

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA

v.

PETER J. SCHWARTZ,

Defendant.

:
:
:
:
:
:
:
:

: Case No. 21-CR-178 (APM)

DEFENDANT PETER SCHWARTZ’S MOTION TO SUPPRESS

Defendant Peter J. Schwartz (“Mr. Schwartz”), by and through undersigned counsel, respectfully moves to suppress as evidence any records taken from his cell phone at trial for the reasons set forth below.

I. INTRODUCTION

On February 2, 2021, Mr. Schwartz was arrested at his home in Uniontown, Pennsylvania. FBI agents restrained Mr. Schwartz with handcuffs, had Mr. Schwartz unlock his phone under false pretenses and snatched the phone out of Mr. Schwartz’s hands as soon as he unlocked it so they could search the phone.

At the time of the search, the 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. The warrantless search and seizure of Mr. Schwartz’s phone was unreasonable and illegal. As such, any evidence obtained as a result of this seizure must be suppressed.

II. FACTUAL BACKGROUND

On January 6, 2021, Mr. Schwartz travelled to Washington, D.C., with his wife, Shelley Stallings, to attend a protest in support of former President Donald J. Trump. He was one of thousands of individuals who then walked to the U.S. Capitol after Trump issued a call to action.

On February 2, 2022, Mr. Schwartz was arrested in his home in Uniontown, Pennsylvania, on an arrest warrant issued by the United States District Court for Western District of Pennsylvania. After FBI agents detained Mr. Schwartz by putting handcuffs on him and restraining him, they told him that “[he] would not have his phone when he [gets] to jail, so if [he] needed to get any phone numbers out of it, [he] better do it right then.” With his hands still handcuffed to his waist, Mr. Schwartz unlocked his phone.

As soon as he unlocked his phone, one of the FBI agents shoved Mr. Schwartz into the wall, while another agent snatched his phone out of his hands and walked away, laughing. Mr. Schwartz then yelled that he was not giving them permission to access his phone and that he would never give them permission to access his phone. The agent continued to laugh and said they would get a warrant for it later. The agent proceeded to search Mr. Schwartz’s phone and took photographs of text messages.

On February 4, 2022, two days after Mr. Schwartz’s arrest, the FBI requested and obtained a search warrant which authorized agents to use biometrics to unlock digital devices on the premises to be searched. Special Agent Matthew B. Solomon’s affidavit in support of the application, however, clarifies that such data may not be obtained by force. Specifically, paragraph 70 of the affidavit which was filed under seal states as follows:

The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned

person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), **the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.**

Case No. 2:21-mj-00238-PLD (ECF 5) (emphasis added).

On September 16, 2021, the FBI seemingly noticed its mistake and filed an application for a warrant to search Mr. Schwartz's phone. *See* Case No. 1:21-sw-00303-ZMF (ECF 2).

Paragraph 38 of Attachment B to the application states that "[d]ue to an oversight, after the FBI agents captured screenshots of text messages from [Mr.] Schwartz's phone, the phone data was not forensically extracted and the phone was not searched further despite a signed search warrant authorizing such a search, and no data has been extracted to-date." Paragraph 33, of the Attachment states that FBI agents used Mr. Schwartz's fingerprint to unlock his phone. However, it neglects to state that Mr. Schwartz was tricked into unlocking his phone and that he did not provide his fingerprint voluntarily as set forth in Special Agent Solomon's affidavit. In fact, Mr. Schwartz was pushed against a wall as he was yelling that he would not and never grant permission for agents to search his phone.

In a Second Superseding Indictment, Mr. Schwartz has been charged with three counts of Assaulting, Resisting, or Impeding Certain Officers Using a Dangerous Weapon, in violation of 18 U.S.C. § 111(a)(1) and (b) (Counts One, Three, and Four); one count of Civil Disorder, in violation of 18 U.S.C. § 231(a)(3) (Count Two); one count of Assaulting, Resisting, or Impeding Certain Officers Using a Dangerous Weapon and Aiding and Abetting, in violation of 18 U.S.C. § 111(a)(1) and (b) and 2 (Count Seven); one Count of Obstruction of an Official Proceeding and Aiding and Abetting, in violation of 18 U.S.C. § 1512(c)(2) and 2 (Count Eight); one count of Entering and Remaining in a Restricted Building or Grounds with a Deadly or Dangerous

Weapon, in violation of 18 U.S.C. § 1752(a)(1) and (b)(1)(A) (Count Nine); one count of Disorderly and Disruptive Conduct in a Restricted Building or Grounds with a Deadly or Dangerous Weapon, in violation of 18 U.S.C. § 1752(a)(2) and (b)(1)(A) (Count Ten); one count of Engaging in Physical Violence in a Restricted Building or Grounds with a Deadly or Dangerous Weapon, in violation of 18 U.S.C. § 1752(a)(4) and (b)(1)(A) (Count Eleven); one count of Disorderly Conduct in the Capitol Grounds or Buildings, in violation of 40 U.S.C. § 5104(e)(2)(D) (Count Twelve); and one count of Act of Physical Violence in the Capitol Grounds or Buildings, in violation of 40 U.S.C. § 5104(e)(2)(F) (Count Thirteen). [ECF 63].

On February 4, 2021, Mr. Schwartz had his initial appearance in the Western District of Pennsylvania. Subsequently, Mr. Schwartz was committed to and transferred to the District of Columbia.

III. ARGUMENT

1. Standard of Review.

The Fourth Amendment guarantees 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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. “A search conducted without a warrant is ‘per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.’” *United States v. Maynard*, 615 F.3d 544, 566 (D.C. Cir. 2010) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)).

It is well-established that law enforcement must obtain either a warrant or consent to search electronic devices such as cell phones. *See Riley v. California*, 134 S. Ct. 2473 (2014). Coercion, both physical and psychological, is prohibited from being used to obtain consent. *See*

United States v. Hernandez, 2015 WL 5007821 (W.D.N.C. July 28, 2015) (“Coercion may be actual or implied, and ‘no matter how subtly the coercion was applied, the resulting ‘consent’ would be no more than a pretext for unjustified police intrusion against which the Fourth Amendment is directed.’ [T]he government must prove that ‘an individual freely and intelligently [gave] ... unequivocal and specific consent to search, uncontaminated by any duress or coercion, actual or implied.’”) (citing *Schneckloth v. Bustamonte*, 412 U.S. 218, 228 (1973); *U.S. v. Morrow*, 731 F.2d 233, 235-36 (4th Cir. 1984)).

The Fifth Amendment provides that no person “shall be compelled in any criminal case to be a witness against himself.” U.S. Const. amend. V. The proper inquiry is whether an act would require the compulsion of a testimonial communication that is incriminating. *See Fisher v. United States*, 425 U.S. 391, 409 (1976).

2. Use of Mr. Schwartz’s Fingerprint Violated his Constitutional Rights.

The use of Mr. Schwartz’s fingerprint to unlock his phone violated his Fourth and Fifth Amendment rights.

A passcode entered into a cell phone, which is designed to keep the contents of the phone hidden from others, is generally considered by society to be something private that should be free from warrantless intrusion by the government. *See Oliver v. United States*, 466 U.S. 170, 177–78 (1984); *cf. Riley v. California*, 573 U.S. 373, 393–98 (2014) (detailing the weighty privacy interests persons have in the contents of their cell phones); *see also United States v. Booker*, 561 F. Supp. 3d 924, 931 (S.D. Cal. Sept. 17, 2017) (finding that defendant’s Fourth and Fifth Amendment rights were violated after defendant was ordered to place phone in plain view and input passcode in front of FBI agents).

Furthermore, courts have previously found that a passcode cannot be compelled under the Fifth Amendment, because the act of communicating the passcode is testimonial, as “[t]he

expression of the contents of an individual's mind falls squarely within the protection of the Fifth Amendment." *See Doe v. United States*, 487 U.S. 201, 219 (1988) (citing *Boyd v. United States*, 116 U.S. 616, 633-635 (1886); *See also Fisher*, 425 U.S. at 409).

"Testimony is not restricted to verbal or written communications." *See In the Matter of the Search of a Residence in Oakland, California*, Case No. 4-19-70053 (N.D. Ca. January 10, 2019) (request to compel owners of any phones and other devices to unlock them using their fingerprints denied because request went "overboard"). Acts that imply assertions of fact can constitute testimonial communication for the purposes of the Fifth Amendment. *Doe*, 487 U.S. at 208. 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." *Id.*; *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 v. California*, 384 U.S. 757, 764 (1966)).

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.” *Id.*

As set forth in detail above, Mr. Schwartz was arrested on February 2, 2022, and a search warrant was obtained two days later which allowed for biometrics to be used to unlock his phone, **if and only if Mr. Schwartz voluntarily provided said information.** Mr. Schwartz was coerced into providing his fingerprint to unlock his phone and made clear that he was not giving permission to agents to search his phone after FBI agents snatched Mr. Schwartz’s phone out of his hands. Nevertheless, FBI agents searched and photographed his phone without a warrant and without his consent. *Miranda v. Arizona*, 384 U.S. 436, 476 (1966) (“[A]ny evidence that the accused was threatened, tricked, or cajoled into a waiver will, of course, show that the defendant did not voluntarily waive his [Fifth Amendment] privilege.”); *Colorado v. Spring*, 479 U.S. 564, 573 (1987) (citation omitted) (“[T]he relinquishment of the right must have been voluntary in the sense that it was the product of a free and deliberate choice rather than intimidation, coercion, or deception.”).

The obtaining of Mr. Schwartz’s fingerprint constituted an unlawful warrantless search under the Fourth Amendment and was compelled in violation of the Fifth Amendment. As such, the information seized as a result of these violations must be suppressed.

CONCLUSION

WHEREFORE, based upon the foregoing, Defendant Peter J. Schwartz respectfully requests that this Honorable Court will grant his motion to suppress.

Respectfully submitted,

/s/ Dennis E. Boyle

Dennis E. Boyle
Boyle & Jasari

1050 Connecticut Ave, NW
Suite 500
Washington, DC 20036
dboyle@dennisboylelegal.com
bjasari@dennisboylelegal.com
Telephone: (202) 430-1900

Counsel for Defendant Peter J. Schwartz

CERTIFICATE OF SERVICE

I hereby certify that on this 30th day of August 2022, I electronically filed the foregoing document with the Court using the CM/ECF system, which sent notification of such filing to all counsel of record.

/s/ Dennis E. Boyle
Dennis E. Boyle