IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF IDAHO

IN THE MATTER OF THE SEARCH OF: A white Google Pixel 3 XL cellphone in a black Incipio case.	Case No. 1:19-mj-10441-REB ORDER DENYING APPLICATION FOR A SEARCH WARRANT

SUMMARY OF DECISION

The Court denies the Government's application for a warrant authorizing law enforcement to compel an individual to use his/her fingerprints to unlock a certain cellphone. Using the individual's fingerprints for this purpose would constitute a search and seizure under the Fourth Amendment. For a search and seizure to be lawful under the Fourth Amendment it must be "reasonable." A search or seizure is unlawful, and therefore unreasonable, when it violates a person's constitutional rights. Here, compelling the use of the individual's fingerprints violates the Fifth Amendment right against self-incrimination because the compelled unlocking of the phone with fingerprints would communicate ownership or control over the phone. Because the compelled use of the individual's fingerprints violates the Fifth Amendment, the search and seizure would not be reasonable under the Fourth Amendment. Thus, the Fourth Amendment and the Fifth Amendment prohibit the result sought by the Government.

BACKGROUND

The Government is investigating an individual[1] believed to be involved in possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). This Court previously approved

[1] The individual was arrested on a criminal complaint, but the warrant application at issue here remains under seal. Hence, the individual's identity will not be disclosed in this decision.

an application for a search and seizure warrant authorizing a search of the individual, a vehicle, and a residence. The warrant permitted seizure of "desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware" if such "constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense." 1:19-mj-10436-REB Dkt. 2 at 6, 9 (sealed).

That warrant was served at the residence. Among other things, law enforcement officers seized a Google Pixel 3 XL cellphone from a bathroom in the residence. However, the phone is "locked" and requires a swipe pattern or a fingerprint to unlock it. Law enforcement presently lacks the ability to unlock the phone and examine its contents forensically in that manner.

After the warrant was served, an authorized law enforcement officer brought a sworn criminal Complaint against the individual. Based upon that Complaint, this Court signed a bench warrant authorizing the individual's arrest. The same day, the Government applied for an additional search warrant authorizing law enforcement "to compel [the individual] to provide biometric input needed to unlock the . . . cellphone . . . . [by] press[ing] any finger and/or thumb of any hand of [the individual] against the sensor of the fingerprint reader used to unlock the . . . phone." Aff. in Supp. of App. for Search Warrant 14. The Government seeks such authorization "for the purpose of unlocking, or logging into the phone in order to search for evidence of … crime(s), indicia of ownership, and other information and evidence." *Id.* The Government represents in its application for this subsequent warrant that, when asked about his/her phone, the individual stated that it was in the bathroom where the individual had been prior to answering the door. This decision addresses constitutional issues raised by the Government's application.

DISCUSSION

An application for a search warrant to compel use of a person's fingerprints[2] to unlock a cellphone implicates both the Fourth and Fifth Amendments of the U.S. Constitution, as described to follow.

A. Fourth Amendment Analysis

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. It recognizes "the sanctity of a man's home and the privacies of life" and prohibits "the invasion of his indefeasible right of personal security, personal liberty, and private property." *Boyd v. United States*, 116 U.S. 616, 630 (1886). "[T]he principal object of the Fourth Amendment is the protection of privacy rather than property . . ." *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 304 (1967). The Amendment's "basic purpose . . . is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Carpenter v. United States*, 138 S.Ct. 2206, 2213 (2018) (citation omitted). Such protection extends to cellphones, and generally law enforcement must obtain a warrant before searching a cellphone. *Riley v. California*, 573 U.S. 373 (2014). "[T]he ultimate touchstone of the Fourth Amendment is reasonableness." *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006) (citation and quotation marks omitted).

Neither the individual who is the subject of the application nor any other person has had an opportunity to argue against the Government's application. However, "the Fourth

[2] As the term is used in this decision, "fingerprints" includes fingerprints and thumbprints. There is no meaningful distinction between a fingerprint and a thumbprint for purposes of the legal analysis in this decision.

Amendment has interposed a magistrate between the citizen and the police. . . . not to shield criminals" but "so that an objective mind might weigh the need to invade that privacy in order to enforce the law." *McDonald v. United States*, 335 U.S. 451, 455 (1948).

On the strength of the Government's original application and its supporting affidavit, this Court found probable cause to permit a lawful search and seizure of the subject individual's cellphone, so long as it "constitute[s] evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense." 1:19-mj-10436-REB Dkt. 2 at 6, 9 (sealed). But such search and seizure must comport with the Fourth Amendment. A search and seizure is unreasonable, and therefore unlawful, if it violates the person's Fifth Amendment rights. *Boyd*, 116 U.S. at 634–635 (implicitly overruled on other grounds by *Hayden*, 387 U.S. 294 (1967)).[3] Thus, assuming arguendo that the proposed search and seizure otherwise comports with the Fourth Amendment,[4] the Government's application turns on whether the individual's Fifth Amendment rights would be violated by the search and seizure.

B. Fifth Amendment Analysis

Under the Fifth Amendment, no person "shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend V. It is intended "to spare the accused from

[3] In *Hayden*, the Court abrogated *Gouled v. United States*, 255 U.S. 298 (1921), and the analysis within *Gouled* that under *Boyd* searches and seizures equivalent to compulsory production of a person's private papers violate the Fifth Amendment and are therefore unreasonable. 387 U.S. at 301–310. But the Court has never taken the step of formally overruling *Boyd*. Regardless, the overruled holding of *Boyd* is not implicated here because the compulsory production sought in this case is not of the individual's private papers, which extensive case law holds are not protected by the Fifth Amendment. Rather, the compulsory production sought here is to use the individual's fingerprints to attempt to unlock a seized phone. *Boyd* applies here to the extent it holds that a search and seizure is unreasonable if it violates a person's Fifth Amendment rights.

[4] This Court previously found probable cause to seize mobile phones at the residence.

having to reveal, directly or indirectly, his 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). "The privilege afforded not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime." *Hoffman v. United States*, 341 U.S. 479, 486 (1951). "The values protected by the Fourth Amendment . . . substantially overlap those the Fifth Amendment helps to protect." *Schmerber v. California*, 384 U.S. 757, 767 (1966) (overruled on other grounds by *Missouri v. McNeely*, 569 U.S. 141 (2013)).

"There is no special sanctity in papers, as distinguished from other forms of property, to render them immune from search and seizure, if only they fall within the scope of the principles of the cases in which other property may be seized, and if they be adequately described in the affidavit and warrant." *Andresen v. Maryland*, 427 U.S. 463, 474 (1976) (quoting *Gouled v. United States*, 255 U.S. 298, 309 (1921)). However,

> "A party is privileged from producing the evidence but not from its production." *Johnson v. United States*, 228 U.S. 457, 458 (1913). This principle recognizes that the protection afforded by the Self-Incrimination Clause of the Fifth Amendment "adheres basically to the person, not to information that may incriminate him." *Couch v. United States*, 409 U.S. 322, 328 (1973). Thus, although the Fifth Amendment may protect an individual from complying with a subpoena for the production of his personal records in his possession because the very act of production may constitute a compulsory authentication of incriminating information, *see Fisher v. United States*, . . . a seizure of the same materials by law enforcement officers differs in a crucial respect the individual against whom the search is directed is not required to aid in the discovery, production, or authentication of incriminating evidence.

Id. at 473–474.

Moreover, "the protection of the privilege reaches an accused's communications, whatever form they might take, and the compulsion of responses which are also

communications." *Schmerber*, 384 U.S. at 764. To qualify for the privilege, a communication must be (1) testimonial, (2) incriminating, and (3) compelled. *Hiibel v. Sixth Jud. Dist. Ct. of Nev., Humboldt Cnty.*, 542 U.S. 177, 189 (2004). Each prong is considered in turn.

1. Testimonial Communication

The protections against self-incrimination contained in the Fifth Amendment are not limited to verbal or written communications. *Matter of Residence in Oakland, Cal.*, 354 F. Supp. 3d 1010, 1015 (N.D. Cal. Jan. 10, 2019); *see also In the Matter of the Search of [Redacted] Wash., D. C.*, 317 F. Supp. 3d 523, 534–535 (D.D.C. June 26, 2018); *United States v. Maffei*, 2019 WL 1864712, Order Granting Mot. to Suppress Evid. at *6 (N.D. Cal. Apr. 25, 2019). The Supreme Court has held that the very "act of producing evidence" in certain circumstances "has communicative aspects of its own" that may qualify as testimonial. *Fisher v. United States*, 425 U.S. 391, 410 (1976). That is, a witness's "act of production itself could qualify as testimonial if conceding the existence, possession and control, and authenticity of the documents tended to incriminate them." *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1343 (11th Cir. 2012) (citing *Fisher*, 425 U.S. at 410).

Even so, some otherwise arguably incriminating acts are not within the Fifth Amendment privilege. Furnishing a blood sample, for instance, or providing a handwriting or voice exemplar, standing in a lineup, or submitting to fingerprinting for identification purposes are not testimonial communications because such actions do not require the suspect "to disclose any knowledge he might have" or to "speak his guilt." *Doe*, 487 U.S. at 210–211 (citations omitted). The relevant distinction is the "extortion of information from the accused, . . . the attempt to force him to disclose the contents of his own mind." *Id.* at 211 (citations omitted).

Here, however, the Government seeks to compel the individual to use his/her fingerprint

to attempt the unlocking of a cellphone seized at the residence. Indeed, the Government acknowledges that one purpose for doing so is to "search for . . . indicia of ownership." Aff. in Supp. of App. for Search Warrant 14. Thus, the Government seeks evidence that the individual's fingerprint unlocks the phone not simply to access its contents but also to establish the individual's possession and control of the phone and knowledge of its contents. For either purpose, compliance with a warrant authorizing an attempt by law enforcement to unlock the phone with the individual's fingerprints inescapably requires a compelled testimonial communication because the individual would provide a "compulsory authentication of incriminating information" and would "aid in the discovery, production, or authentication of incriminating evidence."[5] *Andresen*, 427 U.S. at 474.

2. Self-incrimination

The Fifth Amendment privilege against self-incrimination "protects against any disclosures which the witness reasonably believes 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, 444–445 (1972). In *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, the Eleventh Circuit held that decryption and production of the contents of computer hard drives would be testimonial, rather than merely a physical act, because decryption and production

[5] The applicant avers that, when questioned at the residence at the time the earlier search warrant was executed, the individual told law enforcement his/her phone was in the bathroom. A phone was found in a bathroom, and the application implies that the individual was not in the bathroom when that statement was made. But three other phones were also located during the search. There is no specific information about how many bathrooms were in the residence. There is no information about whether the individual lives alone or whether anyone else lives or was in the residence at the time of the search. To be clear, none of these facts are determinative of the Court's conclusion in this case. But they do illustrate that any connection between the individual and the phone at issue here is more tenuous than it might be under other circumstances.

"would be tantamount to testimony by Doe . . . of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files." 670 F.3d at 1346. The Circuit panel rejected the Government's analogy distinguishing a key from a numerical combination to open a lock, finding that Doe's production of the unencrypted files would be "more than a physical nontestimonial transfer" because such production would necessarily be "accompanied by the implied factual statements noted above [regarding an association with the drives and a capability to decrypt them] that could prove to be incriminatory." *Id.* Moreover, requiring a person to aid law enforcement by unlocking a device using biometrics can potentially incriminate where the act of providing such aid makes it more likely that the person had locked the device in the first place, which in turn makes it more likely that the device was in the person's possession, custody, or control. *See United States v. Spencer*, 2018 WL 1964588, Order Denying Mot. for Relief from Order of Mag. Judge *2 (N.D. Cal. Apr. 26, 2018).

Such reasoning echoes the holding in *In re Application for a Search Warrant*, 236 F. Supp. 3d 1066 (N.D. Ill. Feb. 16, 2017), where the court held that providing a fingerprint key to unlock a smartphone does explicitly or implicitly relate a factual assertion or disclose information:

> The connection between the fingerprint and [the phone's] biometric security system, shows a connection with the suspected contraband. By using a finger to unlock a phone's contents, a suspect is *producing* the contents on the phone. With 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.

Id. at 1073 (footnote omitted).

The same constitutional heartwood is found in this case, where the use of the individual's biometrics (specifically, the fingerprints) may incriminate the individual by providing evidence

of some association or "relatively significant connection" with the phone and, therefore, its contents. Further, compelling the use of fingerprints to unlock the phone could "furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime." *Hoffman*, 341 U.S. at 486.

In sum, what the Government would characterize as innocuous is instead a potentially self-incriminating testimonial communication because it involves the compelled use of biometrics—unique to the individual—to unlock the phone. The Fifth Amendment does not permit such a result. The scenario is exactly within the rationale drawn in *Andresen* that "[a] party is privileged from producing the evidence but not from its production" and that "the very act of production may constitute a compulsory authentication of incriminating information." 427 U.S. at 473–474. The significant distinction is that the seizure of the same materials by law enforcement officers "differs in a crucial respect" because "the individual against whom the search is directed is not required to aid in the discovery, production, or authentication of incriminating evidence." *Id.* at 474.

Upon a proper showing under applicable law, the Government can, of course, search the contents of the device without the need to compel the owner of the cellphone to "unlock" the phone, if a means to do so exists without having to compel the use of biometrics. In such a circumstance, the Government can access the "contents" in some other manner, whether directly or indirectly.[6] But there is a critical distinction between whether the Government may seize the

[6] There are, of course, other investigative techniques to determine who owned or possessed the phone, such as seeking to lift fingerprints from the device or interviewing witnesses who might connect a specific individual to the phone. Further, the Government has investigatory methods available to it to seek stored communications and subscriber information regarding phones known to be used by a particular person, upon a proper showing.

phone pursuant to a search and seizure warrant, and the entirely separate question of whether the Constitution permits compelling the use of an individual's fingerprints so as to allow the Government to access the contents of the phone and, in so doing, establishing his or her connection to the phone.

3. Compulsion

To determine whether testimony has been compelled, courts examine "whether, considering the totality of the circumstances, the free will of the witness was overborne." *United States v. Anderson*, 79 F.3d 1522, 1526 (9th Cir. 1996) (quoting *United States v. Washington*, 431 U.S. 181, 188 (1977)). It is self-evident that the free will of the witness would be overborne on the facts presented by the warrant application; the Government, after all, seeks the Court's order to *compel* the use of the individual's fingerprints to attempt to unlock the phone. There is no consent here, and where consent is refused then the witness's "free will" is, by definition, absent. Consent and compulsion are diametrically different.

CONCLUSION

The Government's warrant application, if granted, would violate the subject individual's Fifth Amendment rights because it would compel the individual to give self-incriminating testimony. The Fifth Amendment protects the right not to incriminate oneself; therefore, the search and seizure would be unreasonable and not permitted under the Fourth Amendment.

For these reasons, the Government's application for a search and seizure warrant on the facts of this matter is hereby **DENIED**.

DATED: May 8, 2019

Honorable Ronald E. Bush
Chief U.S. Magistrate Judge