UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**Criminal No. 21-cr-178-APM**
	:	
PETER SCHWARTZ, et al.	:	
	:	
Defendant.	:	**Pre-Trial Conference: October 21, 2022**

UNITED STATES' OPPOSITION
TO DEFENDANT PETER SCHWARTZ'S MOTION TO SUPPRESS

The United States of America, by and through its attorney, opposes "Defendant Peter Schwartz's Motion to Suppress," (ECF No. 121), in which he seeks to suppress as evidence at trial any records taken from his cell phone. According to defendant Schwartz, the cell phone evidence must be suppressed because at the time that his phone was searched, FBI "agents did not have a warrant for Mr. Schwartz's phone and Mr. Schwartz did not give permission to the agents to search his phone," making the "warrantless search and seizure of Mr. Schwartz's phone [] unreasonable and illegal." Def.'s Mot. at 1. The defendant further claims that the use of his fingerprint to unlock his phone violated his rights under the Fourth and Fifth Amendments. Id.

At the time they arrested Schwartz on February 4, 2021, law enforcement officers had a valid warrant to seize and search his phone and to compel him to provide his fingerprint or other biometric characteristics to unlock it. Such a compelled use of biometric characteristics is permissible under the Fourth and Fifth Amendments to the Constitution and the officers did not violate the defendant's rights when they unlocked Schwartz's phone and conducted a cursory initial search.

Thereafter, on September 16, 2021, law enforcement officers sought a second search warrant for the defendant's phone for the purpose of conducting a complete forensic extraction of the cell phone that was seized, unlocked, and cursorily searched on February 4, 2021. Although the initial February 2021 warrant authorized a full forensic extraction, the extraction was not immediately conducted due to an oversight. When that oversight was discovered, law enforcement then sought the September 2021 search warrant to ensure that the subsequent search was lawful. A full forensic extraction was conducted after the court approved the second search warrant on September 16, 2021. It appears that the defendant seeks to suppress the contents of his cell phone as recovered during both the February and September searches. The United States submits that there is no legal or factual basis for suppression and asks the court to deny the defendant's motion.

Factual Background

On January 6, 2021, defendant Peter Schwartz was among the thousands of individuals who traveled to Washington D.C. and who later breached the restricted area of the United States Capitol grounds. While present in the restricted area on the West Front of the Capitol Building, defendant Schwartz allegedly engaged in violence, including by throwing a chair toward the line of law enforcement officers and by spraying toward officers with chemicals such as oleoresin capsicum spray. The defendant traveled to Washington D.C. with his wife, Shelly Stallings, who was also charged with assaulting federal officers and entered a plea of guilty on August 24, 2022.

During the course of the investigation into defendant Schwartz's activities on January 6, 2021, the United States sought multiple warrants, including a warrant for his arrest, which was signed by a magistrate judge in the District of Columbia on January 29, 2021, and a warrant for the search his residence pursuant to Rule 41, which was signed by a magistrate judge in Pennsylvania on February 4, 2021. The search warrant for defendant Schwartz's residence in

Uniontown, PA, sought authorization to seize and to search digital devices, among other items, that may contain evidence of the alleged crimes. Attachment A of the residential warrant specifically permitted law enforcement to seek the *compelled* display of biometric characteristics – such as a fingerprint – in order to carry out the search of any digital devices that may be seized pursuant to the warrant. Specifically, law enforcement was authorized by the express terms of the warrant to:

> obtain from SCHWARTZ (but not any other individuals present at the **TARGET PREMISES** at the time of execution of the warrant) the *compelled display of any physical biometric characteristics* (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of…
>
> …for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant. (emphasis added)

On February 4, 2021, law enforcement simultaneously executed both the arrest warrant and the search warrant on defendant Schwartz's residence.[1] Upon arriving at Schwartz's home, law enforcement encountered defendant Schwartz outside of the residence and placed him in handcuffs for the purpose of arresting him. Shortly thereafter, he was placed inside of a law enforcement vehicle where F.B.I Special Agent Matthew Solomon conducted a custodial interview. Defendant Schwartz initially waived his right to remain silent and voluntarily spoke with law enforcement. During the time in which Schwartz voluntarily spoke with law enforcement, he made numerous statements regarding his presence in Washington D.C. on January

[1] In his suppression motion defendant Schwartz indicates that he "was arrested at his home in Uniontown, Pennsylvania" on February **2**, 2021. (ECF No. 121, p. 1, 2). This is factually inaccurate. Defendant Schwartz was not arrested until February **4**, 2021, when both the arrest warrant and residential search warrant were simultaneously executed at his Pennsylvania home.

6, 2021. He also indicated that he did have a cell phone, that he had taken that cell phone with him to the Capitol, and that phone – an Android device – was inside of his residence. After initially voluntarily speaking with SA Solomon, defendant Schwartz later asked for an attorney, at which time the interview was concluded.

While Schwartz was in the vehicle being interviewed by SA Solomon, other law enforcement officers remained inside of the residence to conduct the search, as authorized by the residential search warrant signed on February 4, 2021. While inside the residence, Special Agent Mike Nealon seized a Black Samsung Galaxy S10+ cell phone, IMEI 356021701533525, that was later determined to belong to Schwartz. After seizing the cell phone, SA Nealon observed that the phone was locked. As the warrant permitted law enforcement to search any seized digital devices, SA Nealon located Schwartz and asked if Schwartz, who was in handcuffs at the time and still voluntarily speaking with law enforcement, knew the password to the phone. Schwartz voluntarily indicated that he could not recall the passcode but offered three possibilities. SA Nealon entered each of these possible passcodes into the phone, but none successfully opened the phone.

In a hearing on any factual issues related to the initial search of Schwartz's phone, the United States anticipates that SA Nealon will testify that he does not recall the precise method by which Schwartz's finger was used to unlock the phone. Nevertheless, SA Nealon is expected to testify that after seizing the phone inside of the residence and failing to open the phone with Schwartz's proposed passwords, he then approached Schwartz a second time to compel his fingerprint to unlock the phone, as permitted by the express terms of the warrant. SA Nealon will testify that he does not recall the specific conversation with Schwartz regarding unlocking the phone, but that his practice is to invite an arrestee to use biometrics to open their phone for another reason – such as to obtain phone numbers from the phone – and to keep the phone unlocked from

that point to facilitate a subsequent search. SA Nealon will testify unequivocally that at no time did law enforcement engage in physical force with respect to Schwartz. During the search and arrest, law enforcement did not "shove[] Mr. Schwartz into the wall," and did not "snatch[] his phone out of his hands and walk[] away, laughing." Def. Mot. at 2. Additionally, at no time during the search or seizure did Schwartz indicate that he would not give "permission" to search his phone.[2] Further, SA Nealon will testify that neither he, nor any other agent indicated to Schwartz that that they would "get a warrant for [the phone] later" as law enforcement already had a valid warrant to search the phone as of February 4, 2021, when it was seized.

Once defendant Schwartz unlocked his cell phone using his fingerprint, and while conducting the residential search on February 4, 2021, law enforcement began a search of the phone as permitted by the warrant. In that initial review, law enforcement found multiple text messages that were within the scope of the warrant, including text messages containing a photograph of Schwartz at the United States Capitol, as well as messages indicating that while at the Capitol Schwartz had thrown a chair at officers and had also stolen O.C. spray belonging to police officers. During the cursory search of the phone on February 4, 2021, the officers photographed the specific text messages that they located.

When a phone is seized, law enforcement will typically search the phone by extracting the full contents of the phone and then sorting the contents into materials that are within the scope of the warrant and those that are outside of the scope of the warrant. Due to an oversight, however, law enforcement officers did not complete the full cell phone extraction as authorized by the

[2] The United States submits that any facts related to whether Schwartz gave law enforcement "permission" to search the phone are irrelevant for purposes of the suppression motion as law enforcement never requested consent to search Schwartz's Samsung Galaxy S10+ and, instead, relied solely on the terms of the warrant to search the contents of the phone.

warrant signed on February 4, 2021. Instead, they conducted the initial cursory search while at the defendant's residence and then placed the physical phone in storage as evidence. When the oversight was discovered, the officers then sought a second warrant out of an abundance of caution in order to ensure that any subsequent search of the phone was conducted in a lawful manner rather than rely on a warrant that was more than seven months old. In the affidavit submitted in support of that warrant, law enforcement described the initial seizure and search of Schwartz's cell phone on February 4, 2021, the use of Schwartz's fingerprint to unlock the phone, and the fact that the extraction had not been completed following the phone's seizure.

On September 16, 2021, District of Columbia Magistrate Judge Zia Faruqui signed the second warrant to search defendant's Schwartz's Samsung Galaxy S10+. A search of the cell phone – specifically a forensic extraction of its contents – was then completed as authorized by the September 16, 2021 warrant. The extracted contents of the phone contain additional evidence related to Schwartz's participation in the violence at the United States Capitol on January 6, 2021.

Argument

I. Agents Had a Valid Warrant in Advance of the Seizure and Search of the Defendant's Phone

The Fourth Amendment provides in relevant part that "[t]he right of 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." U.S. Const. amend IV. The prohibition on warrantless searches, with some exceptions, generally applies to the search of cellular phones and other digital devices. See Riley v. California, 573 U.S. 373 (2014).

Contrary to the defendant's representations, the United States fully complied with the requirement to obtain a warrant based upon probable cause in advance of seizing and searching defendant Schwartz's cellular phone. Thus, the defendant's motion should be denied as meritless.

On the morning of February 4, 2021, Western District of Pennsylvania Magistrate Judge Patricia Dodge approved a residential search warrant for Schwartz's residence in Uniontown, Pennsylvania. That warrant approved a search of the residence and permitted law enforcement to also *seize and search*, among other items, any "digital devices" that were either used in the commission of the offense or were capable of containing evidence of the crimes. "Digital devices," under the terms of the warrant, include items such as cellular phones. After that warrant was signed by the court, law enforcement simultaneously executed both the arrest warrant and residential search warrant in the afternoon of February 4, 2021. Upon arriving on the scene, FBI agents placed Schwartz in handcuffs on the front porch of his residence. Other agents then searched the inside of the residence and seized, among other items, a Black Samsung Galaxy S10+ cell phone, IMEI 356021701533525. That cellular phone was later determined to belong to defendant Schwartz.

After lawfully seizing the Samsung Galaxy S10+, law enforcement then engaged in a cursory search of the phone by scrolling through text messages and other contents which were immediately visible. Law enforcement also took photographs of specific text messages and photos identified in this initial search of the phone. As detailed above, the warrant expressly approved the search of the phone's contents, as well as the compelled use of the defendant's biometric characteristics to unlock the phone.

In his motion, the defendant inexplicably claims that his phone was seized and searched on February 2, 2021, two days in advance of his arrest or the search of his home. This unsupported claim is inaccurate, as the phone was not seized or searched until the afternoon of February 4, 2021, several hours after the search warrant was signed. As the defendant does not appear to be challenging the validity of the warrant, only the timing of when the warrant was executed, the

court should reject the defendant's claim that the United States unlawfully searched his phone and should deny his suppression motion a meritless.

II. The Use of Mr. Schwartz's Fingerprint to Unlock his Phone Did not Violate His Rights Under the Fifth Amendment

The court should also reject the defendant's claim that his Fourth and Fifth Amendment rights were violated by the use of his fingerprint to unlock his Samsung Galaxy S10+ on February 4, 2022. Significantly, the warrant discussed above specifically permitted the compelled use of defendant Schwartz's biometric characteristics, such as his fingerprint, to unlock the phone. Moreover, it is established practice in the District of Columbia to seek the compelled use of biometric characteristics and prior litigation in this jurisdiction has established that such a compelled use does not offend the Constitution.

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. To qualify for Fifth Amendment privilege against self-incrimination, a communication must be: (1) testimonial, (2) incriminating, and (3) compelled. See *In re* Search [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 534 (D.D.C. 2018, M.J. Harvey) (citing Hiibel v. Sixth Jud. Dist. Ct., 542 U.S. 177, 189 (2004)); Doe v. U.S., 487 U.S. 201, 207 (1988). To be testimonial, a communication "must itself, explicitly or implicitly, relate a factual assertion or disclose information." Doe, 487 U.S. at 210.

In this jurisdiction, the most careful analysis of whether the compelled use of biometric data violates the Fifth Amendment was undertaken in *In re* Search [Redacted] Wash., D.C., in which Magistrate Judge Michael Harvey clarified that a warrant seeking biometric data was both "compelled" and "likely to be incriminating." Id. at 534. Nevertheless, the court found that the compelled use of biometric data was "not testimonial" and, therefore, did not violate the Fifth Amendment. Unlike compelling a defendant to communicate a password, which would be

"testimonial" under the Fifth Amendment, the court described compelling biometric data as "more akin to the surrender of a safe's key rather than its combination." Id. at 535.

In laying out its reasoning, the court compiled other types of compelled acts that higher courts have similarly found to be non-testimonial for Fifth Amendment purposes. For example, compelling a defendant to provide a handwriting example, wear particular clothing, stand in a lineup, and provide a voice sample do not violate the Fifth Amendment privilege against self-incrimination. Id. (citing Schmerber v. California, 384 U.S. 757, 765 (1966), Gilber v. California, 388 U.S. 263, 266-67 (1967), U.S. v. Dionisio, 410 U.S. 1,7 (1973), U.S. v. Wade, 388 U.S. 218, 221-22 (1967), and Holt v. U.S., 218 U.S 245, 252-53 (1910)). Courts have also recognized that the key feature underpinning the nontestimonial nature of these acts of production is that they do not require the subject to use the "contents of his own mind" to explicitly or implicitly communicate a statement of fact. See Curcio v. U.S., 354 U.S. 118, 128 (1957); *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1135, 1145 (11th Cir. 2012); Schmerber v. California, 384 U.S. 757, 764 (1966); Doe, 487 U.S at 211-12. This subtle distinction is best illustrated by the Court's analogy in Hubbell between telling an inquisitor the combination to a wall safe and being forced to surrender the key to a strongbox. U.S. v. Hubbell, 530 U.S. 27, 43 (2000). There, the Court found that compelled disclosure of the existence of incriminating documents was testimonial and violated the Fifth Amendment. See Id. at 45; but see Doe, 487 U.S. at 216-17 (finding that compelled signature of a consent directive authorizing banks to disclose records in the hypothetical was not testimonial and reasoning that the signature itself shed no light on the suspect's state of mind and authentication evidence would need to be provided by the bank).

Here, the February 4, 2021, residential search warrant specifically authorized the "*compelled* display of any physical biometric characteristics" for the purpose of unlocking digital

devices seized pursuant to the warrant. Contrary to the defendant's claims, the warrant did not require the defendant to provide his biometric characteristics "voluntarily."[3] During the search, law enforcement approached defendant Schwartz regarding unlocking his phone and he ultimately unlocked it using his own fingerprint, whereby law enforcement took physical possession of the phone. While S.A. Nealon does not have a specific recollection of the conversation, his past practice is to request that an arrestee unlock the phone for another reason and to reclaim the phone after it is unlocked. S.A. Nealon anticipates that he followed his past practice in obtaining the use of Schwartz's fingerprint here. The agent's approach to obtaining Schwartz's fingerprint was permissible under the warrant, which permitted Schwartz's fingerprint to be compelled.

In fact, and in the alternative, S.A. Nealon's approach to obtaining Schwartz's fingerprint here can be viewed as successfully obtaining his fingerprint by consent, even where the warrant would have allowed compulsion. To determine whether a communication was compelled for Fifth Amendment purposes, courts consider whether it was "free and voluntary; that is, (it) must not be extracted by any sort of threats or violence, nor obtained by any direct or implied promises, . . . nor by the exertion of any improper influence." See Malloy v. Hogan, 378 U.S. 1, 7 (1964). Courts look at the totality of the circumstances when determining whether a communication was involuntary. See Haynes v. Washington, 373 U.S. 503, 514 (1963). At a hearing on this motion the United States expects law enforcement to testify unequivocally that no violence, force, threats, or promises were involved in obtaining Schartz's fingerprint. Instead, S.A. Nealon asked Schwartz to unlock the phone – albeit without informing him that unlocking the phone would facilitate a

[3] The warrant did, however, specify that a passcode, as distinct from biometric features, or other similar information that could only be obtained verbally, could not be compelled and could only be provided on a voluntary basis. As noted above, a defendant's provision of a passcode would be "testimonial" whereas the provision of a fingerprint is not.

search – and then physically took the phone back from Schwartz once it was unlocked. Schwartz unlocked the phone of his own free will, even if under the mistaken impression that he was opening the phone only for his own purposes. Thus, the evidence is expected to show that Schwartz's fingerprint was ultimately obtained by consent, even where the warrant allowed compulsion.

Because the agents had a valid warrant to seize and search Schwartz's phone and also lawfully obtained his fingerprint to unlock the phone, the court should deny the defendant's motion to suppress the evidence obtained from his cell phone. To the extent Schwartz's fingerprint was obtained via compulsion rather than consent, which the government does not concede, the search warrant obtained in advance of the search of the phone specifically and lawfully authorized the compelled use of Schwartz's biometric data to unlock he phone

For the reasons addressed above, and for any reasons stated at a hearing on this issue, the defendant's motion should be denied.

Respectfully submitted,

MATTHEW M. GRAVES
United States Attorney
D.C. Bar No. 481052

By: */s/ Jocelyn Bond*
JOCELYN BOND
Assistant United States Attorneys
D.C. Bar No. 1008904
555 Fourth Street, N.W.
Washington, D.C. 20530
(202) 809-0793
Jocelyn.Bond@usdoj.gov