UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF [redacted] WASHINGTON, DISTRICT OF COLUMBIA,	)	**Case No. 18-sw-0122 (GMH)**

MEMORANDUM OPINION

The government filed an application for a search warrant in this matter that sought to search a premises in the District of Columbia and to seize, among other things, evidence on cellphones and computers found on the premises which reasonably could contain evidence of the offenses under investigation. In addition, the government sought authorization from the Court to "compel biometric features of an individual believed to have perpetrated the alleged offenses under investigation [the "Subject"] in connection with any biometric recognition sensor-enabled" digital device falling within the scope of the warrant. Government Mem. at 1.[1] In English: the government sought an order from the Court permitting it to attempt to unlock cellphones and computers falling within the scope of the warrant through the compelled use of the Subject's physical characteristics—i.e., his fingerprints, face, or irises. Because the compelled unlocking of digital devices is an emerging area of the law raising both Fourth and Fifth Amendment issues, none of which have been addressed in this District, the undersigned appointed as *amicus curiae* the Federal Public Defender for the District of Columbia ("*amicus*" or "Federal Public Defender")

[1] The relevant submissions for the purpose of this opinion are (1) Application for a Search Warrant ("Warrant"), including the Affidavit in Support ("Affidavit"), Attachment A, and Attachment B; (2) the government's Memorandum in Support of an Application under Rule 41 for a Warrant to Search and Seize ("Government Mem."); (3) Brief of *Amicus Curiae* Federal Public Defendant for the District of Columbia ("*Amicus Curiae* Mem."); (4) Reply Memorandum in Support of an Application under Rule 41 for a Warrant to Search and Seize ("Reply Mem.").

to submit its views on the lawfulness of the government's request.[2] The Court heard oral argument on the government's application on June 4, 2018. It granted the application and signed the search warrant on June 7, 2018. The Court now issues this opinion to explain its reasoning for doing so.

I. BACKGROUND

The government's affidavit in support of the warrant established probable cause to believe that the premises to be searched was the Subject's, an individual whom the government had probable cause to believe has violated 18 U.S.C. § 1030, which prohibits fraud and related activity involving computers. The application further established probable cause to believe that personal electronic devices used or controlled by the Subject, and which might be found on the premises to be searched, contained evidence or information about, or were the instrumentalities of, those crimes (the "Subject Devices"). Specifically, Attachment B to the requested warrant described the evidence to be seized during the search of the premises, including,

> for any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, including but not limited to . . . [a certain] computer referenced in the search warrant affidavit [that the Subject has been seen using]:
>
> > . . . evidence of who used, owned, or controlled the [Subject Devices] at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence . . . .

Attachment B, ¶ 3.a. Attachment B further stated:

> Although already generally covered by paragraph 3.a. above, during the execution of the search of the [premises] described in Attachment A, law enforcement personnel are also specifically authorized to compel [the Subject] to provide biometric features, including pressing his fingers (including thumbs) against and/or

[2] The Court thanks the Federal Public Defender for its submission and participation at oral argument, both of which were of considerable assistance in resolving the government's application.

> putting his face before the sensor, or any other security feature requiring biometric recognition, of:
>
> (a) any of the [Subject Devices] found at the [premises], and
>
> (b) where the [Subject Devices] are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,
>
> for the purpose of attempting to unlock the [Subject Devices'] security features in order to search the contents as authorized by this warrant.

Attachment B, ¶ 4. The affidavit in support of the warrant application noted that, from both the affiant's "training and experience, [and] . . . from information found in publicly available materials published by device manufacturers, . . . many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features" rather than with passwords or passcodes. Affidavit, ¶ 59.a. Importantly, the warrant made clear that law enforcement was not authorized "to compel any other individuals found at the [premises] to provide biometric features . . . to access or otherwise unlock any [Subject Device]," or to request the Subject "to state or otherwise provide the password or any other means that may be used to unlock or access the [Subject Devices], including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the [Subject Devices]." Attachment B, ¶ 4. That is, absent the Subject's Mirandized-waiver of constitutional rights, the government was not permitted to ask the Subject to disclose which biometric feature (e.g., which finger) would unlock any of the Subject Devices. Rather, law enforcement was required to select which biometric feature to test on a given device.

II. DISCUSSION

A. Fourth Amendment

"The Fourth Amendment provides in relevant part that '[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause.'" *Missouri v. McNeely*, 569 U.S. 141, 148 (2013) (quoting U.S. Const. amend IV). Here, the affidavit submitted in support of the search warrant established both probable cause to believe that a crime had been committed and that evidence of the crime would be found at the premises to be searched, including on the Subject Devices. Thus, the government's warrant satisfied the requirements of the Fourth Amendment justifying the search of the premises and of the above-described Subject Devices.[3]

[3] Based on the limited information that was provided as part of the Court's order to submit an *amicus* brief, the Federal Public Defender argued that "the government's request to generally search any digital device(s) that *may* be found at the premises likely violates the Fourth Amendment's particularity requirement." *Amicus Curiae* Mem. at 1 n.1. The concern of *amicus* is understandable in light of the fact that it has seen neither the proposed warrant, itself, nor the affidavit supporting it. However, the government's warrant was sufficiently particularized.

The Fourth Amendment's particularity requirement has three components: a warrant "must identify the specific offense" for which law enforcement has established probable cause; it must "describe the place to be searched"; and it must "specify the 'items to be seized by their relation to designated crimes.'" *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013) (quoting *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010)); *see also United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017) ("[T]here must, of course, be a nexus . . . between the item to be seized and criminal behavior." (second alteration in original) (quoting *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967))). "[A] failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary." *Galpin*, 720 F.3d at 446 (quoting *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992)). Here, the warrant identified the crime at issue as 18 U.S.C. § 1030—"Fraud and relat[ed] activity in connection with computers." Warrant. It identified the specific place to be searched. *Id.* And it adequately specified the items to be seized and their connection to the identified crimes. The Affidavit, incorporated by reference into the warrant, explained that "individuals who engage in the . . . described criminal activity use digital devices like [those sought] to facilitate illegal activity . . . ; [and] to store . . . documents and records relating to their illegal activity," among other things, and explained why the affiant had reason to believe that such devices may have been used in furtherance of the crime being investigated. Affidavit, ¶¶ 51–52, 55; *see also United States v. Maxwell*, 920 F.2d 1028, 1031 (D.C. Cir. 1990) ("[A] search warrant may be construed with reference to the affidavit supporting it . . . if '(1) the affidavit accompanies the warrant, and in addition (2) the warrant uses "suitable words of reference" which incorporate the affidavit by reference.'" (quoting *United States v. Vaughn*, 830 F.2d 1185, 1186 (D.C. Cir. 1987))). It further limited the devices to be searched to those located at the searched premises "that based on their location, appearance, and/or other information learned at the time of the execution of the warrant appear capable of containing evidence, fruits, contraband, instrumentalities, and information" relating to the offenses alleged to have been committed by the target of the investigation," explaining further that, given certain facts of the case, such devices are likely to be found on the premises. *Id.*, ¶ 52. Attachment B, in turn, asserted that

The novel question presented by the government's application is whether its request to compel the use of the Subject's biometric features in an attempt to open the Subject Devices found on the premises ran afoul of the Fourth Amendment.

"The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State." *Schmerber v. California*, 384 U.S. 757, 767 (1966). As the Supreme Court has repeatedly recognized, "obtaining . . . physical evidence from a person involves a potential Fourth Amendment violation at two different levels—the 'seizure' of the 'person' necessary to bring him into contact with government agents, and the subsequent search for and seizure of the evidence. *United States v. Dionisio*, 410 U.S. 1, 8 (1973) (internal citation omitted) (citing *Davis v. Mississippi*, 394 U.S. 721 (1969)). That said, when a location is searched pursuant to a valid warrant, law enforcement generally may detain occupants who are on the premises during its execution without violating the Fourth Amendment's prohibition on unreasonable seizures. *See, e.g.*, *Bailey v. United States*, 568 U.S. 186, 201 (2013); *Michigan v. Summers*, 452 U.S. 692, 705 (1981); *cf. United States v. Broussard*, 80 F.3d 1025, 1033 (5th Cir. 1996) (suggesting that "prolonged" or "overly intrusive" detention in relation to execution of warrant may violate Fourth Amendment). Assuming, then, that the government's seizure of the Subject during the execution of the warrant was otherwise done in a manner consistent with the

---

the devices to be searched must be "capable of containing and reasonably could contain fruits, contraband, instrumentalities, and information" relating to the offenses alleged to have been committed by the target of the investigation. Attachment B, ¶ 4. Finally, the warrant lists the categories of information related to the offense under investigation to be seized from the devices, including evidence of who used or controlled the Subject Devices at the time the things described in the warrant were created, edited, or deleted; evidence of software, such as viruses and Trojan horses, that would allow others to control the Subject Devices; evidence of other storage devices for electronic information attached to the Subject Devices; evidence of programs and associated data designed to eliminate data from the Subject Devices; evidence of the times the Subject Devices were used; information that may be necessary to access the Subject Devices; information about IP addresses used by the Subject Devices; and information about the Subject Devices' Internet activity. Attachment B, ¶ 3. This is not, then, a situation in which a proposed warrant lacked sufficient indicia that the target of the investigation owned such devices and used them in furtherance of the alleged crime, *see Griffith*, 867 F.3d at 1273, or failed to limit the items and information seized to that relating to the alleged crime, *see In re Black iPhone 4*, 27 F. Supp. 3d 74, 78 (D.D.C. 2014). In short, the warrant satisfied the particularity requirement of the Fourth Amendment.

Fourth Amendment—that is, that the seizure of the Subject's person was accomplished "in the immediate vicinity of the premises to be searched," *Bailey*, 568 U.S. at 201, and was neither prolonged nor overly intrusive, *Broussard*, 80 F.3d at 1033—the question then becomes whether the government taking the additional step of testing the Subject's biometric features on any Subject Devices found during the search of the premises similarly complies with the Fourth Amendment.

The government's memorandum cites a number of cases to support the proposition that "obtaining an individual's physical characteristics," including fingerprints, palm prints, and photographic likenesses, "does not constitute an intrusion upon his privacy that warrants Fourth Amendment protection." Government Mem. at 5 (citing *United States v. Farias-Gonzalez*, 556 F.3d 1181, 1188 (11th Cir. 2009), *United States v. Kaczmarak*, 62 F. App'x 510, 511 (4th Cir. 2003), *United States v. Teter*, No. 06-4050-01-CR, 2008 WL 141671, at *6 (W.D. Mo. Jan. 11, 2008), *Stehney v. Perry*, 907 F. Supp. 806, 823 (D.N.J. 1995), and *Rowe v. Burton*, 884 F. Supp. 1372, 1384 (D. Alaska 1994)); *but see United States v. Askew*, 529 F.3d 1119, 1158 (D.C. Cir. 2008) (noting that although "[i]n a 1973 case, the Supreme Court hinted in dicta that fingerprinting may not be a search," later precedent, such as *Hayes v. Florida*, 470 U.S. 811 (1985), "plainly considered fingerprinting a search"). However, it acknowledges that "most of the cases that have rejected Fourth Amendment challenges to fingerprinting involved fingerprints obtained: (1) when individuals were already lawfully in custody; (2) via grand jury subpoena or other legal process; or (3) only for identification and not investigative purposes," and concedes that "the Fourth Amendment *is* implicated when the government seeks physical aspects for investigatory purposes." Government Mem. at 5 n.3, 6 (emphasis added).

The government's point is well-taken. For example, in *Davis v. Mississippi*, 394 U.S. 721, 726–27 (1969), the Supreme Court held that fingerprints obtained from a defendant as part of an

investigatory detention without probable cause should have been excluded from trial. Similarly, in *Hayes*, 470 U.S. at 816, the Court held that fingerprints were properly suppressed when the defendant was arrested without probable cause, taken to the police station without consent, and detained and fingerprinted for investigative purposes. *See also, e.g.*, *United States v. Oscar-Torres*, 507 F.3d 224, 232 (4th Cir. 2007) ("[F]ingerprints taken as part of routine booking procedures but intended to provide evidence for criminal prosecution are . . . motivated by an investigative . . . purpose. Such fingerprints are, accordingly, subject to exclusion." (emphasis omitted)); *United States v. Olivares-Rangel*, 458 F.3d 1104, 1114 (10th Cir. 2006) ("In *Davis* and *Hayes*, the Supreme Court held that when an illegal arrest was used as an investigatory devise to obtain fingerprints, the fingerprints were regarded as inadmissible fruit of an illegal detention."); *United States v. Ortiz-Hernandez*, 427 F.3d 567, 580–81 (9th Cir. 2005) (Fletcher, J., dissenting) ("It is established law under *Hayes* . . . and *Davis* . . . that [unlawfully-obtained] fingerprints taken for purely investigatory purposes must be suppressed [pursuant to the Fourth Amendment].").

However, the fact that the Fourth Amendment is implicated when law enforcement detains an individual to obtain fingerprints (or similar physical characteristics) for an investigatory purpose does not mean that all such instances of fingerprinting violate the Constitution. As the Supreme Court observed in *Davis*, "[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." 394 U.S. at 727.

The question then is—even where the government is permitted to detain briefly an individual during a search warrant's execution consistent with *Bailey* and *Broussard*—what further

showing does the Fourth Amendment require before the government may be authorized to compel the use of an individual's biometric features in an attempt to unlock a digital device that it is authorized to search pursuant to a warrant? The decision is not without consequence, and rightfully so given the privacy interests at stake recognized in *Davis*. *See Davis*, 394 U.S. at 726–27 ("Nothing is more clear than that the Fourth Amendment was meant to prevent wholesale intrusions upon the personal security of our citizenry, whether these intrusions be termed 'arrests' or 'investigatory detentions.'"). Surely it would not be constitutional, for example, for the government to demand the use of anyone's biometric features for the purpose of attempting to unlock such a digital device. Rather, the standard should focus on the government's evidence of the connection between the individual and the device and should prove dispositive in situations where the government's evidence concerning that connection is non-existent or amounts to nothing more than a guess or a hunch.

At oral argument, the government argued that the Court should not further define the standard beyond that of the "reasonableness" that the Fourth Amendment requires of law enforcement whenever it executes a search warrant. Under that standard, provided a warrant is properly issued, "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of the search authorized by the warrant—subject of course to the general Fourth Amendment protection 'against unreasonable searches and seizures.'" *Dalia v. United States*, 441 U.S. 238, 255, 257 (1979) (footnote omitted) (first quoting *Warden v. Hayden*, 387 U.S. 294, 307 (1967), then quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Characterizing the compelled use of a detained individual's biometric features during the execution of a warrant as one of "the method[s] of executing the warrant," the government suggested that, as long as law enforcement acts reasonably during a search—including in

determining whose biometric features it may use to attempt to unlock a digital device that it is authorized to search pursuant to a warrant —the Fourth Amendment would be satisfied.

Here, however, the government asked for prior authorization from the Court to place an individual's fingerprints on certain digital devices (or to use other biometric features to gain access to them): namely, the warrant "specifically authorize[s]" law enforcement to compel the Subject to provide biometric features. Attachment B, ¶ 4. Such authorization can have significant consequences for the individual whose biometric features are tested by the government. Nor did the government deny at oral argument that it might later argue that it reasonably relied on the Court's authorization if its compelled use of the individual's biometric features is challenged. *See*, *e.g.*, *United States v. Cardoza*, 713 F.3d 656, 658 (D.C. Cir. 2013) ("Under *United States v. Leon*, [468 U.S. 897, 913 (1984),] suppression of evidence is usually not required when officers conduct a search in reasonable reliance on a search warrant issued by a detached and neutral magistrate."). In such circumstances, the legal standard that the government must apply pursuant to the Court's authorization should be more clearly defined, rather than leaving it to law enforcement to act reasonably "under the particular circumstances" that obtain during the search.

For its part, the Federal Public Defender proposed at oral argument that, before receiving court approval to use biometric features to attempt to unlock a digital device, the government should be required to establish probable cause to believe that the device belongs to the suspect. But while the taking of a fingerprint is undeniably a search, *see, e.g.*, *Hayes*, 470 U.S. at 816–17; *Askew*, 529 F.3d at 1158 ("The Court's . . . decision in *Hayes* plainly considered fingerprinting a search . . . ."), cases have recognized a diminished interest in "purely external searches such as fingerprinting," based on their less intrusive nature, *United States v. Kriesel*, 508 F.3d 941, 948 (9th Cir. 2007); *see also, e.g.*, *Dionisio*, 410 U.S. at 14 ("The required disclosure of a person's

voice is thus immeasurably further removed from the Fourth Amendment protection than was the intrusion into the body effected by the blood extraction in *Schmerber*."); *United States v. Weikert*, 504 F.3d 1, 12 (1st Cir. 2007) ("[A]n internal search such as a blood draw is inherently more intrusive than a purely external search such as fingerprinting or photographing."); *Nicholas v. Goord*, 430 F.3d 652, 658 (2d Cir. 2005) ("[T]he Court has also recognized a distinction between non-intrusive means of obtaining physical evidence (such as fingerprinting) and more invasive measures (such as drawing blood)."); *Cf. McNeeley*, 569 U.S. at 148, 165 (refusing to endorse a blanket exception to the warrant requirement for blood tests of suspects in drunk-driving cases based on exigent circumstances, and emphasizing that the search "involved a compelled physical intrusion beneath [the suspect's] skin and into his veins to obtain a sample of his blood for use as evidence in a criminal investigation," an "invasion of bodily integrity [that] implicates an individual's 'most personal and deep-rooted expectations of privacy'") (quoting *Winston v. Lee*, 470 U.S. 753, 760 (1985)). Further, in *Hayes*, the Supreme Court indicated that the Fourth Amendment would permit "a brief detention in the field for purpose of fingerprinting" for an investigatory purpose on a showing of less than probable cause, a situation analogous to that presented by the government's application here.[4] 470 U.S. at 816. The Court observed in *Hayes*:

> There is . . . 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.

470 U.S. at 817; *see also Hiibel v. Sixth Judicial Dist. Ct. of Nev., Humboldt Cty.*, 542 U.S. 177, 188–89 (2004) (quoting *Hayes* dictum with approval).

[4] In this regard, the Court sees no principled distinction that can be made between the intrusiveness of the government's compelled use of an individual's fingerprints versus his or her face or irises.

Moreover, the reasonable suspicion standard is similar to the reasonableness standard proposed by the government—which already governs the conduct of law enforcement when executing a search warrant, *see, e.g.*, *Dalia*, 411 U.S. at 257—and has been applied by the Court in the search warrant context, *see Richards v. Wisconsin*, 520 U.S. 385, 394–95 (1997) (holding that a "no-knock" entry is justified where, based on the facts as they exist at the time of the execution of the warrant, the police "have a reasonable suspicion that knocking and announcing their presence, under the particular circumstances, would be dangerous or futile, or that it would inhibit the effective investigation of the crime by, for example, allowing the destruction of evidence"). Indeed, even in the absence of a warrant, the Supreme Court "has recognized that a law enforcement officer's reasonable suspicion that a person may be involved in criminal activity permits the officer to stop the person for a brief time and take additional steps to investigate further." *Hiibel*, 542 U.S. at 185. Here, of course, there is a warrant, issued on a showing of probable cause to search both the premises and the Subject Devices found on the premises, so the standard to be imposed governs merely the subsidiary showing to be made to allow law enforcement to engage on-site in "additional steps to investigate further."[5] *Id.*; *see also Michigan v. Summers*, 452 U.S. 692, 703 (1981) (brief detention of occupants on, or in the immediate vicinity of, premises represents "only an incremental intrusion on personal liberty when the search of the house has been authorized by a valid warrant").[6]

[5] This application did not present the question of the proper standard to apply when law enforcement seeks to compel use of biometric features to access a digital device at a time other than during the search of a premises pursuant to a search warrant, and the Court does not address that issue.

[6] In two recent cases, the Supreme Court has addressed the warrant requirement as it applies to cell phones. *Carpenter v. United States* held that law enforcement must get a warrant in order to access historical cell-site location information from a phone; *Riley v. California* required a warrant to search the contents of a cell phone seized incident to arrest. *Carpenter*, 585 U.S. __, __, slip op. at 22 (2018); *Riley*, 573 U.S. __, __, 134 S. Ct. 2473, 2495 (2014). Here, again, the government has a warrant that authorizes search of a cell phone seized during its execution. The privacy interest at issue here is not in the contents of the phone, but in the fingerprints or other biometric features the government

Using *Hayes* as its guide, the Court thus finds that, when attempting to unlock a telephone, computer or other electronic device during the execution of a search warrant that authorizes a search of the device, the government may compel the use of an individual's biometric features, if (1) the procedure is carried out with dispatch and in the immediate vicinity of the premises to be searched, and if, at time of the compulsion, the government has (2) reasonable suspicion that the suspect has committed a criminal act that is the subject matter of the warrant, and (3) reasonable suspicion that the individual's biometric features will unlock the device, that is, for example, because there is a reasonable suspicion to believe that the individual is a user of the device.[7] *Cf. In re Application for a Search Warrant*, 236 F. Supp. 3d 1066, 1070 (N.D. Ill. 2017) (denying warrant on Fourth Amendment grounds where government sought authority "to seize any individual at the subject premises and force the application of their fingerprints as directed by government agents" where "request [was] made without any specific facts as to who is involved in the criminal conduct linked to the subject premises, or specific facts as to what . . . device is being employed"). Future government requests for authorization to compel the use of an

seeks to use. As discussed above, the Supreme Court and lower courts have repeatedly indicated that an individual has a diminished privacy interest in these kinds of physical features.

[7] Further, the government would be prohibited from using the Court's authorization as a basis to coerce any individual to consent to collection of their biometric features. *See, e.g.*, *Moran v. Burbine*, 475 U.S. 412, 421 (1986) (relinquishment of right to remain silent must be "voluntary in the sense that it was the product of a free and deliberate choice rather than intimidation, coercion, or deception"); *Bumper v. North Carolina*, 391 U.S. 543, 550 (1968) ("When a law enforcement officer claims authority to search a home under a warrant, he announces in effect that the occupant has no right to resist the search. The situation is instinct with coercion—albeit colorably lawful coercion. Where there is coercion there cannot be consent."); *United States v. Dietrich*, No. 4:13CR3087, 2014 WL 351961, at *1, 4 (D. Neb. Jan. 30, 2014) (finding that defendant "was induced to cooperate, but there was no unreasonable coercion or duress caused by investigators" under the Fourth Amendment where law enforcement explained to individual that if they "applied [for] and received a search warrant, and if they did not have a key, . . . they would use force to enter his home"). Law enforcement is not absolved of its responsibility to act reasonably in executing a warrant merely because the government has received court authorization to compel the use of an individual's biometric features. Circumstances that obtain during the execution may change the calculus, making an otherwise reasonable search unreasonable.

individual's biometric features as part of a search warrant seeking to seize evidence on digital devices should comply with that standard.[8]

B. Fifth Amendment

The Fifth Amendment provides, in relevant part, that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. The Fifth Amendment is intended to protect an accused "from having to reveal, directly or indirectly, knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the Government." *Doe v. United States*, 487 U.S. 201, 213 (1988) (*Doe II*). The Supreme Court has thus held that "[t]he word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character." *United States v. Hubbell*, 530 U.S. 27, 34 (2000). Therefore, "[t]o qualify for the Fifth Amendment privilege, a communication must be: (1) testimonial, (2) incriminating, and (3) compelled." *Hiibel*, 542 U.S. at 189.

Here, the seizure of any incriminating information found *on* the phones or computers discovered during the search of the premises would not violate the Fifth Amendment because the "creation" of that information was voluntary and "not 'compelled' within the meaning of the privilege [against self-incrimination]." *Hubbell*, 530 U.S. at 35–36; *see also Virginia v. Baust*, 89 Va. Cir. 267, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014) ("The footage [on the phone] . . . would not be protected under the Fifth Amendment because its creation was voluntary, *i.e.*,

[8] While prior judicial authorization would not be required where the exigencies of the situation would make doing so impossible, the government's decision to seek such authorization in this case is consistent with the Supreme Court's instruction in *Terry* and *McNeely* that prior judicial authorization for searches and seizures must be sought whenever practicable. *See McNeely*, 569 U.S. at 153 (noting that "some circumstances will make obtaining a warrant [to draw blood for alcohol testing] impractical," but refusing to adopt a *per se* rule that allows such testing without a warrant in all drunk-driving cases); *Terry*, 392 U.S. at 20 (stating that "police must, whenever practicable, obtain advance judicial approval of searches and seizures"). The Court therefore expects that, absent exigent circumstances, the government will continue to seek prior authorization for the compelled use of an individual's biometric features to unlock digital devices even where the search of such devices is permitted by a warrant.

not compelled."). Rather, the compulsion at issue under the Fifth Amendment is the compelled use of the Subject's biometric features to unlock the Subject Devices and gain access to incriminating information that may be on them. In that sense, the government's warrant was obviously compulsive and was likely to be incriminating, insofar as the compelled use of the biometric features may result in a "disclosure[] that the witness [would] reasonably believe[] could be used in a criminal prosecution or could lead to other evidence that might be so used." *Kastigar v. United States*, 406 U.S. 441, 445 (1972); *see also Baust*, 89 Va. Cir. 267, 2014 WL 10355635, at *2 ("[T]here is no question that a motion to compel is compulsive and the production of the passcode or fingerprint would be incriminating."). The question then is whether the compelled use of the Subject's biometric features can be deemed "testimonial."

The Supreme Court has held that testimonial communications for purposes of the Fifth Amendment include not only oral communications but also certain communicative acts. In *Hubbell*, for example, the Court considered whether a witness' response to a subpoena calling for the production of eleven categories of documents could be deemed testimonial. 530 U.S. at 31. There, when the target of the subpoena appeared before a grand jury he invoked his Fifth Amendment privilege against self-incrimination and refused to state whether any responsive documents were in his possession, custody, or control. *Id.* The prosecutor then produced a court order requiring him to respond to the subpoena and granting him immunity to the extent allowed by law. *Id.* The respondent thereafter produced over 13,000 documents in response to the categories in the subpoena, the contents of which led to his prosecution for tax-related crimes and mail fraud. *Id.* at 31–32. The Supreme Court held that the compelled response to the subpoena was a violation of the respondent's Fifth Amendment privilege, observing more generally that

> the act of producing documents in response to a subpoena may have a compelled testimonial aspect. We have held that "the act of production" itself may implicitly

> communicate "statements of fact." By "producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic."

Id. at 36 (quoting *Doe II*, 487 U.S. at 209). The Court found that responding to the subpoena at issue in *Hubbell* "could provide a prosecutor with a 'lead to incriminating evidence,' or 'a link in the chain of evidence needed to prosecute,'" and thus violated the respondent's privilege against self-incrimination. *Id.* at 42.

The Federal Public Defender equates the conduct at issue here to the production of documents in response to the subpoena in *Hubbell*. It contends that the compelled use of biometric features to unlock a phone or computer is "inherently testimonial" because it "would implicitly communicate that the suspect possessed or controlled the device with incriminating evidence." *Amicus Curiae* Mem. at 3. However, the *Hubbell* Court emphasized that, in responding to the subpoena, "[i]t was unquestionably necessary for respondent to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena." 530 U.S. at 43. "The documents did not magically appear in the prosecutor's office like 'manna from heaven.' They arrived there only after respondent . . . took the mental and physical steps necessary to provide the prosecutor with an accurate inventory of the many sources of potentially incriminating evidence sought by the subpoena." *Id.* at 42. The Court thus analogized the respondent's "assembly of those documents" to "telling an inquisitor the combination to a wall safe," rather than "being forced to surrender the key to a strongbox." *Id.* at 43.

Admittedly, the line between testimonial and non-testimonial communications under the Fifth Amendment is not crystal clear. Here, however, the compelled use of the Subject's biometric

features is far more akin to the surrender of a safe's key than its combination.[9] As other courts have recognized, there will be no revelation of the contents of the Subject's mind with the procedure proposed by the government for collection of the Subject's biometric features. Rather, "[t]he government chooses the finger to apply to the sensor, and thus obtains the physical characteristic—all without the need for the person to put any thought at all into the seizure." *In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d 800, 804 (N.D. Ill. 2017); *see also Minnesota v. Diamond*, 905 N.W.2d 870, 876 (Minn. 2018) ("[The defendant's] act of providing a fingerprint to the police was not testimonial because the act did not reveal the contents of [his] mind."); *Baust*, 89 Va. Cir. 267, 2014 WL 10355635, at *4 ("The fingerprint . . . does not require the witness to divulge anything through his mental processes."). Indeed, the use of the fingerprint is much more like the government's compelled use of other "physical characteristics" of criminal suspects that courts have found non-testimonial even when they are used for

[9] The Federal Public Defender objects to analogizing the seizing of a key from a suspect to open a strongbox, which is a non-testimonial act, to the use of biometric features to unlock a device, arguing that "[a] physical key does not necessarily connote possession, control, or prior access the way a fingerprint or facial technology does" because "[o]ne can borrow, find, or steal a physical key." *Amicus Curiae* Mem. at 7. But surely the possession of a key that turns a strongbox's lock denotes present access, from which prior access can be inferred (and argued in a prosecution). The fact that the possessor of the key has a more credible counter-argument—that a key may be borrowed, found, or stolen, an argument that would be difficult to maintain regarding a fingerprint—speaks to the incriminatory nature of the possession of the object: that possessing a borrowed, found, or stolen key to a strongbox may have a weaker incriminatory consequence than would bearing a fingerprint that opens a device. But the notion that one might have more incriminatory power than the other is not relevant to whether the compelled use of a fingerprint is any more testimonial than the compelled use of a key; "the requirement that the compelled communication be 'testimonial'" is "separate [from the] requirement that the communication be 'incriminating.'" *Doe II*, 487 U.S. at 208 n.6; *see also id.* ("If a compelled statement is 'not testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence.'" (quoting *In re Grand Jury Subpoena*, 826 F.2d 1166, 1171 n. 2 (2d Cir. 1987) (Newman, J., concurring))); *In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d at 805 ("When deciding whether an act is testimonial or not, the governing case law simply does not take into account the power or immediacy of the incriminating inference . . . ."). Moreover, to the extent that the Federal Public Defender is concerned that the fact that using an individual's fingerprint to unlock a device leads "necessarily" to the conclusion that the individual possesses or controls the device, its rhetoric is overstated. Digital devices can be set up so that more than one individual's fingerprints will unlock them, *see* Affidavit, ¶ 59.b (noting that some digital devices allow users to register multiple fingerprints to unlock devices); *see also In re Search Warrant Application for [Redated Text]*, 279 F. Supp. 3d at 802 (same), providing the bearer of the fingerprint similar non-inculpatory explanations to the holder of the key: although I have access to it, that device (or that strongbox) and its contents are not mine. And so, the distinction *amicus* makes between a fingerprint and a key is simply not helpful to answering the question at hand.

investigatory purposes rather than solely for identification. *See, e.g.*, *Doe II*, 487 U.S. at 215–16 (holding compelled signature not testimonial); *Dionisio*, 410 U.S. at 7 (holding voice exemplar not testimonial); *Gilbert v. California*, 388 U.S. 263, 266–67 (1967) (holding handwriting exemplar not testimonial); *United States v. Wade*, 388 U.S. 218, 222–23 (1967) (holding use of voice exemplar in line up not testimonial); *Schmerber*, 384 U.S. at 765 (holding blood sample to test for alcohol content not testimonial, and noting "both federal and state courts have usually held that it offers no protection against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture"); *Holt v. United States*, 218 U.S. 245, 252–53 (1910) (trying on particular clothing not testimonial); *Williams v. Schario*, 93 F.3d 527, 528–29 (8th Cir.1996) (holding fingerprints are non-testimonial evidence and do not therefore implicate privilege against self-incrimiation). The "distinction which has emerged" as a "helpful framework for analysis" is that the Fifth Amendment "privilege is a bar against compelling 'communication' or 'testimony,' but that compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it." *Schmerber,* 384 U.S. at 764.

For example, in *Schmerber* the Supreme Court held that "not even the shadow of testimonial compulsion or enforced communication by the accused was involved" in drawing a defendant's blood and testing it for blood-alcohol level, which was then used to convict him of driving under the influence. *Id.* at 765. Arguably, the blood in *Schmerber* "communicated" as much as, if not more than, the biometric features at issue here might—that the blood was the defendant's and that he had been drinking, for example—but its compelled collection was nevertheless deemed non-testimonial. Indeed, the Court noted that, as the defendant's "participation, except as a donor, was irrelevant to the results of the test," his "testimonial

capacities were in no way implicated." *Id.* It is difficult to make a principled distinction between the donation of blood at issue in *Schmerber* and the Subject's passive "donation" of fingerprints (or other biometric features) at issue here.

Similarly, in *Doe II*, the Supreme Court held that compelling a defendant to sign a directive consenting to the disclosure of his bank accounts, which applied to "any and all accounts over which [he] had a right of withdrawal, without acknowledging the existence of any such account" was not testimonial under the Fifth Amendment. 487 U.S. at 204, 215–16. The Court reasoned that the consent directive itself did not "make reference to a specific account," but spoke "only . . . in the hypothetical." 487 U.S. at 215. For that reason, "[b]y signing the form, [the defendant] ma[de] no statement, explicit or implicit, regarding the existence of a foreign bank account or his control over any such account." *Id.* at 215–16. That is, compelling a suspect's signature is not a testimonial act even when it can be used to further an investigation, because it does not reveal "any knowledge he might have." *Id.* at 217 (quoting *Wade*, 388 U.S. at 222).

Amicus contends that *Doe II* supports its argument because, while the defendant in that case "was not acknowledging control of any *particular* bank account," here, "the compelled access would reveal exactly what particular device the person possessed or controlled."[10] *Amicus Curiae* Mem. at 4. But when law enforcement took the *Doe* petitioner's signed consent directive to a bank at which he had an account, the directive would communicate control of a particular bank account at that point. To be sure, at that point, the petitioner would likely not be present, and, at oral argument, it became clear that the Federal Public Defender is troubled by the immediacy of any identification evidence here: law enforcement will choose the Subject's finger(s) to place on the touch pad (for example) of a Subject Device, and, if it unlocks, instantly know that the Subject had

[10] As noted in footnote 9, *supra*, that position overstates the case.

access to it. But, "[w]hen deciding whether an act is testimonial or not, the governing case law simply does not take into account the power or immediacy of the incriminating evidence acquired from the physical characteristic." *In re Search Warrant Application*, 279 F. Supp. 3d at 805. After all, the Supreme Court has held that the donning of a blouse to test whether accused fits into it and the provision of an accused's voice exemplar to ascertain whether a witness recognizes it—identification determinations that would occur in short order, if not immediately—are not inherently testimonial. *See Holt*, 218 U.S. at 252–53; *Wade*, 388 U.S. at 222–23; *see also In re Search Warrant Application*, 279 F. Supp. 3d at 805 ("In essence, applying the fingerprint to the Touch ID sensor is no different than watching someone put on a shirt to see—immediately—if it fits or listening to someone speak in a live lineup and deciding—immediately—whether the voice matches the suspect's."). In sum, the Fifth Amendment privilege is not triggered where, as here, "the [g]overnment merely compels some physical act, *i.e.*, where the individual is not called upon to make use of the contents of his mind." *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1345 (11th Cir. 2012).

That rule dooms the Federal Public Defender's "decryption" argument, as well. There, it contends that the government gaining access to the Subject Devices using the Subject's fingerprint or other biometric feature is testimonial under the Fifth Amendment because it not only unlocks the device but translates encrypted data on it "into a format that can be used and understood by the government." *Amicus Curiae* Mem. at 4. Thus, *amicus* argues, the use of the Subject's fingerprint "actually *assembles* the information for law enforcement," like the Supreme Court found problematic in *Hubbell*. *Id.* at 5 (emphasis added). But, again, the government's compelled use of the Subject's biometric features in order to decrypt the contents of the Subject Devices will not require the Subject to make any use of the contents of his mind. Similarly, there has been no

showing here that the resulting process of decryption requires any mental effort by the Subject;[11] rather, it would appear that the decryption process is accomplished by the machine—that is, by the digital device and the software on it.

Hubbell and *In re Subpoena Duces Tecum* are instructive. In *Hubbell*, the Supreme Court held that the subpoena respondent's "assembly" of information for the government—a concept that *amicus* invokes in its argument—can constitute a testimonial act of production. However, the respondent's "assembly of literally hundreds of pages of material in response to a request for 'any and all documents reflecting, referring, or relating to any direct or indirect sources of money or other things of value received or provided to' an individual or members of his family during a 3-year period," *Hubbell*, 530 U.S. at 41, required significantly more than is at issue here—and not because it involved physical documents rather than digital data. For example, it required the witness to cull through materials to determine which were responsive and "was tantamount to answering a series of interrogatories asking a witness to disclose the existence and location of particular documents fitting certain broad descriptions." *Id.* The biometric feature collection process outlined in the Affidavit requires no comparable cognitive exertion by the Subject here.

The Eleventh Circuit in *In re Subpoena Duces Tecum* found that compelled decryption of information on a number of digital devices did violate the Fifth Amendment. 670 F.3d at 1352–

[11] Neither party presented a clear description of the state of data on a digital device before and after it is unlocked, failing to explain whether application of a biometric feature merely unlocks the device or actually decrypts the data on it. Nor is the case law particularly helpful in this regard. For example, in *In re Subpoena Duces Tecum*, the court simply states that the target was ordered "to produce the unencrypted contents of [certain] hard drives," that "the decryption and production of the hard drives would require the use of Doe's mind," and referring in passing to a "decryption password," without clearly defining or explaining what is meant by "decryption," the manner in which the decryption would be accomplished, or how, precisely, it would involve the contents of the target's mind. 670 F.3d at 1341, 1346. Nevertheless, for purposes of the analysis in this Opinion, the Court assumes that information on any of the Subject Devices is otherwise "encrypted" and that unlocking the device also "decrypts" its contents. The Court does not assume, however, that the Subject has anything to do with the decryption process other than providing the biometric feature that unlocks the device.

53. That case is readily distinguishable from the facts in this case, however. As the Eleventh Circuit found, the decryption of information "require[d] [the witness] to use a decryption password," and thus to "use . . . the contents of [his] mind" in an action "akin to requiring the production of a combination." *Id.* at 1346; *see also Hubbell*, 530 U.S. at 43 (indicating that requiring production of a combination to a wall safe would be testimonial); *In re Boucher*, No. 2:06-mj-91, 2007 WL 4246473, at *6 (D. Vt. Nov. 29, 2007) ("The password is not a physical thing. If [the witness] knows the password, it exists only in his mind. . . . It is pure testimonial production . . . ."), *rev'd on other grounds*, 2009 WL 424718 (D. Vt. Feb. 19, 2009); *Massachusetts v. Gelfgatt*, 11 N.E.3d 605, 614 (Mass. 2014) ("This is not simply the production of real or physical evidence like a blood sample or a handwriting exemplar. Rather, the defendant's act of entering a decryption key would be a communication of his knowledge about particular facts that would be relevant to the Commonwealth's case."); *but see Florida v. Stahl*, 206 So. 3d 124, 134 (Fla. Dist. Ct. App. 2016) (holding compelled production of passcode non-testimonial). Here, as discussed above, the Subject would be required to communicate nothing: law enforcement will present the device and choose which of the Subject's fingers (or other biometric features) to use in an attempt to unlock it. The decryption is then accomplished without any further interaction with the Subject; it is accomplished not by the mental effort of the Subject but by the device itself. Like the unlocking of the device, the decryption could be effectuated even if the Subject were "asleep—and thus by definition not communicating anything."[12] *In re Search Warrant Application*, 279 F. Supp. 3d at 804.

[12] At oral argument, the Federal Public Defender posited that one whose cellphone can be accessed and decrypted using a fingerprint has used the contents of his or her mind to set up that security feature and that, therefore, the compelled unlocking via the fingerprint *a fortiori* reveals the contents of his or her mind. The problem with that argument is that *configuring* the device to use the fingerprint (or face or iris) to unlock and decrypt it was not compelled; only the present *use* of the fingerprint has been compelled. *See, e.g.*, *United States v. Doe*, 465 U.S. 605, 611–12 & n.9 (1984) (voluntarily-produced documents cannot be said to contain compelled testimony); *Fisher v. United States*, 425 U.S. 391, 409–10 (1976) ("[T]he preparation of all of the papers sought in these cases was wholly

* * * * *

Like other courts addressing similar issues, this Court is mindful of the important privacy interests at stake when government accesses information on a digital device. *See, e.g.*, *Carpenter*, 585 U.S. at __, slip op. at 10 ("[C]ell phone location information is detailed, encyclopedic, and effortlessly compiled."); *Riley*, 573 U.S. at __, 134 S. Ct. at 2485 ("Cell phones . . . place vast quantities of personal information literally in the hands of individuals."); *In re Search Warrant Application*, 279 F. Supp. 3d at 806 (noting "the intensity of the privacy interests at stake in accessing smart devices"). However, even when presented with legal questions impacted by changing technology that has triggered significant modifications of individuals' behavior, a lower court cannot ignore or rewrite the constitutional principles the Supreme Court has articulated. Rather, this Court's job is to interpret and apply those precedents as faithfully as possible. *See, e.g.*, *In re Search Warrant Application*, 279 F. Supp. 3d at 806–07 ("[A]lthough *Riley* certainly instructs courts to avoid mechanical application of legal principles in the fact of technological advances, the constitutional text dictates the result here"). Here, those principles establish that the warrant and authorization requested by the government and issued by the Court violates neither the Fourth Amendment's requirements nor the Fifth Amendment's self-incrimination clause.[13]

---

voluntary, and they cannot be said to contain compelled testimonial evidence . . . ."); *In re Boucher*, 2007 WL 4246473, at *3 ("Both parties agree that the contents of the laptop do not enjoy Fifth Amendment protection as the contents were voluntarily prepared . . . ."). It therefore is irrelevant that the individual who set up the device engaged the contents of his or her mind at an earlier point. If law enforcement compels disclosure of a combination, that disclosure is testimonial not because the user of the safe previously chose that combination, but because, in the compelled revelation of the combination, that individual is using the contents of his or her mind. *See, e.g.*, *In re Boucher*, 2007 WL 4246473, at *6 ("The password is not a physical thing. If [the witness] knows the password, it exists only in his mind. . . . It is pure testimonial production . . . .").

[13] In its opening memorandum, the government argues that its request regarding the use of biometric features was authorized under Rule 41 of the Federal Rules of Criminal Procedure, which governs search and seizure warrants. Government Mem. at 12–14. *Amicus* did not address that question in its opposition. The Court need not decide that question, however, because, even if Rule 41 does not countenance an authorization such as this, the government is correct that the All Writs Act, 18 U.S.C. § 1651, does. Government Mem. at 14 n.7. For example, in *United States v. Apple MacPro Computer*, the Third Circuit indicated that the All Writs Act authorized an order requiring a suspect in a child pornography case to decrypt digital devices subject to search during the execution of a search warrant

III. CONCLUSION

For the foregoing reasons, the government's application for a search warrant including authorization to compel the use of the Subject's biometric features such as his fingerprints, face, or irises to unlock any Subject Devices found at the premises to be searched was granted.

Date: June 26, 2018

_____
G. MICHAEL HARVEY
UNITED STATES MAGISTRATE JUDGE

because the suspect was related to the underlying controversy, compliance with the order required minimal effort, and without the suspect's assistance the authorized search warrant could not be successfully accomplished. 851 F.3d 238 (3d Cir. 2017) (citing *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 174–75 (1977)); *see also United States v. Spencer*, No. 17-cr-259, 2018 WL 1964588, at *4 (N.D. Cal. Apr. 26, 2018) (order requiring defendant to decrypt devices authorized under All Writs Act).