

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

In the Matter of the Search Warrant
Application for the cellular telephone in
United States v. Anthony Barrera

Case No. 19 CR 439

Magistrate Judge Sunil R Harjani

MEMORANDUM OPINION AND ORDER

Consumers are more often than ever using their biometric information to unlock their smartphones and apps with a fingerprint or face scan. Likewise, the government is responding by seeking authority to compel a subject to use their biometrics to unlock devices found during the execution of a search warrant. Such a request triggers potential Fourth and Fifth Amendment considerations that are addressed herein. Because of the differing views about whether a fingerprint unlock warrant violates the Fifth Amendment among courts, and in particular in this district, the Court has issued this opinion to explain its reasoning in this novel area in granting the government’s application for a warrant [57]. For the reasons that follow, this Court holds that compelling an individual to scan their biometrics, and in particular their fingerprints, to unlock a smartphone device neither violates the Fourth nor Fifth Amendment. Accordingly, the Court has signed and authorized the government’s warrant, including the authority to compel fingers and thumbs to be pressed on the iPhone home button in an attempt to unlock the device.

Background

The facts of this case are detailed in the Application and Affidavit for a Search Warrant (“Warrant Aff.”) [57]. Defendant Anthony Barrera was charged by indictment with unlawfully possessing a firearm after having been convicted of a felony offense in violation of 18 U.S.C. §

922(g). Warrant Aff. ¶ 15. Among the evidence establishing that Barrera committed the crime was a video recording made by a confidential informant showing defendant in possession of a firearm. *Id.* ¶ 16.

In the current proceeding, the government has alleged that Barrera made various online threats to this confidential informant through postings on a Snapchat account, in violation of 18 U.S.C. § 1512(b). *Id.* ¶¶ 24-34. In connection with the government’s motion to revoke Barrera’s bond conditions, District Judge Robert W. Gettleman ordered that Barrera’s iPhone be turned over to Pretrial Services. [55]. The government seeks to search this iPhone, with a home button, that was taken from Barrera in order to develop evidence of his alleged threats. Warrant Aff. ¶ 36. The iPhone has a fingerprint lock function (known as Touch ID), and the government asked this Court for a warrant to compel the defendant to place his fingers and thumbs on the iPhone home button in an attempt to unlock the phone. *Id.* ¶ 48. The government alleged in the affidavit in support of its request for a search warrant that it will select the fingers and thumbs to press on to the home button, and that the iPhone fingerprint unlock function will disable after five incorrect attempts. *Id.* ¶ 47. At that time, the iPhone function will demand a passcode to unlock the phone. *Id.*

The Fourth Amendment

The Fourth Amendment protects “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,” except “upon probable cause.” U.S. Const. amend. IV; *Missouri v. McNeely*, 569 U.S. 141, 148 (2013). When the government seeks to search the digital data on a cell phone, the Fourth Amendment generally requires a search warrant. *Riley v. California*, 573 U.S. 373, 401 (2014). Here, the government has properly applied for a warrant to search the cell phone that Barrera turned over to Pretrial Services on November 14, 2019. *See* Warrant Aff. ¶¶ 46, 48-51. The government’s warrant

application seeks authorization for another search and seizure, the taking of Barrera’s fingerprints and thumbprints “for the purpose of attempting to unlock the device via Touch ID” *Id.* ¶ 48. *See Hayes v. Fla.*, 470 U.S. 811, 814 (1985) (fingerprinting is a search subject to the constraints of the Fourth Amendment even though “fingerprinting . . . represents a much less serious intrusion upon personal security than other types of searches and detentions”). The Court’s Fourth Amendment inquiry in this case is thus straightforward: does probable cause support the search of the cell phone and the use of Barrera’s fingerprints to unlock the cell phone?

The government’s affidavit in support of the warrant application demonstrates probable cause. Specifically, the affidavit alleged that in November 2019, threatening photos and videos were posted by a Snapchat account named “cheech360.” Warrant Aff. ¶¶ 24-34. According to the affidavit, the “cheech360” account was registered to the email address of “theonononly53@gmail.com,” an email address subscribed to Barrera. *Id.* ¶ 25. The warrant affidavit further stated that the Snapchat posts captured portions of the discovery file in Barrera’s underlying gun case. For example, the second Snapchat video described in the affidavit portrayed portions of the confidential informant video produced to Barrera during discovery with a Snapchat caption overlaying the video, which stated: “That’s owl from east side Joliet wearing a wire on me.” *Id.* ¶ 29. It appeared that this video was created by using a cell phone to record the confidential informant video being played on a separate computer. *Id.* ¶ 30. The affidavit further averred that Barrera and the confidential informant were both members of a gang in which gang members retaliate against any member who cooperates with law enforcement against other members of the gang. *Id.* ¶ 33. Based on the agent’s training and experience, and the facts surrounding the Snapchat videos, the government submitted facts establishing probable cause to believe that Barrera used a cell phone to post the Snapchat videos and photos in order to intimidate

the confidential informant and influence any potential testimony by the informant. *Id.* ¶ 34.

The warrant affidavit thus establishes that there is probable cause to believe that evidence of a crime, specifically a violation of 18 U.S.C. § 1512(b), exists on Barrera’s cell phone. Because the cell phone to be searched is the cell phone turned over by Barrera, *id.* ¶ 35, the government has also demonstrated probable cause to compel Barrera to use his fingers and thumbs in an attempt to unlock the phone.¹ The search warrant in this case therefore meets the requirements of the Fourth Amendment.

The Fifth Amendment

More complicated is the question of whether the forced fingerprint unlock of a cell phone implicates the Fifth Amendment to the United States Constitution. Under the Fifth Amendment, the government shall not compel an individual in any criminal case to be a *witness* against him or herself. U.S. Const. amend. V. Compelling communications or communicative acts can lead to an individual impermissibly bearing witness against him or herself. “Historically, the privilege was intended to prevent the use of legal compulsion to extract from the accused a sworn communication of facts which would incriminate him. Such was the process of the ecclesiastical courts and the Star Chamber—the inquisitorial method of putting the accused upon his oath and compelling him to answer questions designed to uncover uncharged offenses, without evidence from another source.” *Doe v. United States*, 487 U.S. 201, 212 (1988).

¹ The majority of courts analyzing the Fourth Amendment implications of a fingerprint unlock have been faced with warrants that compel the use of an individual’s biometric features in an attempt to unlock a digital device seized in the execution of a premises warrant. *See, e.g., Matter of Search of [Redacted] Washington, D.C.*, 317 F.Supp.3d 523 (D.D.C. 2018); *In re Application for a Search Warrant*, 236 F.Supp.3d 1066 (N.D. Ill. 2017). Such warrants often involve Fourth Amendment concerns not present here, such as whether there is “probable cause to compel any person who happens to be at the subject premises at the time of the search to give his fingerprint to unlock an unspecified Apple electronic device,” 236 F.Supp.3d at 1068, and whether the government needs to make only a showing of reasonable suspicion in order to compel the use of an individual’s biometric features in an attempt to unlock a digital device. 317 F.Supp.3d at 530. Those issues are not present here and do not need to be further discussed.

The test to determine whether communications or communicative acts are privileged under the Fifth Amendment is whether they are “testimonial, incriminating, and compelled.” *Ruiz-Cortez v. City of Chicago*, 931 F.3d 592, 603 (7th Cir. 2019) (quoting *Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty.*, 542 U.S. 177, 189 (2004)); *see also Fisher v. United States*, 425 U.S. 391, 408 (1976) (Fifth Amendment privilege “applies only when the accused is compelled to make a Testimonial Communication that is incriminating”). Applying those three requirements in reverse order here, a biometric scan is certainly *compelled*—the government is explicitly requesting the Court’s authority to force the scan. Warrant Aff. ¶ 48. The act may also be *incriminating*, as unlocking the phone may lead to the discovery of a nearly unlimited amount of potential evidence including text messages, social media posts, call logs, emails, digital calendars, photographs and videos, and location data. *See Riley v. California*, 573 U.S. 373, 393–98 (2014) (characterizing cell phones as “minicomputers” that could “just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers”). But if a *compelled* act is not *testimonial*, and therefore not protected by the Fifth Amendment, it cannot become protected simply because it will lead to *incriminating* evidence. *Doe*, 487 U.S. at 208 n.6. As a result, the relevant Fifth Amendment inquiry here is whether the compelled act of scanning a subject’s fingerprint to unlock a device is a *testimonial* act.

To be testimonial, a subject’s communicative act “must itself, explicitly or implicitly, relate a factual assertion or disclose information.” *Doe*, 487 U.S. at 210. Otherwise stated, the Fifth Amendment’s self-incrimination clause is implicated wherever the compelled act forces an individual to “disclose the contents of the [subject’s] own mind.” *Id.* at 211 (citing *Curcio v. United States*, 354 U.S. 118, 128 (1957)). Justice Holmes opined that the self-incrimination clause draws a fundamental distinction between compelling a person to communicate something to the

government versus providing some physical characteristic to the government as part of an investigation. See *Holt v. United States*, 218 U.S. 245, 252-53 (1910) (“[T]he prohibition of compelling a man in a criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material.”).

For example, in *Schmerber v. California*, 384 U.S. 757 (1966), the Supreme Court held that the accused’s “testimonial capacities were in no way implicated” when the government’s officers extracted blood from the accused’s body incident to an arrest, over the accused’s objection, to test for alcohol as evidence of criminal guilt. *Id.* at 765. *Schmerber* reasoned that Supreme Court precedent provided that only compulsion of communicative facts triggered the Fifth Amendment privilege, not compulsion of “real or physical evidence.” *Id.* at 764. Thus, the *Schmerber* Court concluded that the incriminating blood test evidence was not testimonial because it was neither the result of the accused’s communication nor evidence of some communicative act. *Id.* at 764-65.

The Supreme Court has similarly held that requiring grand jury witnesses to produce voice and handwriting exemplars neither violates the Fourth nor Fifth Amendment, even though speaking and writing are quintessential means of communication. *United States v. Dionisio*, 410 U.S. 1, (1973); *Gilbert v. California*, 388 U.S. 263 (1967). The *Dionisio* and *Gilbert* Courts reasoned that the voice/handwriting exemplars were identifying physical characteristics that did not reflect the subject’s mental impressions. *Dionisio*, 410 U.S. at 7 (“The voice recordings were to be used solely to measure the physical properties of the witnesses’ voices, not for the testimonial or communicative content of what was to be said.”); *Gilbert*, 388 U.S. at 266-67 (“One’s voice and handwriting are, of course, means of communication. It by no means follows, however, that every

compulsion of an accused to use his voice or write compels a communication within the cover of the privilege. A mere handwriting exemplar, in contrast to the content of what is written, like the voice or body itself, is an identifying physical characteristic outside its protection. No claim is made that the content of the exemplars was testimonial or communicative matter.”) (citations omitted).

In another compelled physical act case, the Supreme Court rejected an argument that the government had violated the privilege against self-incrimination by forcing a defendant to try on a blouse for identification purposes. *Holt*, 218 U.S. at 252. In *Holt*, Justice Holmes emphasized that the purpose of the privilege against self-incrimination was not an exclusion of the body as evidence when it may be material. *Id.* at 252-53. In other words, Justice Holmes explained that the self-incrimination clause’s purpose drew 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. *See id.* And so, *Holt* found no communicative component to trying on a blouse and held that there was no protected testimonial aspect under the Fifth Amendment’s prohibition against self-incrimination.

Relatedly, in a compelled verbal act case, *United States v. Wade*, 388 U.S. 218 (1967), the Supreme Court stated that the Fifth Amendment privilege was not violated when Wade was required to stand in a line-up and say words to the effect of “put the money in the bag.” The Court relied upon *Holt* in concluding that Wade had disclosed a physical characteristic, and not any knowledge he might have. *Id.* at 221-24. Importantly, Wade was forced to actually say words, rather than just display a physical characteristic of his body. Yet the Supreme Court nonetheless concluded that because Wade was not required to “speak his guilt,” but only use his voice as a physical characteristic, there was no compulsion to utter words of testimonial significance. *Id.* at

222-23.

One type of compelled physical act that has been considered testimonial in certain cases is the act of producing documents. Courts have found that producing documents in response to a criminal subpoena request could be a testimonial communicative act because the responding party may need to “make extensive use of ‘the contents of his own mind’ in identifying the hundreds of documents responsive to the requests in the subpoena.” *United States v. Hubbell*, 530 U.S. 27, 43 (2000) (citing *Curcio*, 354 U.S. at 128). The *Hubbell* Court held that the assembly of the documents in that case “was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox.” *Id.* at 43 (citing *Doe*, 487 U.S. at 210 n.9). As the Supreme Court likewise explained in *Fisher*, the compelled act of production becomes testimonial where the act of production “tacitly concedes” that the produced materials exist and are in subject’s possession or control. *Fisher v. United States*, 425 U.S. 391, 410 (1976).²

In evaluating the novel question of whether compelled biometric scans to unlock encrypted devices is permissible under the Fifth Amendment, federal district courts and state courts have reached different results. *See, e.g., In the Matter of Search Warrant Application for [redacted text]*, 279 F.Supp.3d 800, 801 (N.D. Ill. 2017) (Chang, J.) (“[T]he Court holds that requiring the application of the fingerprints to the sensor does not run afoul of the self-incrimination privilege because that act does not qualify as a testimonial communication.”); *In re Application for a Search Warrant*, 236 F.Supp.3d 1066 (N.D. Ill. Feb. 16, 2017) (Weisman, J.) (holding that compelling a thumb print to unlock an encrypted device violated the Fifth Amendment because the act

² This Court notes that an exception to the act of production doctrine exists where “[t]he existence and location of the papers are a foregone conclusion and the [party] adds little or nothing to the sum total of the Government’s information by conceding that he in fact has the papers.” *Fisher*, 425 U.S. at 411. This Court need not address this exception here, and it does not apply, as the government does not know exactly all the items it expects to find on this particular cell phone.

constituted testimonial act of production); *Matter of single-family home & attached garage*, No. 17 M 85, 2017 WL 4563870, at *9 (N.D. Ill. Feb. 21, 2017) (Finnegan, J.), *rev'd by* 279 F.Supp.3d 800 (N.D. Ill. 2017) (denying warrant application to compel four individuals to unlock unspecified Apple devices during the search of subject premises because fingerprint unlock was compelled act of production); *Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 398 F.Supp.3d 785 (D. Idaho 2019) (holding search warrant authorizing law enforcement to place suspect's finger on cell phone to unlock phone did not require suspect to provide any testimonial evidence and therefore did not violate suspect's Fifth Amendment rights); *Matter of Residence in Oakland, California*, 354 F.Supp.3d 1010 (N.D. Cal. Jan. 10, 2019) (denying warrant application because biometric features used to potentially unlock electronic device are testimonial under Fifth Amendment); *Matter of Search of [Redacted] Washington, D.C.*, 317 F.Supp.3d 523 (D.D.C. June 27, 2018) (granting warrant application because compelled use of subject's biometric features was non-testimonial under the Fifth Amendment); *Minnesota v. Diamond*, 905 N.W.2d 870, 878 (Minn. 2018), *cert. denied*, 138 S. Ct. 2003, 201 L. Ed. 2d 261 (2018) ("Because the compelled act merely demonstrated Diamond's physical characteristics and did not communicate assertions of fact from Diamond's mind, we hold that Diamond's act of providing a fingerprint to the police to unlock a cellphone was not a testimonial communication protected by the Fifth Amendment."); *Commonwealth v. Baust*, 89 Va. Cir. 267, 2014 WL 10355635, at *1 (Va. Cir. Ct. 2014) (granting warrant application to compel fingerprint and denying motion to compel cell phone passcode because passcode was testimonial whereas fingerprint was a non-testimonial physical characteristic that did not require Defendant to "communicate any knowledge at all") (internal quotation marks and citation omitted). To date, neither the Supreme Court, the Seventh Circuit, nor any other court of appeals has weighed in.

In analyzing this issue, the key questions, in this Court’s view, are threefold: (1) whether the biometric unlock is more like a key than a combination; (2) whether the biometric unlock is more like a physical act than testimony; and (3) whether the implicit inferences that arise from the biometric unlock procedure is sufficient to be of testimonial significance under the Fifth Amendment.

1. Key Versus Combination

First, the Court holds that the biometric unlock procedure is more akin to a key than a passcode combination. The Supreme Court in *Doe*, and later in *Hubbell*, has illustrated the difference between testimonial and non-testimonial physical acts via this helpful comparison, which aptly applies to an iPhone that has two different unlock features – a fingerprint and a passcode. In *Doe*, the Court noted that the Fifth Amendment permits the government to force an individual to surrender a key to a strongbox containing incriminating documents, but not to reveal the combination to a subject’s wall safe. *Doe*, 487 U.S. at 210 n.9. Thus, using the *Doe* framework, this Court examines whether a biometric scan of an individual’s finger or thumb is more like a key or a combination. *See id.*

A combination passcode requires a verbal statement from the possessor of the code. *Doe*, 487 U.S. at 211. More importantly, compelling someone to reveal a passcode also requires an individual to communicate something against her will that resides in her mind. *See Holt*, 218 U.S. at 252-53. A key, however, is a physical object just like a finger — it requires no revelation of mental thoughts. Nor does a finger require a communication of any information held by that person, unlike a passcode. In fact, the application of a finger to the home button on a iPhone “can be done while the individual sleeps or is unconscious,” and thus does not require any revelation of information stored in a person’s mind. *Google Pixel 3 XL Cellphone*, 398 F. Supp. 3d at 794.

The Supreme Court further expanded on this key/passcode distinction in *Hubbell* holding that reviewing and producing documents required the extensive use of the responding party's mind in determining what was responsive. *Hubbell*, 530 U.S. at 43. The assembly of responsive documents was found to be more akin to providing the combination of a safe rather than surrendering a key. *Id.* In contrast, in the case of a finger and its corresponding print, the compelled party is not assembling anything or disclosing any mental revelations from the act. Further, the Supreme Court has recognized that “both federal and state courts have usually held that it offers no protection against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture.” *Schmerber*, 384 U.S. at 764. These precedents firmly establish, in the Court's view, that a feature of the human body, such as a finger, is an object analogous to a key – another physical object, and not a passcode. In other words, in the context of an iPhone, a finger is a modern substitute for a key.

2. Physical Act Versus Testimony

Second, the biometric procedure is first and foremost a physical act. It utilizes a body part on an individual to perform an act—rather than any implicit or explicit verbal statement. Put another way, the biometric feature is a body part used to essentially determine whether an item of evidence for a case (*i.e.* a cell phone) has any evidentiary value — much like a blood sample, voice exemplar, or blouse is used to determine whether it matches the blood, voice, or physical characteristics of a suspect that would provide evidentiary value in a case. As the Supreme Court appropriately stated in *Wade*, compelling an individual to exhibit his person to the government before trial does not violate the Fifth Amendment because such a forcing is “compulsion of the accused to exhibit his physical characteristics, *not* compulsion to disclose any knowledge he might

have.” *Wade*, 388 U.S. at 222.

The Supreme Court has held that in situations that require a person to be compelled to speak, a circumstance that is often equated with the concepts of witness and testimony, the distinction between testimonial and non-testimonial still applies. As discussed above, the provision of a voice exemplar in *Dionisio*, an act that requires a *verbal* statement by the accused, was deemed non-testimonial because it did not constitute a revelation of someone’s mental thoughts, but simply a physical characteristic of a person – his voice. *Dionisio*, 410 U.S. at 7; *see also Pennsylvania v. Muniz*, 496 U.S. 582, 591 (1990) (slurring of speech evidence deemed non-testimonial because it revealed the physical manner of how a person articulates words). The concept of a fingerprint scan is a significantly less difficult Fifth Amendment issue than the recitation of words by a person under compulsion.

The question of whether a physical act is testimonial is further addressed in the act of production line of cases, as discussed above. In the act of production line of cases, the selection of the documents in response to a subpoena provides some degree of insight into the responding party's mind, which leads to the conclusion that the production has testimonial significance. *Hubbell*, 530 U.S. at 43. That conclusion is not present when a biometric feature merely provides access to the entirety of the cell phone, without any selection process on the part of the compelled party. Furthermore, the government selects the fingers or thumbs to impress on to the phone, not the defendant. This further supports a finding that the compelled party’s thoughts are not being used in the process.

In addition, as the Supreme Court recognized in *Doe*, a physical act that does not directly point the government to incriminating evidence does not constitute a testimonial act. *Doe*, 487 U.S. at 215. The *Doe* Court held that compelling a defendant to sign a directive consenting to the

disclosure of any bank accounts that he had the right of withdrawal without acknowledging the existence of any account, was not testimonial under the Fifth Amendment. *Id.* at 214-18. As explained by the *Doe* Court, as long as the government must locate the evidence on its own (as it had to with the obtention of bank records in *Doe*), the act of signing the consent has no testimonial significance. *Id.* at 215-16. Similarly, the compelled biometric unlock procedure merely gives access to a potential source of evidence; it does not tell the government where to look. *Cf. Hubbell*, 530 U.S. at 41-42 (the collection and production of 11 categories of documents essentially required a responding party to answer a series of interrogatories that would disclose the existence and location of particular documents fitting the descriptions). Remarkably, the potential sources of evidence in a cell phone far exceed those available in any bank record production involved in *Doe* — on average, an Apple iPhone can hold between 16GB and 512GB of data, and in vastly different formats — videos, photos, texts, notes, chats, location data, and data embedded within a multitude of other applications. In other words, the government’s hunt for evidence in the contents of a cell phone requires a much deeper dive than that of the bank account records in *Doe*, making the argument that a biometric unlock is testimonial even less persuasive.

Another concern that has been raised under the act of production doctrine is that the compelled production of the fingerprint permits the implication that the data on the phone is authentic. *See, e.g., Fisher*, 425 U.S. at 412-13 (discussing whether taxpayer’s act of producing documents would authenticate the documents produced). More specifically, the act of producing data in response to a subpoena may allow a court to admit the records as authentic because they came from the responding party, who determined that they were responsive, and the proponent can contend the “item is what the proponent claims it is.” Fed. R. Evid. 901(a). In contrast, the authenticity of the material obtained as a result of the biometric unlock procedure does not rest on

the shoulders of the compelled party. Rather, in the context of data obtained from search warrants, courts routinely rely upon the government's chain of custody testimony to establish the foundation for the authenticity of the items seized from a search. The fact that an individual is able to unlock a phone with a physical characteristic does not automatically make each individual set of data, such as photos, videos, notes, email, texts, *etc.*, immediately authentic. Thus, another rationale for the act of production doctrine applying to fingerprints is not implicated here.

3. Implicit Inferences

Third, the Court holds that the implicit inference from the biometric unlock procedure, that the individual forced to unlock had some point accessed the phone to program his or her fingerprint, is not sufficient to convert the act to testimonial. The Supreme Court considered this similar concept in *Doe*, when it found that requiring a petitioner to execute a consent directive that would result in the production of bank records would not have testimonial significance. *Doe*, 487 U.S. at 214-18. This was true even when the Court found that petitioner doing so, and by allowing the bank to respond to the subpoena, would result in making an implicit declaration that the accounts belong to the petitioner. Similarly, the Supreme Court has permitted compulsions of handwriting exemplars despite the resulting implicit inference that the subject "admits his ability to write and impliedly asserts that the exemplar is his writing." *Fisher*, 425 U.S. at 411. No different with the concept of a physical key — by forcing an individual, pursuant to a warrant, to hand over the key to a strongbox, it allows a firm conclusion that the individual had possession of the key and an inference that he or she had access to the contents of the strongbox. In fact, in almost any compelled physical act, there will be an inference that can be drawn, which could in some fashion prove incriminating. Yet, the Supreme Court has determined that neither the signing of the consent, the requiring of the handwriting exemplar, the wearing of a blouse, nor the seizing

of a key to a strongbox constitute testimonial acts. As explained above, the dividing line the Supreme Court has drawn is whether the suspect is compelled to provide “any knowledge he might have.” *Doe*, 487 U.S. at 216 (citation omitted). Similarly, the implicit inference that one might draw from the biometric unlock procedure — that the cell phone was at some point accessed in order to program the biometric lock feature — is no different in significance than any of the above inferences. It is of the same scale that existed in *Doe*, *Gilbert* and the other cases discussed above. The implicit inference is also not necessarily as firm as on first impression – the Touch ID feature on an iPhone permits up to five fingerprints to be programmed, thus allowing the potential for multiple users to program the feature. As a result, the Court concludes that any implicit inference that can be drawn from a biometric unlock procedure is not of testimonial significance.

4. *Riley and Carpenter*

Finally, courts holding that the biometric unlock procedure implicates the Fifth Amendment often refer to the Supreme Court's opinions in *Riley v. California*, 573 U.S. 373 (2014), and *Carpenter v. United States*, 138 S. Ct. 2206 (2018), for the principle that cell phones have taken on a unique status under our Fourth Amendment jurisprudence and are now viewed differently. In *Carpenter*, the Court held that a warrant was needed to obtain historical cell-site location information from a phone. *Carpenter*, 138 S. Ct. at 2221. In *Riley*, the Court found that a warrant was required to search a cell phone seized incident to arrest. *Riley*, 573 U.S. at 401. *Riley* did caution against the use of old analogies when applied to cell phones. *Id.* at 393. Nevertheless, *Riley* did not eradicate precedent in this area; the Supreme Court's tests in *Wade*, *Doe*, *Schneider*, *Holt*, *Diosinio*, and *Gilbert* all still apply. Just as letters were replaced with electronic mail and cassette tapes were replaced with digital music files, keys are being replaced with biometric functions. Consolidation and digitization, resulting in the carrying of the least amount of physical

items as possible while holding the most amount of functionality and data, is *de jure* and here to stay. However, the applicable analysis — that a fingerprint has now replaced a key — does not automatically transform what has been previously considered non-testimonial into testimonial acts. The old tests, in this particular circumstance, remain relevant and applicable. *Riley* and *Carpenter* furthermore did not address any Fifth Amendment concerns with respect to cell phones. Moreover, the concern in both *Carpenter* and *Riley* was the warrantless searches of cell phone data and how such a process impacted a greater invasion of privacy than previously imagined on any individual. Those concerns are properly addressed here in a manner consistent with *Riley*, as the government is seeking the authority pursuant to a warrant application after demonstrating probable cause to a neutral and detached judicial officer—a process explicitly permitted by the Fourth Amendment.

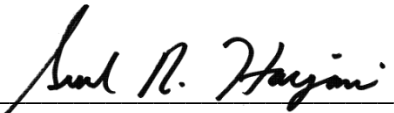
It is also important to recall that the word at issue in the Fifth Amendment is “witness,” and to equate the concept of witness, which was originally conceived to cover compelled and incriminating oral testimony, with a fingerprint press is inconsistent with the plain text of the Fifth Amendment. Indeed, an overbroad interpretation of the Fifth Amendment could diminish the underlying purpose of the Fourth Amendment, by prohibiting a physical act that provides access to evidence through a warrant upon a finding of probable cause, because it is too easily deemed to be testimonial.

Conclusion

For the reasons discussed above, the Court finds that the government's application for the biometric unlock procedure does not violate the Fourth or Fifth Amendments, and as a result, the Court has signed the application and the warrant after its finding of probable cause.

SO ORDERED.

Dated: November 22, 2019



Sunil R. Harjani
United States Magistrate Judge