IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF IDAHO

IN THE MATTER OF APPLICATION FOR SEARCH WARRANT OF CERTAIN PREMISES, INDIVIDUAL, AND PERSONAL PROPERTY INCLUDING A SMARTPHONE	Case No. 1:19-mj-10467-S-REB AMENDED ORDER DENYING APPLICATION FOR A SEARCH WARRANT

SUMMARY OF DECISION

On June 7, 2019, this Court received an application for a search and seizure warrant from a law enforcement official authorized to apply for federal court search warrants pursuant to Rule 41 of the Federal Rules of Criminal Procedure. The application requests that the Court issue a search warrant authorizing law enforcement to search (1) a residence in a certain Idaho municipality; (2) a certain automobile described by make, model, and license plate number; and (3) the person of a named individual. The Government is investigating the individual on suspicion of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). In addition to seeking to conduct a search of the residence, automobile, and individual, the application also seeks authority to compel the individual to use his/her fingerprints to unlock a cellphone (also referred to in this decision as a smartphone) believed to belong to the individual. This Court has previously ruled that compelling the use of an individual's fingerprints to unlock a cellphone violates the Fifth Amendment right against self-incrimination because the compelled unlocking of a phone would communicate ownership or control over the phone. *In the Matter of the Search of: A White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 2019 WL 2082709 (D. Idaho May 8, 2019). The same concerns and the same constitutional protections exist in regard to a portion of the pending application in that the applicant requests that the Court compel

a person who is being investigated and who is a subject of the requested search and seizure warrant to provide biometric information (in the form of fingerprints placed upon a smartphone) to law enforcement to allow law enforcement to access the contents of the smartphone, if the biometric information allows access to the contents.

BACKGROUND

The application stems from an investigation of an individual as to whom law enforcement believes there is probable cause to conclude is guilty of a federal crime. The Government, through the applicant, contends that the requested warrant will uncover evidence of such crime.[1]

An affidavit submitted in support of the application describes evidence obtained from responses to administrative subpoenas and from the execution of search warrants previously issued by other courts. Such evidence, according to the affidavit, links the individual to various email addresses, online accounts, telephone numbers, IP addresses, and digital devices, including a smartphone. Further, the affidavit avers that the cellphone registered to the account is a specific make and model.

The affidavit describes a feature of the smartphone which, according to the investigator, offers users "the ability to unlock the device via the use of a fingerprint or thumbprint." It also describes that, in the investigator's "training and experience, cellular telephone users often enable" such a touch identification security feature "because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened

[1] Because the application is denied on other grounds, this decision does not address whether there is probable cause to grant the application.

concern about securing the contents of the device." The affiant also states that "[t]he passcode or password that would unlock the cellular telephone device found during the search of [the individual, the vehicle, or the residence] is not known to law enforcement. Thus, it will likely be necessary for law enforcement to press [the individual's] fingers and thumbs to the [smartphone] found during the search . . . in an attempt to unlock the device for the purpose of executing the search authorized by this warrant." However, the affidavit does not describe a particular reason to believe that the subject cellphone has enabled a touch identification feature or would have such feature enabled if the device were seized during execution of a search warrant.[2]

Attachment B to the application identifies "Particular Things to be Seized and Searched." Numbered paragraph 6 of Attachment B provides as follows:

> Biometric Authentication Data of the Subject– The Court authorizes law enforcement to compel [the individual] to provide biometric input needed to unlock the [smartphone], found to be on [his/her] person, in [his/her] vehicle, or in [his/her] residence listed in Attachment A. Law enforcement will be permitted to press any finger and/or thumb of any hand of [the individual] against the sensor of the fingerprint reader used to unlock the [smartphone] in order to search the contents as authorized by this warrant. This authorization is for the purpose of unlocking or logging into the phone in order to search for evidence of the aforementioned crime(s) and other information and evidence as outlined in this section.

DISCUSSION

An application for a search warrant to compel use of a person's fingerprints[3] to unlock a cellphone implicates both the Fourth and Fifth Amendments of the U.S. Constitution.

---

[2] Regardless of the constitutional issues, the application may also be premature and not ripe for decision. The applicant presupposes that a search will uncover and result in seizure of a specific smartphone at the time of the search but does not identify the device beyond a make and model and does not account for the possibility that a search might uncover additional or different devices.

[3] 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.

Significantly, the very nature of a smartphone is critical to the analysis. "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" *Riley v. California*, 573 U.S. 373, 403 (2014). Moreover, "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity." *Id.* "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of … protection." *Id.* at 393 (citation omitted). As described more fully by the Supreme Court in *Riley*:

> The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.
>
> Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. See Harris Interactive, 2013 Mobile Consumer Habits Study (June 2013). A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary. See, *e.g., United States v. Frankenberry*, 387 F.2d 337 (C.A.2 1967) (per curiam). But those discoveries were likely to be few and far between. Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. *See Ontario v. Quon*, 560 U.S. 746, 760, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010). Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.

Id. at 394–395 (footnote omitted).

Importantly, the protections of our Bill of Rights still place a frame upon the changes that technology have brought to society. "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter v. United States*, 138 S.Ct. 2206, 2214 (2018) (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)). Thus, in *Kyllo*, the Court rejected a "mechanical interpretation" of the Fourth Amendment that "would leave the homeowner at the mercy of advancing technology." *Kyllo*, 533 U.S. at 35.

It is with these principles in mind that the Court has reviewed the Government's instant application.

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). It "was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 573 U.S. at 403.

"[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). Its "ultimate touchstone . . . is reasonableness." *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006) (citation and quotation marks omitted). Basic to its purpose is the need "to safeguard the privacy

and security of individuals against arbitrary invasions by government officials," *Carpenter*, 138 S.Ct. at 2213 (citation omitted), and the protection of "people, not places," *Katz v. United States*, 389 U.S. 347, 351 (1967). Thus, it has long been understood that such protection extends to cellphones, so that a warrant in nearly every circumstance must be obtained before searching a cellphone. *See generally Riley*, 573 U.S. 373.

Here, there is no party to this matter who would have reason or opportunity to argue at this stage against the Government's application. Nonetheless, "the Fourth 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). As reiterated more recently by the Supreme Court in *Carpenter*, "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Carpenter*, 138 S.Ct. at 2214 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

Any search and seizure must comport with the Fourth Amendment. Understandably, therefore, the Fourth Amendment's requirement of reasonableness is undone if a search or seizure violates a person's Fifth Amendment rights. *Boyd*, 116 U.S. at 634–635 (implicitly overruled on other grounds by *Hayden*, 387 U.S. 294 (1967)).[4] Thus, assuming arguendo that

[4] 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 Supreme Court has never formally overruled *Boyd*; regardless, its 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 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.

the proposed search and seizure otherwise comports with the Fourth Amendment,[5] 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 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."

---

[5] As stated above, the Court does not here decide whether there is probable cause to issue any other portions of the requested warrant, as the application seeks the compelled use of the individual's fingerprints as part of the entire search and seizure.

> *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 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, an "act of production itself could qualify as testimonial if conceding the existence, possession and control, and authenticity of the documents tended to incriminate" the producing witness. *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 actions 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).

There is exactly that "extortion" of information here, however. The Government seeks to use the force of a search warrant to compel an individual to literally "open" the "privacies of [his/her] life," *Riley v. California*, 573 U.S. at 403, and, by doing so, "to conced[e] the existence, possession and control, and authenticity of the documents tend[ing] to incriminate him." *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d at 1343. The act of being forced to use one's fingerprint to successfully open the contents of a smartphone is the equivalent of forcing a tangible oral or written statement from that individual that he or she has at least some degree of possession and control of the phone and possession, control and knowledge of its contents.

Thus, compliance with a warrant authorizing law enforcement to force an individual to open the contents of a smartphone with the individual's fingerprints is a compelled testimonial communication. Doing so results in the individual providing a "compulsory authentication of incriminating information" that would "aid in the discovery, production, or authentication of incriminating evidence." *Andresen*, 427 U.S. at 474. It is no different than if law enforcement were to ask the person whether the cellphone belonged to him or her or whether the data stored

on the cellphone included something that would be unlawful for the person to possess.

The act of pressing the individual's fingers to the cellphone to try to unlock it would be tantamount to compelling him/her to answer. The Fifth Amendment does not permit such a result.

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 was testimonial, rather than merely a physical act, because decryption and production "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 comparing a key to a numerical combination to open a lock. Doe's production of the unencrypted files, the court said, 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.*

In an analogous decision, an Illinois federal trial court ruled that the use of a fingerprint "key" to unlock a smartphone is tantamount to a factual assertion or disclosure of information about the person's connection to that smartphone:

> 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.

In re Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. Feb. 16, 2017) (footnote omitted). Equally so, requiring a person to aid law enforcement by unlocking a device using biometrics is incriminatory as 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).

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. Hence, what the Government might 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. Significantly, 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 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.[7] There is

---

[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 person, upon a proper showing.

[7] Illustrative of this point is the pertinent language of the proposed warrant, which states: "The Court authorizes law enforcement to compel [the individual] to provide biometric input needed to unlock the [smartphone] . . . . Law enforcement will be permitted to press any finger and/or thumb of any hand of [the individual] against the sensor of the fingerprint reader used to unlock the [smartphone] . . . ."

no consent here, and where consent is not present or 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 the individual would be compelled 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 warrant on the facts of this matter is hereby **DENIED**.

DATED: June 27, 2019

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