**IN THE UNITED STATES DISTRICT COURT**

**FOR THE DISTRICT OF COLUMBIA**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA** | : | |
| **v.** | : | **Case No. 21-CR-178 (APM)** |
| **PETER J. SCHWARTZ,** | : | |
| **Defendant.** | : | |

**DEFENDANT PETER J. SCHWARTZ'S SUPPLEMENTAL MEMORANDUM OF LAW IN SUPPORT OF HIS MOTION TO SUPPRESS**

Defendant Peter J. Schwartz ("Mr. Schwartz"), by and through undersigned counsel, respectfully submits this supplemental memorandum of law in support of his motion to suppress records illegally obtained from his cell phone [ECF 121].

## I. INTRODUCTION

The evidence presented at the suppression hearing held on October 21, 2022, demonstrates that Mr. Schwartz's cell phone had a numerical passcode that could also be unlocked using biometric data such as a fingerprint. While in custody, and while protected by his Fifth Amendment rights which were not knowingly and intelligently waived, Mr. Schwartz was deceived by law enforcement into using his fingerprint to provide them with access to his phone. With such access the law enforcement agents then searched Mr. Schwartz's phone and took photographs of text messages and other records.

The initial search of Mr. Schwartz's cell phone violated his Fourth and Fifth Amendment rights, specifically his privilege against self-incrimination. While in custody, and without being read his *Miranda* warnings, Mr. Schwartz's phone was unlocked with the use of his fingerprint. *See Miranda v. Arizona*, 384 U.S. 436 (1966).

As set forth in detail below, the use of biometric data constituted a testimonial communication and is protected by the privilege against self-incrimination under the Fifth Amendment. Furthermore, any consent obtained by law enforcement officers was done so through deception and therefore constitutes an improper purpose. For the foregoing reasons, Mr. Schwartz's phone was unconstitutionally seized and searched.

## II. FACTUAL BACKGROUND

On February 2, 2021, FBI agents entered Mr. Schwartz's residence in Uniontown, Pennsylvania, handcuffed Mr. Schwartz and placed him under arrest.[1] In addition to having a warrant for his arrest, the federal agents who took him into custody had also obtained a search and seizure warrant from the Western District of Pennsylvania. Among the items authorized to be seized and searched pursuant to that warrant was Mr. Schwartz's phone. Notably, FBI Special Agent Matthew B. Solomon's affidavit in support of the search warrant in this case unambiguously states that biometric data may not be obtained by force.

Upon his arrest, FBI agents found what they believed to be his cell phone on a dresser in Mr. Schwartz's residence. The agents were unable to access any information stored on the phone, however, because the passcode security feature was enabled. Notwithstanding his custodial status, without the presence of counsel, without being advised of any rights, and without a knowing and intelligent waiver of his rights being secured, the law enforcement agents engaged Mr. Schwartz in conversation. One statement made to him was that they had a search warrant to seize his phone and that it would be marked and kept as evidence in his case. Mr. Schwartz was told that if there was information stored on his phone that he might need in the future—such as contact numbers for family, friends, or his attorney—he needed to access that

[1] Evidence deduced at the motions hearing before this Court on October 21, 2022, showed that Mr. Schwartz may have been arrested on February 4, 2021.

information before the phone was taken away, and it would be written down for him to have while he was in custody.[2] This was an obvious subterfuge used to gain access to the phone. Mr. Schwartz was then given his phone to use his fingerprint and unlock the phone. As soon as Mr. Schwartz did so one of the agents took the phone away from him and disabled the passcode security feature immediately. Mr. Schwartz was never given any phone numbers as was promised to him.

On September 16, 2021, the FBI filed another application for a warrant to search Mr. Schwartz's phone after it had already been examined. In the Affidavit submitted as part of this application, Special Agent Emily Eckhart stated that Mr. Schwartz's fingerprint was used to bypass the security feature on the phone.

The government now seeks to present at trial said evidence that was illegally obtained from Mr. Schwartz's phone. On August 30, 2022, Mr. Schwartz filed the instant motion to suppress these records.

## III. ARGUMENT

### a. Mr. Schwartz's Fifth Amendment Rights were Violated.

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. This privilege only protects a person "against being incriminated by his own compelled testimonial communications." *Doe v. United States*, 487 U.S. 201, 207 (1988) (citing *Fisher v. United States,* 425 U.S. 391, 409 (1976)). Testimony is not restricted to verbal or written communications. A "testimonial communication" is some form of communication that either "explicitly or implicitly" relates to a

[2] The agent did not recall precisely what happened but stated that this was consistent with his standard practice.

"factual assertion or disclos[ure of] information." *Doe*, 487 U.S. at 210. In *Doe*, the Court stated that an "act of production could constitute protected testimonial communication because it might entail implicit statements of fact[.]" *Id.* at 208, (citing *United States v. Doe,* 465 U.S. 605, 613 (1984); *Fisher,* 425 U.S., at 409–410, 428, 432 (concurring opinion)).

To hold that the privilege against self-incrimination may be asserted only to resist compelled explicit or implicit disclosures of incriminating information would be consistent with the history of the Self-Incrimination Clause. The intention of the Self-Incrimination Clause was to "prevent the use of legal compulsion to extract from the accused a sworn communication of facts which would incriminate him." *Doe,* U.S. 201 at 212. The Supreme Court in *Murphy v. Waterfront Comm'n of New York Harbor*, held the privilege against self-incrimination is founded on:

> our unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt; our preference for an accusatorial rather than an inquisitorial system of criminal justice; our fear that self-incriminating statements will be elicited by inhumane treatment and abuses; our sense of fair play which dictates 'a fair state-individual balance by requiring the government to leave the individual alone until good cause is shown for disturbing him and by requiring the government in its contest with the individual to shoulder the entire load,' ...; our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life,' our distrust of self-deprecatory statements; and our realization that the privilege, while sometimes 'a shelter to the guilty,' is often 'a protection to the innocent.'

378 U.S. 52, 84 (1964). Some actions may be compelled by police that do not constitute testimonial communications such as compelled blood samples, handwriting exemplars, voice exemplars, and standing in a lineup. *Doe*, 487 U.S. at 210 (citing *Schmerber v. California*, 384 U.S. 757, 765 (1966); *Gilber v. California*, 388 U.S. 263, 266–267 (1951); *United States v. Dionisio*, 410 U.S. 1, 7 (1973); *United States v. Wade*, 388 U.S. 218, 221–222 (1967)). In these

cases, the Supreme Court held that the privilege was not implicated because the suspect was not required "to disclose any knowledge he might have." *Doe*, 487 U.S. at 210–11 (citing *Wade,* 388 U.S., at 222–223; *Dionisio,* 410 U.S., at 7; *Gilbert,* 388 U.S., at 266–267). The "extortion of information from the accused," or any attempt to force the accused to "disclose the contents of his own mind," implicates the Self–Incrimination Clause. *Doe*, 487 U.S. at 211 (citing *Couch v. United States,* 409 U.S. 322, 328 (1973); *Curcio v. United States,* 354 U.S. 118, 128 (1957)).

Testimony is not restricted to verbal or written communications. *Schmerber,* 384 U.S. at 763-64 (the privilege extends to "an accused's communications, whatever form they might take."); *see also Wade*, 388 U.S. at 218, 223 (finding that the privilege may apply not only to verbal communications, but also to physical communications). Acts that imply assertions of fact can constitute testimonial communication for the purposes of the Fifth Amendment. *See Doe*, 487 U.S. at 208.

Many courts have previously found that a passcode cannot be compelled under the Fifth Amendment, because "[t]he expression of the contents of an individual's mind falls squarely within the protection of the Fifth Amendment." *See Doe*, 487 U.S. at 219 (citing *Boyd v. United States*, 116 U.S. 616, 633-635 (1886); *see also Fisher*, 425 U.S. at 409.

In *In the Matter of the Search of a Residence in Oakland, California*, the Northern District of California found that "[i]f 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." Case No. 4-19-70053 (N.D. Ca. January 10, 2019); *see also United States v. Wright*, 431 F. Supp. 3d 1175, 1187-88 (D. Nev. 2020) (holding that unlocking a defendant's phone with his face infringed the Fifth Amendment's privilege against self-incrimination, and was an abuse of power and is

unconstitutional). The court further found 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." *Id.* (*citing Schmerber*, 384 U.S. at 764.

Similarly, 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). The court in that case further noted that 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." *Ibid.*

Here, the use of a fingerprint to unlock Mr. Schwartz's cell phone constitutes a "testimonial communication" because it is explicitly, or at the very least, implicitly seeking to determine a factual assertion of who possesses the phone or disclose information regarding the ownership and contents of the phone. *See Doe* 487 U.S. at 210. While blood samples, handwriting exemplars, voice exemplars, and the standing in a lineup do not constitute testimonial communications, the government in those examples already possesses knowledge of ownership and is not seeking to deduce any additional evidence. *Ibid.*

When requesting biometric data from Mr. Schwartz to unlock his cellular device, this is requiring Mr. Schwartz to disclose knowledge that he does in fact possess this cellular device and that the contents of said device can be attributed to him—text messages or emails which he composed or received, photographs or videos which he recorded. As such, using Mr. Schwartz's biometric data to unlock his phone constitutes an "extortion of information from the accused"

and is seeking to force the accused to "disclose the contents of his own mind." *Doe*, 487 U.S. at 211 (citing *Couch,* 409 U.S. at 328; *Curcio*, 354 U.S. at 128).

The government relies on Magistrate Judge Harvey's decision in *In re Search [Redacted] Wash., D.C.,* 317 F. Supp. 3d 523, 534, 538-39 (D.D.C. 2018, M.J. Harvey) for its assertion that the use of biometric data to unlock an accused's phone is not testimonial pursuant to the Fifth Amendment. However, Judge Harvey's decision ineffectively attempts to distinguish the compelled testimony of providing a passcode and the use of biometric data to unlock a phone. A biometric feature is functionally the same as a passcode, and because telling a law enforcement officer your passcode would be testimonial, so too must the compelled use of your biometric feature to unlock a device. *See In the Matter of the Search of a Residence in Oakland*, at 1015-16.

Magistrate Judge Harvey also compares the use of biometric features to the surrender of a safe's key rather than its combination. *In re Search [Redacted] Wash., D.C.,* 317 F. Supp. 3d at 535 (citing *Hubbell*, 530 U.S. at 43). This comparison, however, fails because a safe's key is essentially the same as a safe's combination. It does not matter whether it is a key or a combination which unlocks a safe because both are intended for the same purpose and communicate the same information—they both unlock a safe and convey that the owner of the key/combination has possession over the safe and its contents.[3]

[3] There are, of course, times when using a key to open a safe would not be a testimonial act. For example, if law enforcement agents found a key in a lock itself or on a piece of furniture beside a safe, the use of that key would not involve a testimonial act, just as if agents correctly guessed the combination of a safe. The act is testimonial in nature where, as here, it identifies ownership or access to a place to be searched. Forcing the owner of a safe to identify the correct key from a large number of potential keys would undoubtedly be a testimonial act.

The compelled use of biometric data to unlock a cell phone is a testimonial communication and must be protected under the Fifth Amendment.

**b. Pretextual Reasons for why Mr. Schwartz's Phone was Unlocked were Required.**

The Fifth Amendment provides an individual with "the right … to remain silent unless he chooses to speak in the unfettered exercise of his own will, and to suffer no penalty[.] *Malloy v. Hogan*, 378 U.S. 1, 7–8 (1964). The Fifth Amendment further protects a person against testimonial communications that are "compelled". *Doe*, 487 U.S. at 207.

To determine whether a testimonial communication was compelled, 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, however slight, nor by the exertion of any improper influence." *See Malloy*, 378 U.S. at 7. 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). Further, "whether the confession was obtained by coercion or improper inducement can be determined only by an examination of all of the attendant circumstances." *Haynes v. State of Wash.*, 373 U.S. 503, 513–14 (1963). Additionally, the Supreme Court has held that the use of official pressure, fatigue, or sympathy, can constitute compulsion. *Malloy*, 378 U.S. at 8 (citing *Spano v. New York*, 360 U.S. 315, 323 (1959)).

As discussed in detail above and in his motion, the government used subterfuge to unlock Mr. Schwartz's phone by misleading him into providing a fingerprint so that they could snatch his phone from his hands to search and photograph it. Mr. Schwartz was not instructed on what agents would do once his phone was unlocked. Rather, he was told that he better unlock his phone to retrieve important contact information as he would not have access to his phone.

Special Agent Mike Nealon, who testified before this Court during the motions hearing, stated that he did not recall the exact circumstances which led to the unlocking of Mr. Schwartz's phone. Rather, SA Nealon testified that Mr. Schwartz was in a vehicle outside of the residence when he discovered the cell phone on a dresser in Mr. Schwartz's bedroom. He then allegedly returned to the vehicle and obtained three possible passcodes from Mr. Schwartz. He then allegedly went back inside, attempted to unlock the phone with the three alternative passcodes unsuccessfully and returned to the vehicle, where Mr. Schwartz mysteriously unlocked the phone and gave it to SA Nealon. SA Nealon then allegedly went inside once again where he handed the phone to another agent who proceeded to take photographs of records he found on Mr. Schwartz's phone. Besides the fact that SA Nealon's account of the events on that day strain credulity, the fact that he somehow does not recall how exactly Mr. Schwartz's biometric data was obtained is telling and supports the conclusion that it was not obtained voluntarily.

Mr. Schwartz, while in police custody, and not yet advised of his rights or the ability to consult with counsel, was deceived into providing consent to unlock his phone and to search its contents. This deception was done so through an improper influence and therefore violates the Fifth Amendment's privilege against self-incrimination.

## IV. CONCLUSION

Based upon the foregoing and the reasons set forth in his motion as well as before the Court during the motions hearing on October 21, 2022, Defendant Peter J. Schwartz respectfully requests that this Honorable Court will grant his motion to suppress.

Dated: October 28, 2022

Respectfully Submitted,

*/s/ Dennis E. Boyle*
Dennis E. Boyle
Blerina Jasari

Boyle & Jasari
1050 Connecticut Ave, NW
Suite 500
Washington, D.C., 20036
Email: dboyle@dennisboylelegal.com
bjasari@dennisboylelegal.com
Phone: (202) 798-7600

*Counsel for Defendant Peter Schwartz*

**CERTIFICATE OF SERVICE**

I hereby certify that on October 28, 2022, a true and correct copy of the foregoing document has been served electronically on counsel of record for all parties.

*/s/ Dennis E. Boyle*
Dennis E. Boyle, Esquire