ALAN WILSON
ATTORNEY GENERAL

May 21, 2021

The Honorable B. Lee Miller
Municipal Court Judge
City of Greenwood
P.O. Box 40
Greenwood, SC 29648

Dear Judge Miller:

Attorney General Alan Wilson has referred your letter to the Opinions section. Your letter asks the following:

> Can a police officer obtain a search warrant from a Summary Court Judge compelling a defendant to attempt to open his/her cell phone via facial recognition and/or fingerprint?
>
> Probable cause has been determined that the phone belongs to the defendant and that the evidence, data, pictures, etc..., attempting to be retrieved are stored on that cellphone in connection with the charge(s) being made against him/her.

Law/Analysis

The request letter asks for this Office's opinion regarding an unsettled question of law. There is a clear split among the federal district courts that have addressed whether the Fifth Amendment to the United States Constitution protects a person from being compelled to unlock a cellphone or other device by providing a fingerprint or using facial recognition, referred to as biometric data. See In re Search Warrant, 437 F. Supp. 3d 515, 516 (W.D. Va. 2020) ("No clear consensus has emerged whether the government's request to use Mr. Crowe's biometric data – either fingerprints or facial recognition – is constitutional."); El Ali v. Barr, 473 F. Supp. 3d 479, 522 (D. Md. 2020) (Noting that the "question of whether provision of cell phone passcodes or biometric information amounts to testimonial statements" is "an unsettled question of law"); Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785, 790 (D. Idaho 2019) ("There appears to be several decisions throughout the country that have addressed the issue in the federal district courts with mixed results."). While our state courts in South Carolina have not issued a decision on this point, courts in other states are similarly divided. To date, no federal circuit court has issued an opinion on this topic. With no clear consensus, this opinion cannot be free from doubt. However, this Office is persuaded by the

decisions that conclude compelling a person to provide biometric information to unlock a cell phone is not testimonial and, therefore, not protected by the Fifth Amendment. See, e.g., In re Search Warrant No. 5165, 470 F. Supp. 3d 715 (E.D. Ky. 2020).

First, the South Carolina Supreme Court has held that the Fourth Amendment permits law enforcement to obtain a warrant to search a cell phone, and, in certain circumstances, such as abandonment, "may continue to justify a warrantless search of a cell phone." State v. Moore, 429 S.C. 465, 473 n.4, 839 S.E.2d 882, 886 (2020); see also State v. Brown, 423 S.C. 519, 815 S.E.2d 761 (2018). In State v. Brown, supra, the Court considered whether the Federal Constitution and South Carolina Constitution requires a warrant before searching a locked cell phone left at a crime scene when law enforcement unlocks the phone by guessing the password. In concluding that the subject cell phone had been abandoned and, as a result, a warrant was not needed, the majority explained:

> The Fourth Amendment guarantees us the right to be free from unreasonable searches and seizures. U.S. Const. amend. IV; see also S.C. Const. art. I, § 10. "Abandoned property," however, "has no protection from either the search or seizure provisions of the Fourth Amendment." State v. Dupree, 319 S.C. 454, 457, 462 S.E.2d 279, 281 (1995) (citing California v. Greenwood, 486 U.S. 35, 40-41, 108 S.Ct. 1625, 1628-29, 100 L.Ed. 2d 30, 36-37 (1988)). Under a standard abandonment analysis, "the question is whether the defendant has, in discarding the property, relinquished his reasonable expectation of privacy."

Id. at 522, 815 S.E.2d at 763. Chief Justice Beatty wrote in dissent that Riley v. California, 573 U.S. 373 (2014) "create[d] a categorical rule that, absent exigent circumstances, law enforcement must procure a search warrant before searching the data contents of a cell phone." 423 S.C. at 531, 815 S.E.2d at 767. Quoting Chief Justice Roberts, he explained "it is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search ..." 423 S.C. at 533, 815 S.E.2d at 768–69. Although the majority and dissent differed on the applicability of the abandonment exception, both agreed that, after procuring a warrant, law enforcement can unlock a cell phone and search its contents.

The request letter asks more specifically whether a search warrant can be issued to compel a person to unlock a cell phone by providing biometric data. The scenario raises the issue of the applicability of the Fifth Amendment protection against being "compelled in any criminal case to be a witness against himself." U.S. Const. amend. V; see also S.C. Const. art. I, § 12 ("No person shall be ... compelled in any criminal case to be a witness against himself."). In United States v. Hubbell, 530 U.S. 27 (2000), Justice Stevens explained how the Court has interpreted this prohibition:

> The word "witness" in the constitutional text limits the relevant category of compelled incriminating communications to those that are "testimonial" in character. As Justice Holmes observed, there is a significant difference between the use of compulsion to extort communications from a defendant and compelling

> a person to engage in conduct that may be incriminating. Thus, even though the act may provide incriminating evidence, a criminal suspect may be compelled to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording of his voice. The act of exhibiting such physical characteristics is not the same as a sworn communication by a witness that relates either express or implied assertions of fact or belief.

Id. at 34–35 (2000) (footnotes omitted). Summarized, the Fifth Amendment protects communications that are (1) compelled, (2) incriminating, and (3) testimonial. See In re Search Warrant No. 5165, 470 F. Supp. 3d at 726 ("The privilege only applies where there is (1) compelled, (2) incriminating, (3) testimony. All three must be present for Fifth Amendment protection."); Matter of Residence in Oakland, California, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019) review dismissed sub nom. In re Search of a Residence in Oakland, California, No. 19MJ70053KAW1JD, 2019 WL 6716356 (N.D. Cal. Dec. 10, 2019) ("The proper inquiry is whether an act would require the compulsion of a testimonial communication that is incriminating."). Further, Hubbell discussed how the act of production may have testimonial aspects that are entitled to Fifth Amendment protection:

> [W]e have also made it clear that the act of producing documents in response to a subpoena may have a compelled testimonial aspect. We have held that "the act of production" itself may implicitly communicate "statements of fact." By "producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic." ... Whether the constitutional privilege protects the answers to such questions, or protects the act of production itself, is a question that is distinct from the question whether the unprotected contents of the documents themselves are incriminating.

Id. at 36-37 (citations omitted). Where compelled testimony communicates information that "lead[s] to incriminating evidence," such testimony is still privileged even if the information itself is not inculpatory. Id. at 38. Stevens explained how the act of production can be testimonial by analogizing to unlocking a safe:

> It was unquestionably necessary for respondent to make extensive use of "the contents of his own mind" in identifying the hundreds of documents responsive to the requests in the subpoena. See Curcio v. United States, 354 U.S. 118, 128, 77 S.Ct. 1145, 1 L.Ed.2d 1225 (1957); Doe v. United States, 487 U.S., at 210, 108 S.Ct. 2341. The assembly of those documents 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 (emphasis added). The opinions which address whether the Fifth Amendment protects a person from being compelled to unlock a cellphone by revealing a passcode or using his

biometric data often employ the Doe, supra "contents of his own mind" or the Hubbel, supra, safe analogy to determine whether the act is testimonial.[1]

> [C]onsumers have had the ability to utilize numeric or alpha-numeric passcodes to lock their devices for decades. Courts that have addressed the passcode issue have found that a passcode cannot be compelled under the Fifth Amendment, because the act of communicating the passcode is testimonial, as "[t]he expression of the contents of an individual's mind falls squarely within the protection of the Fifth Amendment."
>
> ...
>
> Notwithstanding, certain acts, while incriminating, are not within the privilege, such as furnishing a blood sample, submitting to fingerprinting, providing a handwriting or voice exemplar, or standing in a lineup. Doe, 487 U.S. at 210, 108 S.Ct. 2341. "The distinction which has emerged, often expressed in different ways, is that the privilege is a bar against compelling 'communications' or 'testimony,' but that compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it."

Matter of Residence in Oakland, California, 354 F. Supp. 3d at 1015 (emphasis added). Broadly, these opinions fall into two groups: (1) those that find biometric unlocking is used as a substitute for passcode unlocking and, therefore, a court cannot compel one but not the other, and (2) those that find a distinction between compelling a person to reveal a passcode, as testimonial equivalent of revealing the combination to a safe, and employing biometric procedures, as non-testimonial equivalent to surrendering a key to a safe. The Court in Residence in Oakland, California explained its reasoning for finding biometrics are merely a substitute for entering a passcode:

> [T]he Government concedes that a finger, thumb, or other biometric feature may be used to unlock a device in lieu of a passcode. (Aff. ¶ 17a.) In this context, biometric features serve the same purpose of a passcode, which is to secure the owner's content, pragmatically rendering them functionally equivalent. As the Government acknowledges, there are times when the device will not accept the biometric feature and require the user to type in the passcode to unlock the device. (Aff. ¶ 17g.) For example, a passcode is generally required "when a device has been restarted, inactive, or has not been unlocked for a certain period of time." Id. This is, no doubt, a security feature to ensure that someone without the passcode

[1] These opinions generally recognize that requiring a person to unlock a phone is a compelled action and presume incriminating evidence is on the device to be searched. See In re Search Warrant No. 5165, 470 F. Supp. 3d 715, 727 (E.D. Ky. 2020) ("Forcing a target to provide his biometrics to allow law enforcement to access a device is unquestionably compelled conduct. The Court must assume, for the sake of this opinion, that there is incriminating evidence on the devices to be searched; otherwise this inquiry is moot.").

> cannot readily access the contents of the phone. Indeed, the Government expresses some urgency with the need to compel the use of the biometric features to bypass the need to enter a passcode. Id. This urgency appears to be rooted in the Government's inability to compel the production of the passcode under the current jurisprudence. It follows, however, that if a person cannot be compelled to provide a passcode because it is a testimonial communication, a person cannot be compelled to provide one's finger, thumb, iris, face, or other biometric feature to unlock that same device.

Id. at 1015–16; see also United States v. Wright, 431 F. Supp. 3d 1175, 1187 (D. Nev. 2020) ("[A] biometric feature is functionally the same as a passcode, and because telling a law enforcement officer your passcode would be testimonial, so too must the compelled use of your biometric feature to unlock a device."). Additionally, the Court reasoned that the action of successfully unlocking a device with biometric data communicates the person had ownership or control over the device, rendering the act testimonial.

> A finger or thumb scan used to unlock a device indicates that the device belongs to a particular individual. In other words, the act concedes that the phone was in the possession and control of the suspect, and authenticates ownership or access to the phone and all of its digital contents. Thus, the act of unlocking a phone with a finger or thumb scan far exceeds the "physical evidence" created when a suspect submits to fingerprinting to merely compare his fingerprints to existing physical evidence (another fingerprint) found at a crime scene, because there is no comparison or witness corroboration required to confirm a positive match. Instead, a successful finger or thumb scan confirms ownership or control of the device, and, unlike fingerprints, the authentication of its contents cannot be reasonably refuted. ... Thus, the undersigned finds that a biometric feature is analogous to the nonverbal, physiological responses elicited during a polygraph test, which are used to determine guilt or innocence, and are considered testimonial.

Id. at 1016 (emphasis added); see also United States v. Wright, 431 F. Supp. 3d at 1188 ("[U]nlocking a phone with your face equates to testimony that you have unlocked the phone before, and thus you have some level of control over the phone.").

The alternative line of cases follows the Hubbell safe analogy to conclude that the use of biometric data is more akin to the nontestimonial act of handing over the key to a safe. In Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case, supra, the Court found that the act of permitting government agents to select which fingers would be pressed onto a cellphone's sensor is not testimonial.

> 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.

Id. at 791 (emphasis in original).

> 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. 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 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.

Id. at 793–94 (footnotes omitted). Similarly, in Matter of Search Warrant Application for cellular telephone in United States v. Barrera, 415 F. Supp. 3d 832, 839 (N.D. Ill. 2019), the Court found that permitting a "biometric unlock procedure is more akin to a key than a passcode combination." The Court explained:

> [C]ompelling 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, 31 S.Ct. 2. 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.

Id. Moreover, In re Search Warrant No. 5165, 470 F. Supp. 3d 715 (E.D. Ky. 2020), the District Court for the Eastern District of Kentucky analyzed whether the use of biometrics could be testimonial according to the "act of production" doctrine. The Court compared the Supreme Court's analysis in Doe v. United States, 487 U.S. 201 (1988), which upheld a court order compelling the target of a grand jury investigation to sign a consent form authorizing banks to disclose records of his accounts:

> [W]hen the United States sought bank records directly from a target's banks through a compelled consent document, the Court rejected the application of the act of production doctrine. Doe, 487 U.S. 201, 108 S.Ct. 2341 ("Doe II"). The Supreme Court concluded that the consent form did "not acknowledge that an account in a foreign financial institution is in existence or that it is controlled by petitioner" or "indicate whether documents or any other information relating to petitioner are present at the foreign bank" or "even identify the relevant bank." Id. at 215, 108 S.Ct. 2341. Because the Court was compelling Doe to sign the consent form, his execution of it "sheds no light on his actual intent or state of mind." Id.

> at 216, 108 S.Ct. 2341. Thus, the Court found that signing the consent form was nontestimonial and not protected by the Fifth Amendment privilege.
>
> ...
>
> [T]he Court is left with only one conclusion: a face, finger, or iris is a physical item that can be physically produced without any mental impressions, communication, or admission of mens rea from the target. Stated another way, the Court finds biometric markers akin to a key in line with Doe II. A passcode, on the other hand, is no different from the combination lock on Justice Stevens' imagined safe as discussed in Doe I and Hubbell.
>
> Requiring a target to look at or place their finger on an electronic device "sheds no light on his actual intent or state of mind."

In re Search Warrant No. 5165, 470 F. Supp. 3d at 728–29.[2] The Court also rejected the conclusion that by unlocking the device a person authenticates its contents.

> A successful biometric scan provides the government with powerful evidence that that individual has owned and/or controlled that device at some point. However, it does not rule out the possibility that another person currently owns and controls the device. Electronic devices can often be programmed to use multiple individuals' biometrics and a passcode, all at the same time. For crimes such as the one at issue here, possession of child pornography, proving possession of the device on which evidence is found may tend to prove an element of the crime. But a successful biometric scan, alone, does not definitively prove ownership or control; nor is it testimony "that he or she currently has some level of control over or relatively significant connection to the phone and its contents." Oakland, 354 F. Supp. 3d at 1016. Again, a very strong inference may be drawn that the individual "has accessed the phone before," but the individual, by merely looking

[2] See also Barrera, 415 F. Supp.3d at 840 (discussing the act of production doctrine).

> 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, 120 S.Ct. 2037. 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.
>
> ...
>
> [A]s 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, 108 S.Ct. 2341. Similarly, the compelled biometric unlock procedure merely gives access to a potential source of evidence; it does not tell the government where to look.

> at a device or placing his or her finger on it, did not communicate any knowledge or mental state from his mind to law enforcement.
>
> Finally, the Oakland court warned that when a device is accessed with a biometric scan, "the authentication of its contents cannot be reasonably refuted." Id. This, too, is false. A successful biometric scan provides no admission or testimony about the existence of documents on the device.

Id. at 733.[3]

Finally, the Court acknowledged the Oakland opinion's conclusion that unlocking a device with biometric data is "functionally equivalent" to unlocking the same device with a passcode, but it disagreed this similarity in operation results in Fifth Amendment protection.

> The Court agrees with Amicus and the Northern District of California that "biometric features serve the same purpose of a passcode, which is to secure the owner's content, pragmatically rendering them functionally equivalent." Oakland, 354 F. Supp. 3d at 1015. Where the Court disagrees, however, is that this *functional* equivalency amounts to *legal* equivalency.

Id. at 734 (emphasis in original). The Court recognized that this is an unsettled legal issue and that it is far from clear that the current Fifth Amendment jurisprudence will ultimately resolve these issues. However, it cautioned that, until a higher court establishes a different test, the Doe and Hubbell analytical frame work should be followed.

> In Riley, Justice Alito cautions courts not to "mechanically apply" a predigital-age constitutional rule to digital devices. Riley v. California, 573 U.S. 373, 406, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014). Unfortunately, where technology has outpaced the legal precedent, lower courts have little choice but to operate within the framework available if stare decisis is to be respected. Riley and Carpenter, discussing Fourth Amendment privileges in the context of warrantless searches, does not negate the Supreme Court's holdings in Doe II or other related cases. The Court, then, is forced to analyze the existing case law and forecast—or perhaps, guess—how higher courts will apply existing law to novel technology. The nature

---

[3] See also Barrera, 415 F. Supp. 3d at 841.

> [T]he 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.

> of the inquiry means that federal district courts—specifically magistrate judges issuing search warrants—find themselves alone in the unmapped territory where old law and new technology intersect. The Court recognizes the law in this area is emerging and may change as the courts "catch up" with technology; this Memorandum Opinion merely reflects the outcome current Fifth Amendment jurisprudence counsels.

Id. at 734–35.

It is this Office's opinion that our state courts likely would find the Eastern District of Kentucky's analysis persuasive, hold that compelling a person to provide biometric information to unlock a cell phone is not testimonial, and, therefore, is not prohibited by the Fifth Amendment. See In re Search Warrant No. 5165, 470 F. Supp. 3d 715 (E.D. Ky. 2020). Again, we emphasize that this conclusion is not free from doubt as several courts have issued well-reasoned opinions that come to opposite conclusions regarding the testimonial nature of compelling a person's biometric data. Yet, this Office finds that the Hubbell analogy of compelling a person to reveal a combination or turnover a key to unlock a safe controls the result. Certainly, the Oakland opinion is correct that using biometric security on a cell phone serves the same purpose as a passcode, which is to secure the device. But the analogy of using a key or combination demonstrates the dichotomy of how the Fifth Amendment applies to functionally equivalent methods of securing a safe depending on whether the compelled action is testimonial. When this analogy is applied to the various technologies used to secure cellphones, the apparent outcome is that the Fifth Amendment would prohibit courts from compelling some technologies to be bypassed while others would be permitted, depending on whether the compelled method to unlock the device is fairly classified as testimonial. Therefore, as is discussed above, it is this Office's opinion that our state courts likely would hold that unlocking a cell phone with biometric information is not testimonial and may be compelled.

Conclusion

As discussed more fully above, there is a clear split among the federal district courts that have addressed whether the Fifth Amendment to the United States Constitution protects a person from being compelled to unlock a cellphone or other device by providing a fingerprint or using facial recognition, referred to as biometric data. While our state courts in South Carolina have not issued a decision on this point, courts in other states are similarly divided. To date, no federal circuit court has issued an opinion on this topic. With no clear consensus, this opinion cannot be free from doubt. It is, however, this Office's opinion that our state courts likely would find the Eastern District of Kentucky's analysis in In re Search Warrant No. 5165, 470 F. Supp. 3d 715 (E.D. Ky. 2020), persuasive, hold that compelling a person to provide biometric information to unlock a cell phone is not testimonial, and, therefore, is not prohibited by the Fifth Amendment.

Sincerely,

Matthew Houck
Assistant Attorney General

REVIEWED AND APPROVED BY:

Robert D. Cook
Solicitor General