UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

KAW

In the Matter of the SEARCH OF A RESIDENCE IN OAKLAND, CALIFORNIA

Case No. 4-19-70053

**ORDER DENYING APPLICATION FOR A SEARCH WARRANT; ORDER SEALING APPLICATION**



The Government is investigating two individuals believed to be involved in extortion in violation of 18 U.S.C. § 875(d). In brief, the suspects allegedly used Facebook Messenger to communicate with a victim, in which they threatened to distribute an embarrassing video of him if he did not provide them with monetary compensation. (Aff. ¶ 7.) The Government has submitted an application for a search and seizure warrant to seize various items presumed to be located at a residence in Oakland, California ("Subject Premises") connected to the two named suspects. The Application further requests the authority to seize various items (identified in Attachment B), including electronic devices, such as mobile telephones and computers ("digital devices"). The Court has reviewed the Application and finds that there are sufficient facts to support a finding of probable cause to conduct a search of the Subject Premises.

The Government, however, also seeks the authority to compel any individual present at the time of the search to press a finger (including a thumb) or utilize other biometric features, such as facial or iris recognition, for the purposes of unlocking the digital devices found in order to permit a search of the contents as authorized by the search warrant. For the reasons set forth below, the Court finds that the Government's request runs afoul of the Fourth and Fifth Amendments, and the search warrant application must be DENIED. The Government may submit another search warrant

application for the Subject Premises subject to the limitations outlined below.

## DISCUSSION

The issues presented in the Application implicate the constitutional protections afforded by the Fourth and Fifth Amendments. The undersigned has found no legal authority explicitly restricting the Court from considering the privileges and protections afforded by the Fifth Amendment prior to signing a warrant. In fact, the prejudice that suspects may suffer should the Fifth Amendment be ignored at this juncture—both due to the practical difficulty in prevailing on a motion to suppress and the fact that they are not represented in the warrant process—gives rise to a moral imperative demanding consideration of the Fifth Amendment. To do otherwise would be a miscarriage of justice.

### A. Fourth Amendment Analysis

#### i. Probable Cause Exists to Search the Premises

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. "The 'basic purpose of this Amendment,' our cases have recognized, 'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2213, 201 L. Ed. 2d 507 (2018) (quoting *Camara v. Mun. Court of City & Cty. of San Francisco*, 387 U.S. 523, 528 (1967)).

There are sufficient facts in the affidavit to believe that evidence of the crime will be found at the Subject Premises, so the Government has probable cause to conduct a lawful search, so long as it comports with the Fourth Amendment. If, however, law enforcement violates another constitutional right in the course of executing a warrant, it inherently renders the search and seizure unreasonable.

#### ii. No Probable Cause to Use Biometric Features of All Present During Search

In addition to the search of the premises, the Government seeks an order that would allow agents executing this warrant to compel "any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features...." (Aff. ¶ 17h.) This request is overbroad. There are two suspects identified in

the affidavit, but the request is neither limited to a particular person nor a particular device.

Thus, the Court finds that the Application does not establish sufficient probable cause to compel any person who happens to be at the Subject Premises at the time of the search to provide a finger, thumb or other biometric feature to potentially unlock any unspecified digital device that may be seized during the otherwise lawful search.

**iii. Application Overbreadth**

Furthermore, the Government's request to search and seize all digital devices at the Subject Premises is similarly overbroad. The Government cannot be permitted to search and seize a mobile phone or other device that is on a non-suspect's person simply because they are present during an otherwise lawful search.

While the warrant is denied, any resubmission must be limited to those devices reasonably believed by law enforcement to be owned or controlled by the two suspects identified in the affidavit.

**B. The Fifth Amendment Privilege**

Even if probable cause exists to seize devices located during a lawful search based on a reasonable belief that they belong to a suspect, probable cause does not permit the Government to compel a suspect to waive rights otherwise afforded by the Constitution, including the Fifth Amendment right against self-incrimination.[1] The Fifth Amendment provides that no person "shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. The proper inquiry is whether an act would require the compulsion of a testimonial communication that is incriminating. *See Fisher v. United States*, 425 U.S. 391, 409 (1976). Here, the issue is whether the use of a suspect's biometric feature to potentially unlock an electronic device is testimonial under the Fifth Amendment.

The challenge facing the courts is that technology is outpacing the law. In recognition of this reality, the United States Supreme Court recently instructed courts to adopt rules that "'take

[1] For instance, a suspect arrested pursuant to an arrest warrant issued under to the Fourth Amendment, does not waive the right against self-incrimination provided by the Fifth Amendment absent a *Miranda* warning.

account of more sophisticated systems that are already in use or in development.'" *Carpenter*, 138 S. Ct. at 2218–19 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)). Courts have an obligation to safeguard constitutional rights and cannot permit those rights to be diminished merely due to the advancement of technology. *See Carpenter,* 138 S. Ct. at 2214 (quoting *Kyllo*, 533 U.S. at 34) (The United States Supreme Court has repeatedly sought to "assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.") (internal quotations omitted). Citizens do not contemplate waiving their civil rights when using new technology, and the Supreme Court has concluded that, to find otherwise, would leave individuals "at the mercy of advancing technology." *Carpenter,* 138 S. Ct. at 2214 (citation omitted).

While securing digital devices is not a novel concept, the means of doing so have changed. Indeed, consumers have had the ability to utilize numeric or alpha-numeric passcodes to lock their devices for decades. Courts that have addressed the passcode issue have found that a passcode cannot be compelled under the Fifth Amendment, because the act of communicating the passcode is testimonial, as "[t]he expression of the contents of an individual's mind falls squarely within the protection of the Fifth Amendment." *See Doe v. United States*, 487 U.S. 201, 219 (1988) (Stevens, J., dissenting) (citing *Boyd v. United States*, 116 U.S. 616, 633–635 (1886); *Fisher v. United States*, 425 U.S. 391, 420 (1976)); *see also United States v. Kirschner,* 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (citing *Doe,* 487 U.S. at 208 n. 6); *Com. v. Baust*, 89 Va. Cir. 267, at *4 (2014). Today, technology has provided citizens with shortcuts to entering passcodes by utilizing biometric features. The question, then, is whether a suspect can be compelled to use his finger, thumb, iris, or other biometric feature to unlock a digital device.

Testimony is not restricted to verbal or written communications. Acts that imply assertions of fact can constitute testimonial communication for the purposes of the Fifth Amendment. *Doe*, 487 U.S. at 208. Specifically, a witness's "act of production itself could qualify as testimonial if conceding the existence, possession and control, and authenticity of the documents tended to incriminate them." *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1343 (11th Cir. 2012) (citing *Fisher*, 425 U.S. at 410).

Notwithstanding, certain acts, while incriminating, are not within the privilege, such as furnishing a blood sample, submitting to fingerprinting, providing a handwriting or voice exemplar, or standing in a lineup. *Doe*, 487 U.S. at 210. "The distinction which has emerged, often expressed in different ways, is that the privilege is a bar against compelling 'communications' or 'testimony,' but that compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it." *Schmerber v. California*, 384 U.S. 757, 764 (1966); *see also Doe v. United States,* 487 U.S. at 210.

**i. The Proposed Use of Biometric Features is Testimonial**

The Court finds that utilizing a biometric feature to unlock an electronic device is not akin to submitting to fingerprinting or a DNA swab, because it differs in two fundamental ways. First, the Government concedes that a finger, thumb, or other biometric feature may be used to unlock a device in lieu of a passcode. (Aff. ¶ 17a.) In this context, biometric features serve the same purpose of a passcode, which is to secure the owner's content, pragmatically rendering them functionally equivalent. As the Government acknowledges, there are times when the device will not accept the biometric feature and require the user to type in the passcode to unlock the device. (Aff. ¶ 17g.) For example, a passcode is generally required "when a device has been restarted, inactive, or has not been unlocked for a certain period of time." *Id.* This is, no doubt, a security feature to ensure that someone without the passcode cannot readily access the contents of the phone. Indeed, the Government expresses some urgency with the need to compel the use of the biometric features to bypass the need to enter a passcode. *Id.* This urgency appears to be rooted in the Government's inability to compel the production of the passcode under the current jurisprudence. It follows, however, that if a person cannot be compelled to provide a passcode because it is a testimonial communication, a person cannot be compelled to provide one's finger, thumb, iris, face, or other biometric feature to unlock that same device.

Second, requiring someone to affix their finger or thumb[2] to a digital device is fundamentally different than requiring a suspect to submit to fingerprinting. A finger or thumb

[2] The finger and thumb scans versus actual fingerprints are one example. The same rationale applies to using facial recognition or an optical scan versus submitting to a lineup.

scan used to unlock a device indicates that the device belongs to a particular individual. In other words, the act concedes that the phone was in the possession and control of the suspect, and authenticates ownership or access to the phone and all of its digital contents. Thus, the act of unlocking a phone with a finger or thumb scan far exceeds the "physical evidence" created when a suspect submits to fingerprinting to merely compare his fingerprints to existing physical evidence (another fingerprint) found at a crime scene, because there is no comparison or witness corroboration required to confirm a positive match. Instead, a successful finger or thumb scan confirms ownership or control of the device, and, unlike fingerprints, the authentication of its contents cannot be reasonably refuted. In a similar situation, the court in *In re Application for a Search Warrant* observed that "[w]ith a touch of a finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents." 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017). It is also noteworthy that many smartphone applications providing access to personal, private information—including medical records and financial accounts—now allow users to utilize biometric features in lieu of passcodes to access those records. As Judge Weisman astutely observed, using a fingerprint to place someone at a particular location is a starkly different scenario than using a finger scan "to access a database of someone's most private information." *In re Application for a Search Warrant*, 236 F. Supp. 3d at 1073. Thus, the undersigned finds that a biometric feature is analogous to the nonverbal, physiological responses elicited during a polygraph test, which are used to determine guilt or innocence, and are considered testimonial. *See Schmerber*, 384 U.S. at 764.

While the Court sympathizes with the Government's interest in accessing the contents of any electronic devices it might lawfully seize, there are other ways that the Government might access the content that do not trample on the Fifth Amendment. In the instant matter, the Government may obtain any Facebook Messenger communications from Facebook under the Stored Communications Act or warrant based on probable cause. While it may be more expedient to circumvent Facebook, and attempt to gain access by infringing on the Fifth Amendment's privilege against self-incrimination, it is an abuse of power and is unconstitutional. That the

Government may never be able to access the complete contents of a digital device, does not affect the analysis.

**ii. The Foregone Conclusion Doctrine Does Not Apply**

The foregone conclusion doctrine is an application of the Fifth Amendment "by which the Government can show that no testimony is at issue." *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1343 n. 19 (11th Cir. 2012). Specifically, "[w]hen the 'existence and location' of the documents under subpoena are a 'foregone conclusion' and the witness 'adds little or nothing to the sum total of the Government's information by conceding that he in fact has the [documents],' then no Fifth Amendment right is touched because the 'question is not of testimony but of surrender.'" *In re Grand Jury Subpoena, Dated Apr. 18, 2003*, 383 F.3d 905, 910 (9th Cir. 2004) (quoting *Fisher v. United States*, 425 U.S. 391, 411 (1976)). Notwithstanding, a witness's response to a subpoena designed to elicit potentially incriminating evidence is testimonial. *United States v. Hubbell*, 530 U.S. 27, 43 (2000). The foregone conclusion doctrine not does not apply when the Government cannot show prior knowledge of the existence or the whereabouts of the documents ultimately produced in response to a subpoena. *Id.* at 45.

Today's mobile phones are not comparable to other storage equipment, be it physical or digital, and are entitled to greater privacy protection. *See Riley v. California*, 573 U.S. ——, 134 S. Ct. 2473, 2445, 2489 (2014) (An unlocked smartphone cannot be searched incident to arrest other than to determine whether it may be used as a weapon.); *see also Carpenter*, 138 S. Ct. at 2220. In so finding, the Supreme Court acknowledged that smartphones are minicomputers with the capability to make phone calls, a search of which "would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is [present]." *Riley,* 134 S. Ct. at 2491. Further, "[i]n the cell phone context . . . it is reasonable to expect that incriminating information will be found on a phone regardless of when the crime occurs." *Id.* at 2492. Thus, mobile phones are subject to different treatment than more traditional storage devices, such as safes, and should be afforded more protection.

It follows that any argument that compelling a suspect to provide a biometric feature to access documents and data is synonymous with producing documents pursuant to a subpoena would fail. As the *Riley* court recognized, smartphones contain large amounts of data, including GPS location data and sensitive records, the full contents of which cannot be anticipated by law enforcement. *See Riley,* 134 S. Ct. at 2492.[3] Consequently, the Government inherently lacks the requisite prior knowledge of the information and documents that could be obtained via a search of these unknown digital devices, such that it would not be a question of mere surrender. *See Hubbell*, 530 U.S. at 44-45. Additionally, the Government would be unable to articulate facts to compel the unlocking of devices using biometric features by unknown persons the Government could not possibly anticipate being present during the execution of the search warrant. Indeed, the affidavit makes no attempt to do so.

For these reasons, the foregone conclusion doctrine does not apply.

///

///

///

///

///

///

///

///

///

[3] Compelling a suspect to unlock a phone to allow the viewing of applications installed on a smartphone could be self-incriminating and not be a foregone conclusion. For example, a mobile application for a previously unknown cloud storage service—e.g. Dropbox on an iPhone, which also utilizes iCloud—is tantamount to identifying the location, and ultimately producing the contents, of a locked filing cabinet that the Government did not know existed. *See Hubbell*, 530 U.S. at 45 (act of production testimonial, because the Government had no knowledge of the existence or location of documents); *cf. Fisher*, 425 U.S. at 411 (Compliance with a summons directing the taxpayer to produce the accountant's documents was not testimonial, because the Government knew of the existence of the documents and who had possession of them, and did not rely on the testimony of the taxpayer to prove authenticity.). Similarly, a suspect's access to a mobile application for bank accounts could aid in "following the money" even if the accounts are not in the suspect's name and were otherwise unknown to the Government.

## CONCLUSION

For the reasons set forth above, the Government's search warrant application is DENIED. The Government may not compel or otherwise utilize fingers, thumbs, facial recognition, optical/iris, or any other biometric feature to unlock electronic devices. Furthermore, the Government may only seize those digital devices that law enforcement reasonably believes are owned and/or possessed by the two suspects named in the affidavit. The Government may submit a new search warrant application consistent with this order.

Finally, the undersigned hereby SEALS the search warrant application, including all attachments thereto. This order, however, is a matter of public record and shall, accordingly, be issued a case number and docketed by the Clerk of the Court.

IT IS SO ORDERED.

Dated: January 10, 2019

Kandis Westmore

KANDIS A. WESTMORE
United States Magistrate Judge

United States District Court
Northern District of California