

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

* * *

UNITED STATES OF AMERICA,

Plaintiff,

v.

WEI SENG PHUA, et al.,

Defendants.

Case No. 2:14-cr-00249-APG-PAL

IN RE APPLICATION FOR SEARCH
WARRANT FOR DEVICE 1 KNOWN AS
AN APPLE IPAD MODEL A1455, SERIAL
NUMBER DLXJRF5DF19M

Case No. 2:15-mj-0262-PAL
Case No. 2:14-mj-0611-PAL

IN RE APPLICATION FOR SEARCH
WARRANT FOR DEVICE 2 KNOWN AS
AN APPLE IPHONE MODEL A1530, IMEI
NUMBER 358030059205968

Case No. 2:15-mj-0263-PAL
Case No. 2:14-mj-0612-PAL

IN RE APPLICATION FOR SEARCH
WARRANT FOR DEVICE 3 KNOWN AS
AN APPLE IPHONE MODEL A1530, IMEI
358030054212647

Case No. 2:15-mj-0264-PAL
Case No. 2:14-mj-0613-PAL

IN RE APPLICATION FOR SEARCH
WARRANT FOR DEVICE 4 KNOWN AS
AN APPLE IPAD MODEL A1432, SERIAL
NUMBER F87L6RPF196

Case No. 2:15-mj-0265-PAL
Case No. 2:14-mj-0614-PAL

IN RE APPLICATION FOR SEARCH
WARRANT FOR DEVICE 5 KNOWN AS
AN APPLE IPAD MODEL A1474, SERIAL
NUMBER DLXLL11JFK17

Case No. 2:15-mj-0266-PAL
Case No. 2:14-mj-0618-PAL

IN RE APPLICATION FOR SEARCH
WARRANT FOR DEVICE 6 KNOWN AS

Case No. 2:15-mj-0267-PAL
Case No. 2:14-mj-0619-PAL

1 AN APPLE IPAD MODEL A1454, SERIAL
2 NUMBER F4KK8049F196

3 The government submitted six ex parte search warrant applications to me on February 19,
4 2015. The applications seek search warrants directing Apple to assist the Federal Bureau of
5 Investigation in their search of four iPads and two iPhones seized in a search conducted on July
6 9, 2014, pursuant to a search warrant issued by the Honorable Nancy J. Koppe. Judge Koppe
7 issued a warrant authorizing the search of Villas 8881, 8882 and 8888 at Caesars Palace under
8 Case No. 2:14-mj-0458-NJK. The warrant authorized the search and seizure of evidence
9 including all cell phones, Blackberries, iPhones, iPads and other electronic devices, laptop and
10 desktop computers and other specified computer equipment and peripheral devices.

11 I reviewed these six search warrant applications, decided not to issue them, and had staff
12 notify the government counsel of my decision. Government counsel requested a meeting to
13 explain the government's position that these warrants should be issued. I declined to conduct an
14 ex parte meeting with the AUSA who submitted the warrants because these warrants pertain to a
15 criminal case to which I am assigned and will be responsible for addressing any additional
16 pretrial motions or other matters referred automatically or by order of the district judge. This
17 order is entered to explain why I declined to authorize the search warrants requested, and to
18 allow the government to appeal my decision to the district judge.

19 The caption of this order contains the case numbers issued to the search warrants issued
20 in September 19, 2014, for these same six devices as well as the case numbers issued for these
21 six devices when new warrants were submitted to me on February 19, 2015. The government
22 did not reapply for search warrants for five devices recovered from Villas 8882 and 8888, which
23 the court authorized under Case Nos. 2:14-mj-0609-PAL, 2:14-mj-0610-PAL, 2:14-mj-0615-
24 PAL, 2:14-mj-0616-PAL and 2:14-mj-0617-PAL.

25 **BACKGROUND**

26 **I. The September 19, 2014, Search Warrants.**

27 On September 19, 2014, I issued eleven search warrants for eleven devices recovered from
28 Villas 8881, 8882 and 8888. The initial eleven applications for search warrants were supported
by the affidavit of Task Force Officer ("TFO") Matthew Downing. The affidavit supporting the

1 search warrant application for all eleven devices was identical except for identifying the Villa
2 from which the devices were recovered. The purpose of the applications for the warrants for all
3 eleven devices was to require Apple to assist the FBI in their search of the devices which were
4 passcode protected. The government requested and received judicial authorization to require
5 Apple to provide reasonable technical assistance, if the devices were in reasonable working
6 order, to unlock the passcode protection, and to the extent possible, extract data from the devices.
7 The government requested and received judicial authorization for Apple to copy the data from
8 the devices onto an external hard drive or other storage medium. The initial applications
9 provided that Apple would return the storage medium containing copied data to the FBI. Upon
10 return, the devices would be impounded into evidence, the copied data would be searched for
11 evidence of the enumerated crimes eventually charged in the indictment, in accordance with the
12 provisions of a search warrant protocol described in Attachment C to the warrants and in
13 compliance with the provisions of Rule 41 of the Federal Rules of Criminal Procedure.

14 The affidavit of TFO Downing supporting the warrants attached a copy of Judge Koppe's
15 earlier warrant to support the statement of probable cause. The government also applied for and
16 received an order sealing the affidavits and warrants based on the government's assertion "that
17 disclosure of the information might possibly jeopardize the investigation" and that the
18 government's "right to secrecy far outweighs the public's right to know."

19 Task Force Officer Downing executed certified search warrant returns for all eleven
20 warrants on October 2, 2014, to chambers as is our local practice. The returns indicated the
21 warrants were executed on Apple on September 22, 2014. The returns also indicated that Apple
22 did not "honor" the search warrant issued under Case No. 2:14-mj-0617-PAL because the
23 warrant contained an incorrect serial number for the device described. With respect to the
24 remaining ten, the search warrant returns indicated Apple advised it would take approximately
25 nine months to extract data from the devices.

26 **II. The February 19, 2015, Applications for Search Warrants.**

27 These six applications for search warrants were submitted to me rather than the magistrate
28 judge on criminal duty. When chambers inquired why the warrants were submitted to me, staff

1 was advised that the warrants were “piggy back”¹ search warrant applications following up on
2 prior search warrants I had issued. The practice in this district is for the duty magistrate judge to
3 handle any search warrant applications which are made during that judge’s duty week. However,
4 the custom and practice in this district is to present a “piggy back” warrant to the judge who
5 issued the original warrant on which the supplemental application depends.

6 **III. Disclosures at February 6, 2015, Hearing.**

7 I set a status and case management conference in the criminal case on February 6, 2015,
8 after issuing reports and recommendations concerning motions to suppress filed by the
9 Defendants in this case. At the hearing, the parties advised me that they had reached agreements
10 concerning briefing deadlines for objections to the three pending reports and recommendations.
11 I addressed counsel concerning whether additional pretrial motions would be filed and the status
12 of discovery that may impact setting a realistic trial date. Government counsel stated that the
13 government was in the process of conducting forensic review of computers and electronic
14 devices and would be supplementing discovery as additional information became available.
15 Government counsel stated that it had been informed by Apple that Apple would need
16 approximately nine months to assist the government in its attempts to access and copy Apple
17 devices.

18 Counsel for both sides had indicated that they were mutually requesting an April 13,
19 2015, trial date. When government counsel disclosed on the record that it needed Apple’s help
20 to access and copy certain devices, I asked government counsel whether they had requested and
21 received judicial authorization for Apple’s assistance in this regard. AUSA Silva confirmed the
22 government had obtained judicial authorization for Apple’s assistance on the record. Counsel for
23 the Defendants responded that they were unwilling to continue the trial date for the nine month
24 period Apple stated it needed to assist in the government’s forensic examination efforts.

25 ///

26 ///

27 _____
28 ¹ A piggy back warrant is a search warrant that relies upon or follows up on a prior warrant
which is typically attached to the new application.

1 **IV. Orders Sealing September 19, 2014, Warrants.**

2 The eleven applications and warrants remain under seal. However, the court finds that
3 there is no longer any justification for maintaining these warrants under seal for several reasons.
4 First, the government disclosed the existence of these warrants in open court. Second, the
5 Defendants are aware from prior search warrant returns produced in discovery in this criminal
6 case that all of these devices were seized pursuant to the search warrant Judge Koppe issued on
7 July 9, 2014. Third, these devices were all listed as items subject to forfeiture in the indictment.
8 Fourth, the affidavit and application supporting the search warrants attached Judge Koppe's
9 earlier search warrant. This is the search warrant that resulted in the motions to suppress, four
10 days of evidentiary hearings, and my reports of findings and recommendations. It is the same
11 warrant I have found was fatally flawed and lacked probable cause to support the search of Villa
12 8882. Under these circumstances, the government's unsupported statement that disclosure of the
13 information in the search warrants "might possibly jeopardize the investigation" and that the
14 government's "right to secrecy far outweighs the public right to know" do not support
15 maintaining the applications and warrants under seal. For the same reasons, the court will deny
16 the government's request to seal the affidavit and applications for the six devices submitted to
17 me on February 19, 2015.

18 **DISCUSSION**

19 The government's February 19, 2015, applications for search warrants to require Apple to
20 provide reasonable technical assistance, if the devices are in reasonable working order, to unlock
21 the passcode protection and to the extent possible, extract data from the devices, are denied for
22 the reasons explained below.

23 First, the amended affidavits in support of the applications for search warrants do not
24 state probable cause. The amended affidavit was submitted by Thayne A. Larson, a Special
25 Agent of the FBI who is one of several agents participating in this investigation. Paragraph 6 of
26 the affidavit submits that there is probable cause to believe that all six devices contain evidence,
27 fruits, instrumentalities, or proceeds of the target offenses. The target offenses are described as
28 violations of 18 U.S.C. § 1955 – Operating an Illegal Gambling Business; 18 U.S.C. § 1084 –

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 Paragraph 10 attests that eight Defendants were indicted for transmission of
2 wagering information, illegal gaming, and aiding and abetting in violation of federal law on July
3 29, 2014. A court deciding whether to issue a search warrant must determine whether the
4 warrant states probable cause that a crime had been committed, and that the property to be
5 searched will contain evidence of the criminal offenses from the information provided within the
6 four corners of the search warrant application. The fact that the grand jury indicted the
7 Defendants does not state probable cause for issuance of a search warrant. The grand jury found
8 probable cause based on whatever evidence was presented to it. The court has no way of
9 knowing what evidence was submitted to the grand jury and may not simply find that because
10 the grand jury found probable cause to believe the Defendants committed a criminal offense and
11 that the devices listed in the indictment should be forfeited, that probable cause exists to believe
12 the devices contain evidence of the crimes.

13 Paragraph 11 indicates that one Defendant pled guilty to a felony charge of transmission
14 of wagering information, four Defendants pled guilty to a Class A misdemeanor of accessory
15 after the fact to transmission of wagering information, and the case against a sixth Defendant was
16 dismissed. The affidavit does not state who admitted to doing what, whether any of the
17 Defendants who pled guilty implicated the Phuas in illegal gaming activity, where the illegal
18 gambling business was being conducted, how the illegal gaming activity was being conducted, or
19 the role played by each individual charged. The affidavit contains no facts indicating the six
20 devices recovered from Villa 8881 and 8888 were used to commit the enumerated offenses, or
21 what facts law enforcement has to believe the devices may contain evidence of the enumerated
22 offenses.

23
24
25
26
27
28

1 things for which there is probable cause to search, the particularity requirement ensures that the
2 search will be carefully tailored to its justifications, and will not become a wide-ranging,
3 exploratory search the Fourth Amendment prohibits. The scope of a lawful search is defined by
4 the object of the search. *Id.* The test is an objective one: would a reasonable officer have
5 interpreted the warrant to permit the search at issue. *United States v. Gorman*, 104 F. 3d 272,
6 274 (9th Cir. 1996).

7 Search warrants must be specific. *United States v. Hill*, 459 F.3d 966, 973 (9th Cir.
8 2006). “Specificity has two aspects: particularity and breadth. Particularity is the requirement
9 that the warrant must clearly state what is sought. Breadth deals with the requirement that the
10 scope of the warrant be limited by the probable cause on which the warrant is based.” *Id.* The
11 description of items need only be reasonably specific, rather than elaborately detailed. *Id.* In
12 determining whether a warrant is sufficiently particular, the Ninth Circuit

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 There is a well-developed body of Fourth Amendment law addressing the search and
2 seizure of large quantities of materials to review and sort the material for items within the scope
3 of probable cause underlying warrants. For example, in *Anderson v. Maryland*, 427 U.S. at 482
4 n.11, the Supreme Court recognized that “in searches for papers, it is certain that some innocuous
5 documents will be examined, at least cursorily, in order to determine whether they are, in fact,
6 among those papers authorized to be seized.”

7 The Ninth Circuit has exhaustively addressed search warrants for computer and
8 electronically stored information in a series of decisions involving grand jury investigations into
9 illegal steroid use by Major League baseball players. Three published decisions culminated in an
10 *en banc* decision in *United States v. Comprehensive Drug Testing, Inc.*, 621 F. 3d 1162 (9th Cir.
11 2010) (“*CDT III*”). There, the Ninth Circuit recognized that data individuals used to keep in the
12 file cabinets in physical facilities are now usually stored electronically, and law enforcement
13 faces many challenges in retrieving electronically stored information. *Id.*, at 1175. “Electronic
14 storage facilities intermingle data, making them difficult to retrieve without a thorough
15 understanding of the filing and classification systems used—something that can often only be
16 determined by closely analyzing the data in a controlled environment.” *Id.* Because of these
17 challenges, the Ninth Circuit recognized that law enforcement’s legitimate need to seize large
18 quantities of data is an inherent part of the electronic search process. *Id.*, at 1177. However, the
19 legitimate need of law enforcement for authorization to examine large quantities of electronic
20 records “creates a serious risk that every warrant for electronic information will become, in
21 effect, a general warrant, rendering the Fourth Amendment irrelevant.” *Id.*, at 1176.

22 To address these concerns, *CDT III* updated its earlier decision in *United States v.*
23 *Tamura*, 694 F.2d 591 (9th Cir. 1982) “to apply to the daunting realities of electronic searches.”
24 *Id.*, at 1177. *Tamura* preceded the dawn of the information age and involved the seizure of
25 several boxes and dozens of file drawers of paper documents to be stored off site for documents
26 the search warrant authorized later. *CDT III* made it clear that the procedural safeguards outlined
27 in the *Tamura* opinion have “provided a workable framework for almost three decades” and
28 should be applied to the realities of electronic searches. Specifically, the Court of Appeals

1 reiterated that wholesale seizure of voluminous documents to be sorted out for documents a
2 search warrant authorizes the government to seize may sometimes be necessary. Although often
3 necessary, the Ninth Circuit continues to disapprove of the wholesale seizure of documents,
4 particularly where the government fails to return materials that were not the object of the search
5 once they have been segregated. *Id.*

6 With respect to electronically stored information, *CDT III* called upon magistrate judges
7 issuing search warrants to apply *Tamura* procedures to electronically stored information “to
8 maintain the privacy of materials that are intermingled with seizeable materials, and to avoid
9 turning a limited search for particular information into a general search of office file systems in
10 computer databases.” *Id.*, at 1170. Because of the unique problems inherent in the electronic
11 search process, judicial officers should exercise greater diligence “in striking the right balance
12 between the government’s interests in law enforcement and the right of individuals to be free
13 from unreasonable searches and seizures.” *Id.*, at 1177. The Ninth Circuit concluded that “the
14 process of segregating electronic data that is seizeable from that which is not must not become a
15 vehicle for the government to gain access to data which it has no probable cause to collect.” *Id.*

16 The court will not approve a search warrant for electronically stored information that
17 does not contain an appropriate protocol delineating what procedures will be followed to address
18 these Fourth Amendment issues. A protocol for forensic review of a device that stores data
19 electronically must make reasonable efforts to use methods and procedures that will locate and
20 expose those categories of files, documents, or other electronically stored information that are
21 identified with particularity in the warrant, while minimizing exposure or examination of
22 irrelevant, privileged, or confidential files to the extent reasonably practicable.

23 Third, according to Special Agent Larson’s ame
24
25
26
27
28

1 before they will assist the government in accessing the devices and downloading the information
2 is not a basis for this court to issue one. If, as the government claims, all six devices have been
3 forfeited by those who had any interest in them, it would have been a simple matter for the
4 government to require the prior owners of the devices to provide the government with the
5 passcodes as a condition of their plea agreements.

6 Fourth, as stated earlier, the affidavit is inaccurate in stating that I suppressed any
7 evidence in this case. I made recommendations that are now before the district judge who may
8 adopt, modify, or overrule some or all of the recommendations. I found that the July 9, 2014,
9 search warrant supporting the search of all three Villas was fatally flawed. I did not make a
10 the(guiltydidET/C3D.0009 Tc.1342 T04(the aB the)TJnce intiary h ofupprom)TJ two19.8457.66.000

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 new search warrants because of my findings and recommendations under either the independent

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28