Case [redacted]

EILEEN M. DECKER
United States Attorney
LAWRENCE S. MIDDLETON
Assistant United States Attorney
Chief, Criminal Division
J. MARK CHILDS (Cal. Bar No. 162684)
Assistant United States Attorney
OCDETF Section
1400 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-2433
Facsimile: (213) 894-0142
E-mail: mark.childs@usdoj.gov

Attorneys for Plaintiff
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN RE THE SEARCH OF [redacted]

No. [redacted]

NOTICE OF FILING MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF SEARCH WARRANT APPLICATION

Plaintiff United States of America, by and through its counsel of record, the United States Attorney for the Central District of California and Assistant United States Attorney J. MARK CHILDS, hereby files its Notice of Filing Memorandum of Points and Authorities in Support of Search Warrant Application.

This Notice is based upon the attached memorandum of points and authorities, the files and records in this case including the

///

[redacted]

application and search warrant filed in this matter, and such further evidence and argument as the Court may permit.

Dated: May 9, 2016

Respectfully submitted,

EILEEN M. DECKER
United States Attorney

LAWRENCE S. MIDDLETON Assistant
United States Attorney
Chief, Criminal Division

/s/
J. MARK CHILDS
Assistant United States Attorney

Attorneys for Plaintiff
UNITED STATES OF AMERICA

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

The government submits this supplemental authority in support of its application for a search warrant which seeks authorization to depress the fingerprints and thumbprints of every person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant. The government seeks this authority because those fingerprints, when authorized by the user of the device, can unlock the device.

This procedure will not vi Attached hereto is an article from the Daily Journal dated Friday, May 6, 2016, entitled "Thumbprints to unlock phones can be compelled, courts say."

II. FACTUAL BACKGROUND

In the affidavit in support of the search warrant, the affiant states that Apple Inc., Motorola, HTC, and Samsung, among other companies, produce devices that can be unlocked by the user with a numerical or an alpha-numerical password, or, for some newer versions of the devices, with a fingerprint placed on a fingerprint sensor. Each company has a different name for its fingerprint sensor feature; for example, Apple's is called "Touch ID." Once a user has set up the fingerprint sensor feature in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor. If that sensor recognizes the fingerprint or thumbprint, the device unlocks. Most devices can be set up to recognize multiple prints, so that different prints, not

necessarily from the same person, will unlock the device. If there is no sensor on the device, the device will not open with prints.

There are limits on the ability to use a fingerprint or thumbprint to unlock a device, which varies by manufacturer. For example, with Apple, the Touch ID feature only permits up to five attempts with a print before the device will require the user to enter a passcode. Furthermore, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the device will require the passcode or password programmed by the user and will not allow access to the device based on a print alone. Similarly, Touch ID will not allow access if the device has been restarted or was off and has been turned on, if the device has received a remote lock command, or if five attempts to match a print have been unsuccessful. Other brands have similar restrictions.

In order to attempt to gain access to the devices found at the SUBJECT PREMISES, the search warrant seeks the authority to use the fingerprints and thumbprints of any person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant. Without the numerical or alpha-numerical passcode, the government may not be able to obtain the contents of the devices if those prints are not used. Furthermore, delaying action may prevent even the use of this method of gaining access if that delay prevents the government from attempting to access the device beyond 48 hours since the last time

the device was accessed. It is not known which finger(s) or thumb of which person(s) will unlock the device, but in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

III. LEGAL DISCUSSION

Compelling a person to provide a fingerprint or thumbprint as part of a search warrant violates neither the Fifth nor the Fourth Amendment.

A. The Fifth Amendment Presents No Barrier to Obtaining a Person's Fingerprints

Compelling a person to provide his or her fingerprint does not implicate, let alone violate, the Fifth Amendment. "[B]oth federal and state courts have usually held that [the Fifth Amendment] offers no protection against compulsion to submit to fingerprinting." Schmerber v. California, 384 U.S. 757, 764 (1966). That is so because the Fifth Amendment privilege against self-incrimination only prevents the use against an accused[1] of testimonial or communicative evidence obtained from him. Id. As the Supreme Court explained in Schmerber, that prohibition does not apply to the use of a person's "body as evidence when it may be material." Id. at 763 (quoting Holt v. United States, 218 U.S. 245, 252-53 (1910)); see United States v. Dionisio, 410 U.S. 1, 5-6 (1973) ("It has long been held that the compelled display of identifiable physical characteristics infringes no interest protected by the privilege against compulsory self-incrimination."). The Ninth Circuit has held the same: "requests by

[1] It is, moreover, worth noting that the Fifth Amendment protects the accused, and as of this point, no person is being accused.

the prosecution for . . . fingerprint evidence from a defendant or a suspect are not prohibited by the Fifth Amendment right against self-incrimination because such evidence is not testimonial in nature." Commonwealth of Northern Mariana Islands v. Bowie, 243 F.3d 1109, 1120 n.5 (9th Cir. 2001); see also United States v. De Palma, 414 F.2d 394, 397 (9th Cir. 1969) ("Identifying physical characteristics are not evidence of a testimonial nature."); United States v. Sanudo-Duarte, 2016 WL 126283 (D. Ariz. 2016) (holding that defendant could be compelled to provide exemplar of his palm prints); Virginia v. Baust, CR14-1439 (Va. Cir. Ct. Oct. 28, 2014) (holding that defendant could be compelled to provide his fingerprint in order to unlock phone)

While the government does not know ahead of time the identity of every digital device or fingerprint (or indeed, every other piece of evidence) that it will find in the search, it has demonstrated probable cause that evidence may exist at the search location, and needs the ability to gain access to those devices and maintain that access to search them. For that reason the warrant authorizes the seizure of "passwords, encryption keys, and other access devices that may be necessary to access the device." A password, "key," or use of a fingerprint are all means of gaining access to other spaces or devices, and are seizable both to gain and maintain access. See, e.g., United States v. Shi, 525 F.3d 709, 731 (9th Cir. 2008) (authorizing seizure of keys and identification cards to show indicia of ownership); United States v. Honore, 450 F.2d 31, 33 (9th Cir. 1971). The fact that a successful unlocking of the device could also demonstrate a connection between the person and the device thus does not make the requested fingerprints testimonial, any more than does a

warrant's authorization to seize a person's keys. If anything, the connection raises a Fourth Amendment concern, which is discussed and dispatched below. Finally, as law enforcement will only be seeking to depress the fingerprints of those persons present at the search location for whom law enforcement has cause to believe may be a user of a device, neither the Fifth nor Fourth Amendment is violated.

B. The Fourth Amendment Permits the Acquisition of the Fingerprints

The requested warrant also does not violate anyone's Fourth Amendment rights. It is true that the Fourth Amendment is implicated when the government seeks fingerprints for investigatory purposes. See, e.g., United States v. Parga-Rosas, 238 F.3d 1209, 1215 (9th Cir. 2001); but see Dionisio, 410 U.S. at 4 ("The Fourth Amendment prohibition against unreasonable search and seizure applies only where identifying physical characteristics, such as fingerprints, are obtained as a result of unlawful detention of a suspect, or when an intrusion into the body, such as a blood test, is undertaken without a warrant, absent an emergency situation."). But the Fourth Amendment's requirements are satisfied when the taking of fingerprints is supported by reasonable suspicion. See Hayes v. Florida, 470 U.S. 811, 817 (1985) ("There is thus support in our cases for the view that the Fourth Amendment would permit seizures for the purpose of fingerprinting, if there is reasonable suspicion that the suspect has committed a criminal act, if there is a reasonable basis for believing that fingerprinting will establish or negate the suspect's connection with that crime, and if the procedure is carried out with dispatch."); United States v. Garcia-Beltran, 389 F.3d 864, 868 (9th Cir. 2004) ("[T]he Court has reaffirmed the

principle that the Fourth Amendment does not permit admission of fingerprint evidence resulting from a seizure without reasonable suspicion"); but see Davis v. Mississippi, 394 U.S. 721, 728 (1969) (holding that warrantless "dragnet" investigatory "[d]etentions for the sole purpose of obtaining fingerprints are no less subject to the constraints of the Fourth Amendment. It is arguable, however, that, because of the unique nature of the fingerprinting process, such detentions might, under narrowly defined circumstances, be found to comply with the Fourth Amendment even though there is no probable cause in the traditional sense.").

A fortiori, a search warrant based on probable cause, such as that sought here, would satisfy the Fourth Amendment, especially since law enforcement will not obtain the fingerprints from any person for whom they do not have cause to believe may be a user of a device. Because there is probable cause sufficient to seize the digital device, there is probable cause sufficient to seize "the key" to that device in the form of a person's fingerprint - similar to the provisions in the warrant to seize other keys. Moreover, while executing this provision of the search warrant may result in a brief detention of persons found at the Subject Premises, this too is consistent with Hayes because it will be done "with dispatch" and because it is done pursuant to the judicial authorization sought here. 470 U.S. at 814; see also Michigan v. Summers, 452 U.S. 692, 705 (1981) (a valid search warrant implicitly carries with it the limited authority to briefly detain the occupants on, or in the immediate vicinity of, the premises while the search is being conducted); United States v. Broussard, 80 F.3d 1025, 1033 (5th Cir. 1996) (holding that 10-to 15-minute detention of occupant was

reasonable while agents searched occupant's residence pursuant to valid search warrant).

IV. CONCLUSION

The government respectfully requests that the search warrant be issued with the procedures permitting the law enforcement personnel to depress the fingers of every person who is located at the SUBJECT PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the SUBJECT PREMISES and falls within the scope of the warrant.

[redacted]

ATTACHMENT-1

Friday, May 6, 2016

Thumbprints to unlock phones can be compelled, courts say

By L.J. Williamson

Though the legal wrangling between Apple and the FBI over access to a San Bernardino mass shooter's iPhone has ended, new questions about permissible ways for police to gain access to phone data are being answered in lesser-known cases.

A search warrant issued in February by Central District Magistrate Judge Alicia G. Rosenberg authorized law enforcement personnel to depress the thumbprint of a Glendale woman onto the touch ID sensor of her iPhone so they could examine its contents. A previous ruling in Virginia v. Baust, (No. CR14-1439 Va. Cir. Oct. 28, 2014), held that a suspect "cannot be compelled [by the police] to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same."

The Virginia case hinged on the controversial definition of what comprises "testimonial communication." The court concluded that a passcode was entitled to Fifth Amendment protection because it only existed in the defendant's mind, and forcing him or her to speak the passcode to authorities would be a form of self-incrimination. Yet a fingerprint, which case law has likened to a key ☐ a physical object that can be handed over ☐ was not entitled to that same protection.

To some, focusing on the distinction between two different methods of obtaining the same result may seem forced.

"Despite the fact that it seems artificial, it's consistent with the approach the Supreme Court has taken to the Fifth Amendment," said Stanford law professor David Sklansky, citing the court's reasoning in Pennsylvania v. Muniz 496 U.S. 582 (1990), in which the court drew a sharp distinction between invading information from a suspect's mind versus demanding access to physical characteristics of his body. "The artificiality is in Supreme Court doctrine ☐ not in what the lower court did."

If police have a warrant, they have a legal right to search a phone, but that doesn't answer the problem of getting access to it, Sklansky explained. If police compel a user to place their thumb on a phone, it is compelling a suspect to do something with their body, much like compelling a suspect to stand in a lineup, and it does not impinge on the privilege against self-incrimination. "It's only compulsory self-incrimination if they get you to divulge the contents of your mind," Sklansky said. "A lot of people think it's artificial to draw the line that way, but that's what the Supreme Court says."

Albert Gidari, director of privacy at Stanford Law School's Center for Internet and Society, said the court is following a line of argument that the government likes to put forward, "there is nothing testimonial about unlocking a device you locked, whether it be by password, fingerprint, or otherwise."

It is compelled speech, however, Gidari argued. "It is akin to saying, 'Open up, it's me,' which raises Fifth Amendment issues."

The notion that biometrics generally are not testimonial, and that a fingerprint is akin to a hair sample or blood, is an "imperfect at best" analogy, Gidari said.

A better biometric analogy would be a voice print lock or an iris scanner, he said. "Could the court compel the person to state their password? Could a court force a person to look at the

camera? These methods unlock a device, but only after the person presents themselves and 'testifies' that they are the person with the right to access it ... The trend is against privacy here, but we don't have the last word on it yet."

Though she can see why law enforcement might want to make the distinction ☐ because it is more difficult to force someone to speak a passcode, invoking compelled speech and thought ☐ professor Jill Bronfman, director of the Privacy and Technology Project at UC Hastings College of the Law, said, "As a matter of access to data, passcodes are passcodes, regardless of the methodology or technology."

Yet at a future time, if biometric passcodes include wearable, implantable, and digestible biometric identifiers, compelling a suspect to divulge a passcode may seem tame by comparison, Bronfman said.

lj_williamson@dailyjournal.com