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-DCN **DECISION AND ORDER ON REVIEW OF MAGISTRATE JUDGE'S ORDER**

I. INTRODUCTION

The United States seeks review of a Magistrate Judge's order denying the Government's search warrant application. Dkt. 5. The Government's application sought permission to place a subject's finger on a cellphone to unlock the phone to conduct a forensic search. The Magistrate Judge denied the application, ruling that the requested search warrant would violate the subject's Fifth Amendment rights. Dkt. 3. The Government subsequently filed a Motion to Reverse or Vacate the Magistrate's Order. Dkt. 5. Upon review, and for the reasons set forth below, the Court GRANTS the Government's Motion.

II. BACKGROUND

The Government was investigating an individual believed to be in possession of child pornography in violation of 18 U.S.C. § 2252(a)(5)(B). As part of that investigation, the Government properly obtained a search warrant authorizing a search of the individual, his vehicle, and his 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." Dkt. 3, at 2. The Government used the warrant to search the residence and to seize, among other things, a Google Pixel 3 XL cellphone from a bathroom in the residence.

The seized cellphone was "locked" and required a swipe pattern ("passcode") or a fingerprint to unlock it. After the original warrant was served, an authorized law enforcement officer brought a sworn criminal Complaint against the individual and the Magistrate Judge signed a bench warrant authorizing the individual's arrest. The Government then applied for an additional search warrant authorizing law enforcement to "compel [the subject] 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." Dkt. 3, at 2. The Government's stated purpose in seeking the authorization was "to authorize law enforcement to press the fingers, including thumbs, of [the subject] to the touch identification sensor on the Google Pixel 3 XL cellphone." Affidavit in Supp. Of App. for Search Warrant, Dkt. 2, at ¶ 18. The Government further represented in its application for the additional warrant that it already knew this particular cellphone belonged to the individual who was subject to the warrant because the individual stated—when questioned at his residence by police officers executing the warrant—that his phone was in the bathroom where he had been just prior to answering the door. The Google Pixel 3 XL cellphone was subsequently found in that bathroom.

The Magistrate Judge issued an order denying the additional warrant on the basis that the warrant, if granted, would violate the individual's Fifth Amendment rights because it would compel the individual to give self-incriminating testimony. The Magistrate Judge further held that the violation of the individual's Fifth Amendment rights would violate the Fourth Amendment.

The Government filed a motion with this Court to reverse or vacate the Magistrate Judge's order claiming that using a fingerprint to open a cellphone is not a Fifth Amendment violation. Additionally, the Government asserts there is a split at the magistrate judge level of this District Court on this issue.

III. JURISDICTION

The Federal Magistrates Act gives magistrate judges the authority to decide non-dispositive pretrial matters. *28 U.S.C. § 636(b)(1)(A).* Decisions regarding search warrants are part of that authority. *See Gomez v. United States,* 490 U.S. 858, 868 n.16 (1989). The Act also gives district judges the authority to review or reconsider any non-dispositive pretrial matter. *28 U.S.C. § 636(b)(1)(A); See also Fed. Rule Crim Proc. 59(b)(2) and (3).* Thus, the Magistrate Judge had the authority to issue the order and this Court has the authority to review the Magistrate Judge's order.

IV. MOOTNESS

The ability to unlock a cellphone with a fingerprint (biometric encryption) expires after 48 hours of not unlocking it. At that point, a passcode of some type must be used.

Here, it took the Magistrate Judge a few days to issue the order denying the warrant[1] and then took the Government eight days to file its motion for review. Consequently, any decision by the court in this case will have no impact on this case. The Government simply can no longer unlock the cellphone with a fingerprint. The issue is, therefore, moot under *County of Los Angeles v. Davis,* 440 U.S. 625, 631 (1979).

The Government argues that there are two exceptions to the mootness doctrine applicable here. First, the issue is capable of repetition yet evading review. Second, the two magistrate judges in the District of Idaho appear to be split regarding the use of biometrics in search warrants. Both exceptions will be discussed.

Article III of the Constitution limits federal court jurisdiction to "cases and controversies." *Hamamoto v. Ige,* 881 F.3d 719 (9th Cir. 2018). Thus, to qualify as a case fit for federal court jurisdiction, an actual controversy must be extant at all stages of review, not merely at the time the complaint is filed. *Davis v. Fed. Election Comm'n,* 554 U.S. 724, 732-33 (2008). An exception exists for controversies that are "capable of repetition, yet evading review." *Hamamoto,* at 721 (quoting *Kingdomware Techs, Inc. v. United States,* 136 S. Ct. 1969 (2016) ("Although a case would generally be moot in such circumstances, this Court's precedents recognize an exception to the mootness doctrine for a controversy that is 'capable of repetition, yet evading review.'")). According to the Ninth Circuit, that exception only applies in limited situations, where (1) the challenged action is in its duration too short to be fully litigated prior to cessation or expiration, and

[1] In no way is the Court criticizing the Magistrate Judge for taking a few days to issue his order. This is a complex legal question with courts throughout the country ruling on both sides of the issue.

(2) there is a reasonable expectation that the same complaining party will be subject to the same action again. *Hamamoto,* at 721. The Ninth Circuit further explained that to fit this "exceptional situation" exception, the controversy must be of inherently limited duration. *Id.* That is, the controversy will only ever present a live action until a particular date, after which the alleged injury will either cease or no longer be redressable. The limited duration of the controversy must be clear at the action's inception. *Id.*

In this case, the Government is the complaining party. The prevalence of cellphones continues to rise and the Government's applications for search warrants for biometric data likewise continues to rise. A search warrant must be processed within 48 hours of the Government's seizure of a cellphone or the biometric data becomes meaningless. This situation fits the "capable of repetition, yet evading review" exception to the mootness doctrine. The Court concludes that this motion can be heard and decided despite the mootness of the issue due to this exceptional situation.

This Court is not prepared to rule that this situation also fits the split of authority exception within this District. The Government has cited two cases in which one magistrate judge granted search warrants for biometric data relating to a cellphone. The Government then juxtaposes those two cases against this case to argue that a split exists within the District of Idaho as to how magistrate judges rule in this type of situation.

However, the Government has not cited to a single written decision—and none exists to the Court's knowledge—where a magistrate judge, or any judge from this District, has held that biometric data relating to a cellphone can be obtained by a warrant despite either Fourth Amendment or Fifth Amendment concerns. The mere fact that a

magistrate judge has signed search warrants that permitted law enforcement to use a person's biometrics to unlock electronic devices does not mean that the magistrate judge has had the opportunity to carefully and meaningfully decide the issue raised in this case. After all, the very *ex parte* nature of applications for search warrants does not lend itself to issues being raised as part of the process. It is not clear to this Court that there is a reasoned split of opinion between the magistrate judges in this District. This Court does not rely on the "split of authority" exception to address this issue.

V. DISCUSSION

In the original search warrant application, the Government sought authority to search an individual, a vehicle, and a residence. The Magistrate Judge found that the application established probable cause and signed the warrant. That probable cause finding is not at issue in this review. In the additional search warrant application, the Government sought authority to have law enforcement officers apply the individual's fingers to a cellphone found during the search of the residence.

The Magistrate Judge denied the authorization for biometric data, holding that the compelled pressing of the fingerprint to the cellphone sensor would violate the Fifth Amendment's privilege against self-incrimination. The Magistrate Judge reasoned that 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." Dkt. 3, at 9 (citing *Andresen v. Maryland*, 427 U.S. 463, 474

(1976)). This in turn, according to the Magistrate Judge, would violate the individual's Fifth Amendment rights because it would compel the individual to give self-incrimination testimony.

The compelled unlocking of digital devices using biometric means is an emerging area of law that raises both Fourth and Fifth Amendment concerns. There appears to be several decisions throughout the country that have addressed the issue in the federal district courts with mixed results. However, it also appears that neither the United States Supreme Court or any federal circuit court have addressed this issue.

One case relied upon by the Idaho Magistrate Judge is *In re Application for a Search Warrant,* 236 F. Supp. 3d 1066 (N.D. Ill. Feb. 16, 2017), where an Illinois Magistrate Judge held that providing a fingerprint to unlock a smartphone does explicitly or implicitly relate a factual assertion or disclose information in violation of the Fifth Amendment. The Government did not appeal or seek district judge review of that decision. However, five days later, in *In the Matter of the Search of: The SINGLE-FAMLY HOME AND ATTACHED GARAGE located at [redacted],* 2017 WL 4563870 (N.D. Ill. Feb. 21, 2017), a Magistrate Judge in the Northern District of Illinois again held that providing a fingerprint to unlock a smartphone relates a factual assertion or discloses information in violation of the Fifth Amendment. This time, the Government did seek review from a district judge. *See, In the MATTER OF the SEARCH WARRANT APPLICATION FOR [redacted text],* 279 F. Supp. 3d 800 (N.D. Ill. 2017). The facts of that Illinois case are substantially similar to the facts present in this case. The District

Judge reversed the decision of the Magistrate Judge and authorized the search warrant seeking to use biometric data to unlock a cellphone.

In doing so, the District Judge recognized:

> The privacy concerns at stake in government access to smart devices are intense, both because of the nature of the information that people store on those devices – pretty much every kind of information there is, from personal, financial, and professional – and because of the sheer volume of information that can be stored on them. But the constitutional text, as interpreted by governing case law, draws a distinction between compelling a person to *communicate* something to the government versus compelling a person to provide some *physical* characteristic as part of an investigation. Indeed, as the Supreme Court has explained, this distinction renders what is widely known as the "privilege against self-incrimination" as something of a misnomer. *United States v. Hubbell,* 530 U.S. 27, 34, 120 S. Ct. 2037, 147 L.Ed.2d 24 (2000) ("[t]he term 'privilege against self-incrimination' is not an entirely accurate description of a person's constitutional protection").

Id. at 803. The Illinois District Judge held that so long as the person being investigated was only compelled to provide a physical characteristic, *i.e.,* a fingerprint, instead of being compelled to provide a communication or thought process, there was no Fifth Amendment violation:

> Again, the fingerprint seizure itself does not reveal the contents of the person's mind in the way that disclosure of a passcode would or in the way that disclosure of a cryptography key would. Yes, compelling someone to reveal information on how to decrypt data is compelling testimony from that person. *But obtaining information from a person's mind is not what happens when agents pick a finger to apply to the sensor. So compelling physical access to information via the fingerprint seizure is no different from requiring someone to surrender a key to a safe whose contents otherwise would not be accessible to the government.* The surrender of the key may be compelled, but the compelling of the safe's combination is forbidden. *See Doe*, 487 U.S. at 210 n.9, 108 S. Ct. 2341 (signing generic consent form does not force a person "to express the contents of his mind," so it is more like surrendering a key rather than revealing the combination"). *The same principle applies here: a person generally cannot be compelled to disclose*

> *the passcode (like the safe's combination) but can be compelled to provide the fingerprint (like the key to the safe).*

Id. at 803 (emphasis added).[2]

A Magistrate Judge addressed this same issue in the DC circuit, in *In Matter of Search of [Redacted] Washington, District of Columbia,* 317 F. Supp. 3d 523 (D.D.C. 2018) and reached the same conclusion as the Illinois District Judge. In that case, the application for a warrant asked that law enforcement be allowed to compel the subject to provide biometric features such as their face or fingerprints. The Magistrate Judge held, as to the Fourth Amendment:

> [T]he Court thus finds that, when attempting to unlock a telephone, computer or other electronic device during the execution of a search warrant that authorizes a search of the device, the government may compel the use of an individual's biometric features, if (1) the procedure is carried out with dispatch and in the immediate vicinity of the premises to be searched, and if, at time of the compulsion, the government has (2) reasonable suspicion that the suspect has committed a criminal act that is the subject matter of the warrant, and (3) reasonable suspicion that the individual's biometric features will unlock the device, that is, for example, because there is a reasonable suspicion to believe that the individual is a user of the device.

Id. at 532-533.

Then, as to the Fifth Amendment, the D.C. Magistrate Judge held:

> [T]he seizure of any incriminating information found *on* the phones or computers discovered during the search of the premises would not violate the Fifth Amendment because the "creation" of that information was voluntary

[2] The concept referenced here—and found throughout many similar decisions on this issue—regarding the use of a key or combination in conjunction with a safe comes from *Doe v. United States*, 487 U.S. 201 (1988). In that case, the United States Supreme Court made a comparison between being compelled to surrender a key to a strongbox or safe containing incriminating documents (and how that would not be a testimonial act), and being compelled to reveal the combination to a safe (which would be a testimonial act). *Id*. at 210 n. 9. The Court explained that whether an act was testimonial—and therefore unconstitutional—revolved around whether the act forced the defendant to "disclose the contents of his own mind." *Id*. at 211.

> and "not 'compelled' within the meaning of the privilege [against self-incrimination]."

Id. at 534 (emphasis in original).

The Magistrate Judge went on to recognize however that the compulsion at issue under the Fifth Amendment was the compelled use of the subject's biometric features to unlock the subject devices and gain access to incriminating information that may be on them. The Judge then stated:

> As other courts have recognized, there will be no revelation of the contents of the subject's mind with the procedure proposed by the government for collection of the subject's biometric features. Rather, "[t]he government chooses the finger to apply to the sensor, and thus obtains the physical characteristic – all without the need for the person to put any thought at all into the seizure." Indeed, the use of the fingerprint is much more like the government's compelled use of other "physical characteristics" of criminal suspects that courts have found non-testimonial even when they are used for investigatory purposes rather than solely for identification.

Id. at 536 (internal citations omitted).

The issue has also been addressed by judges in this Circuit. A Magistrate Judge in the Northern District of California recently declined to reach the Fifth Amendment issue in this type of case, applying instead the "foregone conclusion doctrine".[3] In doing so, that Magistrate Judge wrote:

> The Court turns next to the critical question: whether the testimony inhering to Mr. Spencer's act of production is a foregone conclusion such that ordering him to decrypt the at-issue devices will not implicate the Fifth Amendment. The foregone conclusion doctrine is an application of the Fifth Amendment "by which the Government can show that no testimony is at

[3] This was not a fingerprint case but a passcode case. The police were not seeking a warrant to place the suspect's finger on a cellphone to unlock it. Instead, the police were seeking a warrant forcing the suspect to enter the passcode on to the cellphone. If a warrant can require the suspect to enter a passcode, it can also require the suspect to allow his finger to be placed on the cellphone because entering a passcode requires more mental energy than involuntarily placing a finger on a sensor.

> issue." *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1343 n.19 (11th Cir. 2012). The Supreme Court articulated the foregone conclusion doctrine in *Fisher v. United States*, where it upheld the subpoena of potentially incriminating tax documents because the government did not rely on the respondent's tacit testimony—that is, the "truth-telling" arising from the very act of production—to prove the existence of the documents or that the respondent possessed them. The Court thus held that "[t]he existence and location of the papers [were] a foregone conclusion and the taxpayer add[ed] little or nothing to the sum total of the Government's information." *Id.* ("doubtful that implicitly admitting the existence and possession of the papers [rose] to the level of testimony within the protection of the Fifth Amendment"). Because the implicit testimony was a foregone conclusion, the matter reduced to a question "not of testimony but of surrender."

Matter of Search of a Residence in Aptos, California 95003, No. 17-MJ-70656-JSC-1, 2018 WL 1400401, at *6 (N.D. Cal. Mar. 20, 2018). On review, the District Judge denied the defendant's Motion for Relief from a Magistrate Judge's Order. *See, United States v. Spencer,* 2018 WL 19644588 (N.D. Cal. 2018).

Later, in *In the Matter of the Search of a Residence in Oakland, California,* 354 F. Supp. 3d 1010 (N.D. Cal. 2019), another Magistrate Judge held that biometric features that are utilized to potentially unlock an electronic device are testimonial under the Fifth Amendment's privilege against self-incrimination. That Magistrate Judge further held that the foregone conclusion doctrine did not apply. In doing so, the Magistrate Judge reasoned that biometric features serve the same purpose as a passcode, and existing caselaw uniformly does not allow warrants that compel the disclosure of passcodes. However, caselaw makes a clear distinction between biometric features and passcodes on

the basis that passcodes are testimonial.[4]

The Fifth Amendment prevents the Government from compelling a person to be a witness against himself. To qualify for the Fifth Amendment privilege, a communication must be: (1) testimonial, (2) incriminating, and (3) compelled. *See Hiibel v. Sixth Judicial Dist. Court*, 542 U.S. 177, 189 (2004). Witnesses provide testimony, so that is the forbidden compulsion: the Government cannot force someone to provide a communication that is "testimonial" in character. *Hubbell,* 530 U.S. at 34. The Supreme Court has repeatedly distinguished between compelling a communication versus compelling a person to do something that, in turn, displays a physical characteristic that might be incriminating. *Id.* at 35.

The Illinois District Judge provided a list of examples[5] where the Supreme Court has held that compelling displays of certain physical features do not violate the privilege against self-incrimination: putting on a shirt to see whether it fit the defendant, *Holt v. U.S.*, 218 U.S. 245 (1910); providing a blood sample to test for alcohol content, *Schmerber v. California,* 384 U.S. 757 (1966); submitting to the taking of fingerprints or photographs, *see Schmerber*, 384 U.S. at 764 and *United States v. Wade,* 388 U.S. 218

[4] *See, United States v. Maffei,* 2019 WL 1864712 (N.D. Cal. 2019) ("Thus, the Court finds that obtaining defendant's passcode, rather than a biometric key, constituted materially different conduct for the purposes of determining whether law enforcement exceeded the scope of the warrant."); *Commonwealth v. Baust*, 89 Va. Cir. 267, 271 (Va. Cir. Ct. 2014) (finding that the defendant could not be compelled to provide access to his smartphone through his passcode because "compelling Defendant to provide access through his passcode is both compelled and testimonial and therefore protected" by the Fifth Amendment, but he could be compelled to produce his fingerprint to provide access because it was more akin to a key which "does not require the witness to divulge anything through his mental processes").

[5] *See In the MATTER OF the SEARCH WARRANT APPLICATION FOR [redacted text],* 279 F. Supp. 3d at 803.

(1967); providing a voice exemplar, *United States v. Wade,* 388 U.S. 263 (1967); and providing a handwriting exemplar, *Gilbert v. California,* 388 U.S. 263 (1967).

Where, as here, the Government agents will pick the fingers to be pressed on the Touch ID sensor, there is no need to engage the thought process of the subject at all in effectuating the seizure. The application of the fingerprint to the sensor is simply the seizure of a physical characteristic, and the fingerprint by itself does not communicate anything.[6] It is less intrusive than a forced blood draw. Both can be done while the individual sleeps or is unconscious. Accordingly, the Court determines—in accordance with a majority of Courts[7] that have weighed in on this issue—that the requested warrant would not violate the Fifth Amendment because it does not require the suspect to provide any testimonial evidence.[8]

---

[6] The Court takes no position on the issue of cellphone ownership vis-a-vi the introduction of the fact that a defendant's fingerprint opened the cellphone. That issue is not before the Court today. The Court's narrow finding relates to law enforcement's use of a fingerprint to gain access to a cellphone under a valid search warrant.

[7] None of the cases cited by the Government, referenced in the Magistrate Judge's decision, or even cited in this decision are binding on the Court (except insofar as the United States Supreme Court's cases are on point). This is an emerging issue and while many Courts from around the Country provide helpful analysis in their decisions, each is but persuasive on this Court. The reader may also be interested in *State v. Diamond*, 905 N. W. 2d 870 (Minn.) (2018), and *People v. Davis*, 438 P.3d 266 (Colo.) (2019), State Supreme Court cases discussing these issues.

[8] The Court need not discuss whether the communications and actions here are incriminating or compelled because, even assuming arguendo they are, the Court has already determined that it is nonetheless *not testimonial.* "To qualify for the Fifth Amendment privilege, a communication must be testimonial, incriminating, *and* compelled." Hiibel, 542 U.S. at 189 (emphasis added).
Along a similar vein, the Court need not address the Fourth Amendment arguments raised. The Magistrate Judge in this case determined that because the Government's actions impermissible violated the Fifth Amendment, they, in turn, violated the Fourth Amendment's requirement that a search and seizure be "reasonable." By determining that the Government would not violate the Fifth Amendment by placing a defendant's finger on a cellphone sensor, the Court accordingly finds that such a "search and seizure" would likewise comport with the Fourth Amendment's reasonableness requirement.

IV. ORDER

1. The United States' Motion to Reverse or Vacate Magistrate's Order Denying Search Warrant (Dkt. 5) is GRANTED.
2. The Magistrate Judge's Order (Dkt. 3) is VACATED.

DATED: July 26, 2019

David C. Nye
Chief U.S. District Court Judge