

1 EILEEN M. DECKER
United States Attorney
2 PATRICIA A. DONAHUE
Assistant United States Attorney
3 Chief, National Security Division
TRACY L. WILKISON (California Bar No. 184948)
4 Chief, Cyber and Intellectual Property Crimes Section
Assistant United States Attorney
5 1500 United States Courthouse
312 North Spring Street
6 Los Angeles, California 90012
Telephone: (213) 894-2400
7 Facsimile: (213) 894-8601
Email: Tracy.Wilkison@usdoj.gov

8 Attorneys for Applicant
9 UNITED STATES OF AMERICA

10 UNITED STATES DISTRICT COURT
11 FOR THE CENTRAL DISTRICT OF CALIFORNIA

12 IN THE MATTER OF THE SEARCH
OF AN APPLE IPHONE SEIZED
13 DURING THE EXECUTION OF A
SEARCH WARRANT ON A BLACK
14 LEXUS IS300, CALIFORNIA
LICENSE PLATE #5KGD203

ED No. CM 16-10 (SP)

SUPPLEMENTAL DECLARATION OF
CHRISTOPHER PLUHAR IN SUPPORT
OF GOVERNMENT'S REPLY IN
SUPPORT OF MOTION TO COMPEL
AND OPPOSITION TO APPLE INC.'S
MOTION TO VACATE ORDER

Hearing Date: March 22, 2016
Hearing Time: 1:00 p.m.
18 Location: Courtroom of the
19 Hon. Sheri Pym

SUPPLEMENTAL DECLARATION OF CHRISTOPHER PLUHAR

I, Christopher Pluhar, declare and state as follows:

1. I am a Supervisory Special Agent (“SSA”) with the FBI, and I have knowledge of the facts set forth herein and could and would testify to those facts fully and truthfully if called and sworn as a witness.

A. The Subject Device Was Off When Seized

2. In paragraph 8 of my declaration dated February 16, 2016 (the “Initial Declaration”), I explained that the Subject Device was “locked” because it presented a numerical keypad with a prompt for four digits. To add further detail, on December 3, 2015, the same day the Subject Device was seized from the Lexus IS300, I supervised my Orange County Regional Computer Forensics Laboratory (“OCRCFL”) team who performed the initial triage of the Subject Device, and observed that the device was powered off, and had to be powered up, or booted, to conduct the triage. Upon power-up, we observed that the device was protected with a four-digit passcode (because it displayed a number pad with four spaces), and was running iOS9. I confirmed with two FBI Evidence Response Team agents that the device was found in the center console of the Lexus IS300 described in the search warrant, and that it was found there powered off.

B. Accessing the iCloud Back-Ups

3. As described in paragraphs 5 and 6 of my Initial Declaration, after the shootout on December 2, 2016, the Subject Device was seized pursuant to the search warrant on December 3, 2016. After case agents and forensic examiners from the OCRCFL met with personnel (including Information Technology (“IT”) personnel) from the San Bernardino County Department of Public Health (“SBCDPH”), I then met personally on December 6, 2015 with IT specialists at the SBCDPH to gather more information about the Subject Device and the SBCDPH account(s) associated with the Subject Device. I learned from SBCDPH personnel that the department had deployed a mobile device management (“MDM”) system to manage its recently issued fleet of iPhones, that the MDM system had not yet been fully implemented, and that the

1 necessary MDM iOS application to provide remote administrative access had not been
2 installed on the Subject Device. As a result, SBCDPH was not able to provide a method
3 to gain physical access to the Subject Device without Farook's passcode.

4 4. As described in paragraph 7 of my Initial Declaration, the Subject Device is
5 owned by SBCDPH. I learned from SBCDPH IT personnel that SBCDPH also owned
6 the iCloud account associated with the Subject Device, that SBCDPH did not have the
7 current user password associated with the iCloud account, but that SBCDPH did have
8 the ability to reset the iCloud account password.

9 5. Without the Subject Device's passcode to gain access to the data on the
10 Subject Device, accessing the information stored in the iCloud account associated with
11 the Subject Device was the best and most expedient option to obtain at least some data
12 associated with the Subject Device. With control of the iCloud account, the iCloud
13 back-ups of the Subject Device could be restored onto different, exemplar iPhones,
14 which could then be processed and analyzed.

15 a. As described in Apple's security documentation, a "passcode" is a
16 component of the encryption key that protects the device itself, which is distinct from the
17 "password" associated with an Apple ID needed to access Apple's Internet Services,
18 such as iCloud. *See* Apple's iOS Security for iOS 9.0 (Sept. 2015) ("iOS Security")
19 attached to the Declaration of Nicola T. Hanna as Exhibit K; *id.* at 11-12 (describing
20 passcode's role in creating device's class key); *id.* at 38 (describing different password
21 requirements for Apple ID needed for Apple's Internet Services); *id.* at 41 ("Users set up
22 iCloud by signing in with an Apple ID"). Each iCloud account is associated with a
23 specific Apple ID.

24 b. Therefore the *password* necessary to access the iCloud account
25 associated with the Subject Device is unrelated to the *passcode* needed for physical
26 access to the Subject Device itself.

27 6. While in discussions with SBCDPH IT personnel, I also spoke with Lisa
28 Olle, attorney for Apple Inc. Ms. Olle provided me various pieces of useful information

1 about the iCloud account associated with the Subject Device, including information
2 about the existing back-ups, confirmation that the entire iCloud account had already been
3 preserved by Apple in response to an FBI request for preservation, and that the remote-
4 wipe function was not activated for the Subject Device. Ms. Olle advised that once the
5 search warrant was received by Apple, there would be an unknown time delay for Apple
6 to provide the Subject Device iCloud account data.

7 7. After that conversation with Ms. Olle, and after discussions with my
8 colleagues, on December 6, 2015, SB CDPH IT personnel, under my direction, changed
9 the password to the iCloud account that had been linked to the Subject Device. Once
10 that was complete, SB CDPH provided exemplar iPhones that were used as restore
11 targets for two iCloud back-ups in the Subject Device's iCloud account. Changing the
12 iCloud password allowed the FBI and SB CDPH IT to restore the contents of the oldest
13 and most recent back-ups of the Subject Device to the exemplar iPhones on December 6,
14 2015. Once back-ups were restored, OCRCFL examiners processed the exemplar
15 iPhones and provided the extracted data to the investigative team. Because not all of the
16 data on an iPhone is captured in an iCloud back-up (as discussed further below), the
17 exemplar iPhones contained only that subset of data as previously backed-up from the
18 Subject Device to the iCloud account, not all data that would be available by extracting
19 data directly from the Subject Device (a "physical device extraction").

20 **C. Not All Data on an iPhone is Backed Up to the iCloud**

21 8. Subsequently, a search warrant was issued on January 22, 2016, to obtain
22 the preserved contents of the Apple ID and iCloud account associated with the Subject
23 Device. Review of the iCloud search warrant results that were received from Apple on
24 January 26, 2016 is ongoing, but review of this data is difficult compared to the data
25 restored to the exemplar iPhones due to the manner in which it has been formatted and
26 delivered by Apple.

27 9. The results of the iCloud search warrant confirm that the last Subject
28 Device back-up to the iCloud account was on October 19, 2015 (approximately 6 weeks

1 before the December 2, 2015 attack in San Bernardino), as stated in paragraph 8 of my
2 Initial Declaration. According to the logs contained in those results, on October 22,
3 2015, it appears that the “iForgot” web-based password change feature was used for the
4 account associated with the Subject Device. I know based on my experience, and review
5 of Apple’s website, that “iforgot.apple.com” provides iCloud customers with the ability
6 to reset the password associated with their iCloud account over the Internet.

7 10. Regarding iCloud back-ups, I know from training and experience as a
8 mobile device forensic examiner, and consultation with other FBI technical experts that,
9 in general, cloud-based back-ups of physical devices contain only a subset of the data
10 that is typically obtained through physical device extractions.

11 a. For example, with iCloud back-ups of iOS devices (such as iPhones
12 or iPads), device-level data, such as the device keyboard cache, typically does not get
13 included in iCloud back-ups but can be obtained through extraction of data from the
14 physical device. The keyboard cache, as one example, contains a list of recent
15 keystrokes typed by the user on the touchscreen. From my training and my own
16 experience, I know that data found in such areas can be critical to investigations.

17 b. I also know that the Apple iOS allows users to change settings on the
18 device to exclude certain apps from including their user data in iCloud back-ups, but the
19 user data associated with apps excluded from iCloud back-ups by the user may still be
20 obtained via physical device extraction.¹ I consulted with an OCRCFL examiner who
21 reviewed the exemplar iPhones that were used as restore targets for the iCloud back-ups
22 of the Subject Device. Each of the restored exemplars includes restored settings, and
23 those settings showed that, for example, iCloud back-ups for “Mail,” “Photos,” and
24 “Notes” were all turned off on the Subject Device.

25 11. For these reasons, iCloud back-ups as currently implemented are not
26


27 ¹ I also know that developers of iOS apps have the ability to design their apps to
28 specifically exclude app user data from iCloud back-ups, but the user data associated
with those apps may still be obtained via physical device extraction.

1 considered a comprehensive method of extracting all available stored data from an iOS
2 device. For iOS devices, as well as other mobile device platforms, back-ups such as
3 those made to iCloud can provide valuable evidence, but forensic examiners rely on
4 physical device extractions to obtain the most data available from mobile devices.
5 Therefore, even if it had been possible, via any means, to initiate a fresh iCloud back-up
6 of the Subject Device, so that it included information through December 2, 2015, the FBI
7 would still need to conduct a physical device extraction of the Subject Device in order to
8 obtain all potential evidence from the Subject Device.

9 12. Before seeking the February 16, 2016, Order, in a phone conversation of
10 which I was a part, the government explained to Lisa Olle and Erik Neuenschwander,
11 among others from Apple, in detail its proposal for technical assistance including
12 specifics of the three desired functions and how they might be achieved as embodied in
13 the Order. After hearing the government's proposal, the Apple representatives declined
14 to discuss the feasibility of the government's proposal and instead provided a list of
15 alternative ways the government might be able to access some of the data on the Subject
16 Device. Although the FBI had already explored these avenues, I, and others from the
17 technical team re-explored them at the suggestion of Apple representatives. We again
18 determined that none provided any means to access the full set of data on the Subject
19 Device. In a subsequent phone conversation with Erik Neuenschwander and Lisa Olle,
20 we explained that the alternatives they had suggested did not work. Erik
21 Neuenschwander and Lisa Olle declined to discuss the feasibility of the government's
22 proposal as embodied in the Order.

23 I declare under penalty of perjury under the laws of the United States of America
24 that the foregoing is true and correct and that this declaration is executed at

25 California, on March 9, 2016.

26
27 
28 Christopher Pluhar
Supervisory Special Agent
Federal Bureau of Investigation