR 20-
28 579-SVW, that the investigation was ongoing, and that the government
was evaluating whether to supersede to add more defendants and more
fraudulent loans. The government further disclosed to the magistrate
judge that the government had already produced a copy of the search
warrants to the four defendants in discovery, and requested that the
search warrants remain under seal and that the application be filed
under seal while the government completed its investigation and

1 sought additional charges:

2 The search warrants in this case remain under seal. The
3 affidavits have been produced to the defendants; however, this
4 production was subject to a protective order that restricts
5 their dissemination. If this application were made public
6 before any additional charging decisions can be made, there is a
7 significant risk that the case would be jeopardized by, among
8 other reasons, potentially alerting additional subjects that the
9 investigation is ongoing.

10 (See ECF 363, Ex. D, 2:20-MJ-05282.) The government's application
11 was granted, and the government was given until July 3, 2021 to
12 complete its responsiveness review.

13 The government subsequently decided to focus on one of the
14 digital devices belonging to each of the four original defendants and
15 selected the Four Digital Devices that are the subject of the instant
16 motion. (Fenton Decl. ¶ 7, Ex. 10 (Apr. 26, 2021 Letter).) The
17 complete forensic copy of the Four Digital Devices had already been
18 produced to defendants on February 1, 2021, so that defendants could
19 conduct their own examination. (ECF 363, Ex. F.) The independent
20 filter team then generated Cellebrite reports for each of the Four
21 Digital Devices and redacted from those reports any potentially
22 privileged communications. On April 30, 2021, as soon as the
23 independent filter team completed its review and released the
24 redacted Cellebrite reports to the prosecution team, the prosecution
25 team produced the reports to defendants. (Fenton Decl. ¶ 8, Ex. 11.)
26 The prosecution team then reviewed the Cellebrite reports for each of
27 the Four Digital Devices and identified the materials it intended to
28 seize pursuant to the search warrants. The prosecution team
29 completed its responsiveness review of these Four Digital Devices
30 approximately five weeks before the July 3 deadline. And on May 26,
31 2021, the government reproduced to defendants a further redacted copy

1 of the Cellebrite reports for each of the Four Digital Devices that
2 included only the limited subset of information it was seizing
3 pursuant to the search warrants. (Fenton Decl. ¶ 9, Ex. 12.)

4 **C. Defendants' Prior Motions to Exclude Digital Evidence**

5 On March 11, 2021, the defendants moved to suppress evidence
6 recovered from the Tarzana and Encino residences, including the Four
7 Digital Devices, on the ground that the warrants lacked particularity
8 and were overbroad. (ECF 146, 149.) Defendants also argued for
9 suppression of the evidence on the Four Digital Devices, among
10 others, based on their claim that the magistrate judge's extension of
11 time was invalid and that allowing the government to continue its
12 review violated the Court's discovery cutoff. (ECF 146 at 23-24; 149
13 at 11-12; ECF 222 at 14-15.) The Court denied defendants' motions,
14 ruling that the warrants were sufficiently particular and were not
15 overbroad, and rejecting defendants' arguments that the warrants had
16 been executed in an unreasonable manner. (ECF 296, 297.) Defendants
17 separately moved to exclude evidence based on allegations of undue
18 delay and prosecutorial misconduct. (ECF 248, ECF 289.) The Court
19 denied defendants' motions.

20 In the instant motion (ECF 363), defendants, once again, move
21 the Court to suppress the contents of the digital devices and raise
22 the same arguments that the Court already rejected.

23 **III. Argument**

24 Although styled as a "motion to exclude digital device files
25 from devices obtained on November 5, 2020," the defendants' pleading
26 is, in essence, another motion to suppress evidence that the Court
27 has already deemed to have been seized in compliance with the Fourth
28 Amendment. (See ECF 296). The defendants' pleading is lengthy and

1 the government finds the precise bases for suppression difficult to
2 ascertain. Nonetheless, it appears the defendants are making two
3 primary arguments for suppression: 1) the delay between the date that
4 the government seized the digital devices and when it examined their
5 contents renders the search "unreasonable" under the Fourth
6 Amendment; and 2) the search protocol that the government applied to
7 the devices was improper because prosecutors - not agents - searched
8 the devices for potential trial exhibits. Both arguments rely on
9 faulty factual and legal premises.

10 **A. The Length of the Government's Examination of the Digital**
11 **Devices Was "Reasonable" under the Fourth Amendment.**

12 Defendants argue that the Court should take the drastic action
13 of excluding overwhelming evidence of their guilt that is contained
14 on the Four Digital Devices because the government did not review the
15 data as soon as practicable. (ECF 363 at 5.) The government's
16 review, however, was timely because it sought and obtained in good
17 faith a court order extending the time to complete its responsiveness
18 review until July 3, 2021 - and then completed that review
19 approximately five weeks early.

20 Unable to dispute the fact of the extension, defendants instead
21 argue that the extension was "invalid." (ECF 363 at 5-6.)
22 Defendants do not seriously challenge the underlying reasons for why
23 the government requested a one-time extension.¹ Rather, defendants
24

25 ¹ For example, defendants assert - without any factual basis -
26 that the January 6, 2021 insurrection at the U.S. Capitol in
27 Washington, D.C. did not actually result in an increased workflow
28 that placed competing demands on the CART team's time and resources.
Baseless conjecture should not be credited in a motion seeking
drastic sanctions like the exclusion of overwhelming evidence of
guilt.

1 allege that the extension was "obtained by deceiving the Court."
2 (Id.) Like the myriad allegations of prosecutorial misconduct that
3 the Court has already considered and rejected, these allegations are
4 also without basis in fact.

5 Defendants' primary argument is that the government should have
6 told the magistrate judge about the Court's March 15 discovery cutoff
7 and the May 4 trial date. Defendants, however, fail to explain how
8 or why such information would have been material to the question
9 before the magistrate judge: whether the government had good cause
10 to request a one-time extension to complete its responsiveness review
11 based on the facts and circumstances. Moreover, the government
12 simply had nothing to hide from the magistrate judge. It had already
13 produced to defendants on February 1, 2021 a complete copy of the
14 forensic image of the Four Digital Devices so that defendants could
15 conduct their own examination and, at the time that the government
16 submitted its application on March 4, 2021, the District had not yet
17 resumed jury trials.

18 In any event, even putting aside the magistrate's order granting
19 an extension, any delay in completion of the government's review of
20 the digital evidence does not render the search "unreasonable" under
21 the Fourth Amendment because the passage of time did not result in an
22 expiration of probable cause. Neither the Fourth Amendment nor Rule
23 41 of the Federal Rules of Criminal Procedure places per se limits on
24 the duration of any forensic analysis, and the courts have upheld
25 forensic analysis begun months after investigators acquired a
26 computer or data. See United States v. Burns, No. 07 CR 556, 2008 WL
27 4542990, at *8-9 (N.D. Ill. Apr. 29, 2008) (ten month delay); United
28 States v. Gorrell, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) (same).

1 Rather than applying rigid time limits, courts assess whether delays
2 in forensic analyses were "reasonable" under the circumstances.
3 United States v. Mutschelknaus, 564 F. Supp. 2d 1072, 1077 (D.N.D.
4 2008).

5 The Ninth Circuit and other appellate courts view the
6 dissipation of probable cause as the chief measure of
7 "reasonableness" when assessing whether the length of a search
8 violated the Fourth Amendment. In United States v. Nepstead, for
9 example, the Ninth Circuit held that a search was "reasonable"
10 despite a delay in execution because the passage of time did not
11 impact the probable cause determination:

12 In the case before us, nothing, other than the passage
13 of time, occurred during the six-day period between
14 issuance and execution of the search warrant which
15 changed the facts upon which the original affidavit
16 was based and which gave the agents probable cause to
17 believe that articles subject to seizure were in the
house. And, on the facts before us, the passage of
time could not detract from probable cause because the
house was kept under surveillance for signs of
activity.

18 424 F.2d 269, 271 (9th Cir. 1970). In United States v. Syphers,
19 the First Circuit employed similar reasoning in assessing whether a
20 five-month delay in searching a computer already in police custody
21 attributable to a "backlog" at the laboratory rendered the search
22 "unreasonable." 426 F.3d 461, 469 (1st Cir. 2005). The panel ruled
23 that the "the five-month delay did not invalidate the search of
24 appellant's computer because there is no showing that the delay
25 caused a lapse in probable cause, that it created prejudice to the
26 defendant, or that federal or state officers acted in bad faith to
27 circumvent federal requirements." Id.; see also United States v.
28 Triumph Capital Group, Inc., 211 F.R.D. 31, 66 (D. Conn. 2002)

1 (“[t]he purpose of Fed R. Crim. P. 41(c)(1)’s time limitation is to
2 prevent a stale warrant”).²

3 Here, the defendants do not allege that passage of time negated
4 probable cause, nor can they. This is because the government had
5 probable cause on the day that it seized the devices, as the Court
6 held when it denied defendant’s prior motion to suppress evidence
7 from the premises searches. (ECF 296 at 18-22; ECF 297 at 2-6.)
8 Any delay in reviewing their contents in no way impacted the initial
9 probable cause determination. Delayed reviews of copied digital
10 evidence cannot impact the initial probable cause determination
11 because the act of copying devices essentially “freezes” the evidence
12 in time. Burns, 2008 WL 4542990 at *9 (“the delay [in reviewing
13 digital evidence] in this case was certainly lengthy and the
14 government does not give any reason for the delay. However, Burns
15 does not assert that the time lapse affected the probable cause to
16 search the computer (nor could he, given that suspected child
17 pornography had already been found on the hard drive), that the
18 government has acted in bad faith, or that he has been prejudiced in
19 any way by the delay, and the warrant does not specify a date by
20 which the search must have been conducted”); Triumph Capital, 211
21 F.R.D. at 66 (“when the mirror image was made within the ten-day
22 period the evidence was frozen in time. Thus, there was no danger
23

24 ² More broadly, violations of Rule 41 do not require suppression
25 unless: “(1) there was ‘prejudice’ in the sense that the search might
26 not have occurred or would not have been so abrasive if the rule had
27 been followed, or (2) there is evidence of intentional and deliberate
28 disregard of a provision of the Rule.” United States v. Stefanson,
648 F.2d 1231, 1235 (9th Cir. 1981) (magistrate judge’s failure to
record affiant’s oath in violation of Rule 41 did not warrant
suppression).

1 that probable cause ceased to exist during the search of the hard
2 drive"). As in Burns and Triumph Capital, the quality of the
3 evidence did not degrade as a result of the time it took to examine
4 the devices because the government made copies of the media. Unlike
5 some forms of physical evidence, the integrity of electronic evidence
6 does not decay with time, particularly in the short period at issue
7 here.

8 Beyond the absence of impact on the probable cause
9 determination, the defendants have not shown that the longevity of
10 the review prejudiced them. This is so for two reasons. First, the
11 government provided forensic copies of the entire devices to these
12 four defendants in discovery on February 1, 2021. See Triumph
13 Capital, 211 F.R.D. at 66 (noting that "[t]he defendants were given
14 copies of everything seized. This obviates the need for a detailed
15 inventory"). The government then followed up with a copy of
16 Cellebrite reports on April 30, 2021. Second, by virtue of the
17 court's order requiring production of an exhibit list by June 1,
18 2021, the government is required to disclose well in advance of trial
19 any items from the digital devices that it plans to offer in its
20 case-in-chief. In other words, the exhibit list will identify those
21 files extracted from the drives that are at issue.

22 The defendants try to demonstrate prejudice with a question:
23 "how can the defendants (without the resources of the federal
24 government) possibly be expected to complete an in-depth substantive
25 content review and prepare a defense while simultaneously processing
26 the other information the government has amassed?" The website of
27 Steptoe and Johnson, the international law firm that represents
28 defendant Richard Ayvazyan, suggests an answer. Specifically,

1 Steptoe's website touts its state of the art "Complex Litigation &
2 Discovery Center," which it says "bring[s] a wealth of e-discovery
3 experience and subject matter insight that comes from the successful
4 hands-on management of more than 300 document reviews" and which
5 employs sophisticated techniques such as "technology-assisted review"
6 and "email threading." See [https://www.steptoe.com/en/about/complex-](https://www.steptoe.com/en/about/complex-litigation-discovery-center.html)
7 [litigation-discovery-center.html](https://www.steptoe.com/en/about/complex-litigation-discovery-center.html). Given Steptoe's forensic resources
8 and defendants' likely already existing familiarity with the contents
9 of their own digital devices, defense counsel's attempts to assert
10 prejudice are not well taken.

11 **B. The Defendants' Process Argument Fails Because the Warrant**
12 **Authorized Prosecutors to Participate in the Search of the**
Digital Devices.

13 The defendants' brief seems to argue that the digital evidence
14 should be suppressed because prosecutors themselves are reviewing the
15 material to identify trial exhibits. According to the defendants,
16 this is a problem because "[the government's] attorneys [] are not
17 authorized members of the search team. . . ." (ECF 363 at 17.) To
18 the extent that the defense is suggesting that prosecutors are
19 prohibited from participating in the review of evidence obtained by a
20 search warrant, their proposition is, in a word, nonsense.

21 The "search procedure for digital devices" set out in the
22 warrant are perfectly contrary to the defendants' assertion that
23 prosecutors are not "authorized members of the search team."
24 Specifically, paragraph five of Attachment B to the warrant says
25 "[t]he review of the electronic data obtained pursuant to this
26 warrant may be conducted by any government personnel assisting in the
27 investigation, who may include, in addition to law enforcement
28 officers and agents, attorneys for the government, attorney support

1 staff, and technical experts." (Emphasis added). Even absent this
2 explicit authorization, it is common for prosecutors to participate
3 personally in the review of seized electronic evidence, and this
4 should come as no surprise given the objective of a search warrant is
5 to provide prosecutors with evidence to use at trial. The
6 information wall between prosecutors and agents posited by the
7 defendants would also have the undesirable policy consequence of
8 inhibiting searching agents from seeking legal advice from
9 prosecutors about whether or not particular evidence falls within the
10 scope of the warrant.

11 The defendants' assertion that "the government has jettisoned
12 the search protocol requirement altogether" has no basis in fact.
13 (ECF 363 at 17.) The government reviewed the devices for documents
14 that fall within the scope of the warrant. That the government is
15 identifying trial exhibits as part of this process is not a problem.
16 See United States v. Aboshady, 951 F.3d 1, 5 (1st Cir. 2020)
17 (government permitted to retain and search electronic data "in
18 preparation for trial"). This is because the documents that the
19 government intends to introduce at trial are merely a subset of the
20 scope of documents that Attachment B to the warrant authorizes the
21 government to "seize."

22 At any rate, the remedy for any errors in the search process is
23 exclusion of evidence that exceeded the bounds of the warrant, not
24 suppression of all information contained on the device at issue. As
25 the Court held in Aboshady, "[i]f the scope of the government's
26 search was too broad, Aboshady would only be entitled to suppression
27 of those emails that were introduced at trial and that reasonably
28 fell outside the scope of the warrant unless the lawful and unlawful

1 parts of the search are inextricably intertwined or where the lawful
2 part seems to have been a kind of pretext for the unlawful part.”
3 Id. at 9.

4
5 **C. Defendants’ Request for Exclusion Based on Rule 16 and the
6 Court’s Orders Is Frivolous.**

7 Defendants’ last-ditch effort to have the Court afford relief
8 that it previously denied should be rejected. Defendants’ request
9 based on Rule 16 and the Court’s orders is without basis in law or
10 fact and should be denied. The government has made good faith
11 efforts to comply with its discovery obligations in a timely manner,
12 and defendants have not been prejudiced in any way.

13 At the outset of the case, the government notified defendants of
14 the process it would use to promptly produce to them a forensic copy
15 of the dozens of digital devices it had seized so that defendants
16 could conduct their own examination. Defendants did not seek relief
17 from the Court. Consistent with its notice, the government promptly
18 produced a complete forensic copy of the Four Digital Devices (among
19 many others) to defendants by February 1, 2021. The government’s
20 production of this evidence was made approximately six weeks prior to
21 the discovery cutoff, and four and half months before trial.

22 Defendants do not and cannot demonstrate any prejudice based on this
23 record.

24 To the extent that steps were taken that may have delayed the
25 time when defendants would have otherwise received additional copies
26 of the data – in the form of Cellebrite reports – such steps were
27 taken to protect defendants’ privileges: an independent filter team
28 conducted a filter review, using an Armenian language specialist, to
respect and protect defendants’ potentially privileged

1 communications. Filtering foreign language documents for privilege
2 takes time.

3 Moreover, the government produced to defendants approximately
4 six weeks before trial a Cellebrite report summarizing the data
5 available from the complete forensic copies that the government had
6 produced months prior, and the government produced to defendants
7 nearly three weeks before trial a reproduction of the Cellebrite that
8 contains only the limited subset of data the government decided to
9 seized after it completed its responsiveness review. These reports
10 are searchable and organized by file type. In addition, the
11 government is producing to defendants two weeks before trial a copy
12 of the specific trial exhibits containing the evidence from the Four
13 Digital Devices that it intends to use at trial. Even had defendants
14 decided not to conduct their own examination of the complete forensic
15 copies that the government had produced four and half months before
16 trial, defendants had more than sufficient time to review the
17 Cellebrite reports produced in discovery well in advance of trial.

18 Defendants do not make a serious effort to argue how or why they
19 have been prejudiced based on the facts present here. Defendants
20 state only that "prejudice will occur in this case because the
21 addition of the seized data to the government's already large pool of
22 seizures, with only two weeks until trial, would make it potentially
23 impossible for the defendants to adequately prepare." (ECF 363 at
24 13-14.) Defendants' claim -- that the reproduction of a limited
25 subset of material, which they have already had in their possession,
26 negatively impacts their efforts to prepare for trial -- defies
27 common sense.

28 Finally, defendants argue, as they have done repeatedly during

1 the extensive litigation in this case, that they need not demonstrate
2 prejudice. (ECF 363 at 14.) But defendants still must proffer an
3 actual reason as to why, based on this record, the Court should take
4 extraordinary and drastic steps to exclude direct evidence of
5 defendants' involvement in serious crimes when that evidence has been
6 available to defendants and their counsel for months in advance of
7 trial. Defendants do not make such a showing because they cannot.

8 Moreover, none of the decisions on which defendants rely
9 actually support the drastic sanctions defendants seek here. In all
10 of the opinions defendants cite (ECF 363 at 14), the government had
11 access to the discovery at issue before the defendants. Here,
12 however, defendants had access to the discovery three months before
13 the government, because the government provided defendants with a
14 complete forensic copy of the Four Digital Devices on February 1 (per
15 defendants' request) and the government did not obtain access until
16 the end of April (after the contents had been reviewed by the
17 independent filter team to redact potentially privileged
18 communications). Moreover, none of the cases involved information
19 about which defendants had intimate knowledge - namely, the contents
20 of their own smartphones. To the contrary, the opinions and orders
21 relied on by defendants concerned the belated disclosure of
22 information known or knowable only to the government, such as
23 information relating to a government informant, expert witness,
24 witness list, co-defendant plea, or police reports. There is no
25 legal support for the extraordinary relief defendants seek.

1 **D. The Court has Already Ordered a Post-trial Kastigar**
2 **Hearing.**

3 The defendants suggest that the government's search of the
4 devices was somehow influenced by information compelled in violation
5 of Kastigar. (ECF 363 at 23). This is not so, and, at any rate, the
6 Court has already set a post-trial Kastigar hearing and
7 considerations of judicial economy counsel in favor of dealing with
8 all Kastigar arguments at that time.

9 **IV. Conclusion**

10 For the foregoing reasons, the Court should deny the motion
11 filed as ECF 363.

12 Dated: May 31, 2021

Respectfully submitted,

13 TRACY L. WILKISON
14 Acting United States Attorney

15 SCOTT M. GARRINGER
16 Assistant United States Attorney
 Chief, Criminal Division

17 /s/_____
18 SCOTT PAETTY
19 CATHERINE AHN
 BRIAN FAERSTEIN
 Assistant United States Attorneys

20 CHRISTOPHER FENTON
21 Department of Justice Trial Attorney
22 Attorneys for Plaintiff
23 UNITED STATES OF AMERICA
24
25
26
27
28