UNITED STATES DISTRICT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Case No. 1:21-cr-00178-APM
	)	
PETER SCHWARTZ,	)	
	)	
Defendant.	)	

DEFENDANT'S MOTION TO SUPPRESS

INTRODUCTION

Comes now Defendant Peter Schwartz, by and through is counsel of record, John M. Pierce, and hereby moves this court for an order suppressing the search of his Samsung Galaxy S10 cellular telephone.

The searches were only accomplished because of violations of Mr. Schwartz's rights under the Fourth, Fifth and Sixth Amendments to the Constitution by law enforcement agents. Mr. Schwartz's cellular telephone had a numerical passcode feature enabled which prevented the phone from being opened and accessed without the passcode being entered.

While in custody, and while protected by his Fourth Amendment and Fifth Amendment rights which were not knowingly and intelligently waived, Mr. Schwartz was deceived by law enforcement in a manner that tricked him into providing them with access to his cellular telephone, and with such access the law enforcement agents who had violated his rights in a custodial setting, did disable the passcode feature. This made it possible to later search the cellular telephone pursuant to warrants obtained from federal district court magistrate judges.

FACTUAL BACKGROUND

Defendant Peter Schwartz was arrested at his residence in Uniontown Pennsylvania on February 4, 2021.

In addition to having a warrant for his arrest, the federal agents who took him into custody also had obtained a search and seizure warrant from a magistrate judge in the Western District of Pennsylvania. Among the items authorized to be seized and searched pursuant to that warrant as a Samsung Galaxy S10 cellular telephone.

Upon making entry into the residence, Mr. Schwartz was placed under arrest and handcuffed. At that point Mr. Schwartz was in a "custodial" status, and all his relevant Fifth and Sixth Amendment rights applied.

After finding the Galaxy cellular telephone and discovering that the passcode security feature was enabled, the law enforcement agents present were unable to access information stored on the telephone such as text messages, email, photographs, and video data.

Notwithstanding his custodial status, without the presence of counsel, 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 telephone 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 information before the phone was taken away, and it would be written down for him to have while he was in custody. Mr. Schwartz was then given his phone to type in the passcode and unlock the phone. As soon as Mr. Schwartz did so the agent took the phone away from him and disabled the passcode security feature.

The initial search warrant obtained by the government, pursuant to which the cellular telephone was seized, authorized the agents to use biometric information from Mr. Schwartz to bypass or unlock any safety feature. In the Affidavit submitted as part of the application for a

subsequent search warrant, Special Agent Emily Eckhart stated that Mr. Schwartz's fingerprint was used to bypass the security feature on the phone consistent with the warrant's authorization. Mr. Schwartz disputes that claim as set forth above.

With the phone unlocked, the agents reviewed text messages, emails, stored photographs, and stored video.[1] Information taken from the phone has now been produced in discovery, and the defendant believes the government intends to use some/all of that evidence in its case-in-chief at trial.

ARGUMENT

The use of security features on cellular telephones that employ biometric identification technology, such as facial scans or fingerprint readers, is a burgeoning area of legal controversy. The government has represented to this Court in an affidavit that it employed a biometric means of gaining access to Mr. Schwartz's cellular telephone at the time of his arrest and the seizure of his telephone, i.e., it used his fingerprint to unlock the phone, consistent with authority granted to it under the terms of the warrant.

Mr. Schwartz denies that the security feature of his phone was bypassed in this fashion. Mr. Schwartz's telephone had a numeric passcode feature enabled. The agents executing the warrant did not ask him for the code, as doing so without a waiver of rights in a custodial situation would have violated the Fifth Amendment, and would subjected the item found during the search to likely suppression.

[1] The government obtained a second search warrant from this Court on September 16, 2021. According to the Affidavit of Special Agent Emily Eckert, the second search warrant was necessary because the cellular telephone had not been fully searched and data exploited in a timely fashion after the first search warrant was issued. Eckert Affidavit, at P. 19, ¶ 38.

But what the agents did was functionally no different than obtaining Mr. Schwartz's consent to search his phone by deception, and they did so while he was in custody, not yet advised of his rights, and without the opportunity to consult with counsel or at least know of his right to consult with counsel on the subject of unlocking his phone.

The Fourth Amendment protects "[tjhe right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." "The 'basic purpose of this Amendment,' our cases have recognized, 'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.'" Carpenter v. United States, 138 S. Ct. 2206, 2213, 201 L. Ed. 2d 507 (2018) (quoting Camara v. Mun. Court of City & Cty. of San Francisco, 387 U.S. 523, 528 (1967)). If the Government had probable cause to search the phone, it still had to comport itself with the limitations of the Fourth Amendment in doing so. If the government violated a different constitutional right in the course of executing a lawfully issued warrant, that violation renders the subsequent search unreasonable.

The challenge facing the courts and the citizenry is that technology is outpacing the law. In recognition of this reality, the Supreme Court has instructed lower courts to adopt rules that "take account of more sophisticated systems that are already in use or in development." Carpenter, 138 2 S. Ct. at 2218-19. (quotation omitted). Courts have an obligation to safeguard constitutional rights and cannot permit those rights to be diminished merely due to the advancement of technology. Id., at 2214. The existence of a valid warrant to search a phone does not permit the Government to compel a suspect to waive rights otherwise afforded by the Constitution, including the Fifth Amendment right against self-incrimination, in its efforts to execute that warrant.

The question here is whether deceiving Mr. Schwartz for the purpose of getting him to unlock his cellular phone by inputting the passcode number is "testimonial" under the Fifth Amendment. Was he tricked into communicating by his actions information known only to him in the form of transferring that information into his phone for the benefit of the government and to his personal and legal detriment?

How was the conduct engaged in by Mr. Schwartz in response to the deceptive instructions of the government meaningfully different than what a hearing-impaired subject might do by responding to questioning with sign language? Neither would use his voice, but both would convey information to the government agents by use of hands and fingers in response to the deception.

Securing digital devices is not new but the means by which such security is afforded to the owners of the devices has evolved and advanced in ways that make them nearly impossible for law enforcement to bypass with available electronic countermeasures. Courts have for a considerable time considered passcodes as information that cannot be compelled under the Fifth Amendment, because the act of communicating the passcode by a defendant is "testimonial", as "[t]he expression of the contents of an individual's mind falls squarely within the protection of the Fifth Amendment." See Doe v. United States, 487 U.S. 201, 219 (1988) (Stevens, J., dissenting) (citing Boyd v. United States, 116 U.S. 616, 633-635 (1886); Fisher v. United States, 425 U.S. 391, 420 (1976)

Testimony is not restricted to verbal or written communications. Acts that imply assertions of fact can constitute testimonial communication for the purposes of the Fifth Amendment. Doe, 487 U.S. at 208. It was long ago established that certain types of compelled acts are not "testimonial" because the actions produce physical evidence -- furnishing a blood

sample, submitting to fingerprinting, providing a handwriting or voice exemplar, or standing in a lineup are all "compelled acts" which are not testimonial so they do not violate the Fifth Amendment. Doe, 487 U.S. at 210.

But the transmission of numeric passcode information certainly involves the thought processes of a defendant, is not independent inculpatory evidence on its own, and is therefore "testimonial" in nature.

REQUEST FOR A FRANKS HEARING

Although there is a "presumption of validity" with respect to affidavits in support of search warrants, Franks v. Delaware, 438 U.S. 154, 171, 98 S.Ct. 2674 (1978), a court is required to hold an evidentiary hearing "where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause." Id. at 155-56, 98 S.Ct. 2674; see also United States v. Dale, 991 F.2d 819, 843 (D.C.Cir. 1993);

As the D.C. Circuit has instructed, "a defendant is entitled to an evidentiary hearing only if his attack on the accuracy of the affidavit is `more than conclusory' and is accompanied by `allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof.'" United States v. Gaston, 357 F.3d 77, 80 (D.C.Cir. 2004) (quoting Franks, 438 U.S. at 171, 98 S.Ct. 2674) (emphasis added).

The government has claimed in an affidavit that the Defendant's cellular telephone was accessed via an authorized biometric feature – his fingerprint – which would have involved no "testimonial" information from him protected by his rights under the Fifth and Sixth Amendment. Mr. Schwartz's offer of proof is that he was deceived by the agents executing the

warrant into communicating to them the numeric passcode that only he knew without his consent. The subsequent search and exploitation of the phone's contents violated the Fourth Amendment as an unreasonable search.

Date: December 1, 2021

Respectfully Submitted,

John M. Pierce
355 S. Grand Avenue, 44th Floor
Los Angeles, CA 90071
Tel: (213) 400-0725
Email: jpierce@piercebainbridge.com

CERTIFICATE OF SERVICE

I, John M. Pierce, hereby certify that on this day, December 1, 2021, I caused a copy of the foregoing document to be served on all counsel through the Court's CM/ECF case filing system.

/s/ John M. Pierce
John M. Pierce