Passcodes, Biometric Features, and Fifth Amendment Self-Incrimination

BY ROBERT C. PHILLIPS

An interesting debate has surfaced recently concerning a criminal suspect's Fifth Amendment self-incrimination rights as they relate to passcodes and certain "biometric" features used to prevent third-party access to cellphones and other digital or electronic devices. The issue recently came to a head when federal Magistrate Judge Kandis A. Westmore declined to authorize a search warrant and chose to publish an opinion as to her reasons in *In re Search of a Residence in Oakland*.[1]

Search Warrant Application

A federal investigation was initiated in a case where it was alleged that two specific individuals used Facebook Messenger to extort money from a victim by threatening to distribute an embarrassing video of him if he did not provide the suspects with monetary compensation. As a part of the ensuing investigation, government agents (the agency not being identified) submitted an application to federal Magistrate Judge Westmore for a search warrant for the suspects' Oakland residence. Listed in the warrant application as things to be seized and searched were all electronic and digital devices found in the residence. Also included in the warrant application was a request for authority to compel any individuals present at the time of the search to provide their passcodes to those devices, or, if necessary, use their finger, thumb, or other biometric feature, such as facial or iris recognition, to unlock the digital or electronic devices found at the scene and to gain entry to and permit a search of the contents of each respective device.

Although the magistrate judge found sufficient Fourth Amendment probable cause to justify a search of the listed premises as well as the two suspects (based upon facts not described in her written decision), she declined the agents' requests for permission to search anyone else who happened to be present, as well as any and all electronic devices. The court found these requests to be overbroad in that they were neither limited to a particular person or persons (i.e., the two suspects in the extortion), nor to any particular device, noting the lack of probable cause to compel anyone other than the two listed suspects to do anything, or to include within its provisions the right to search any and all unspecified digital devices that might be found at the premises during the search.

Electronic Device Passcodes

But more to the point of this article, Judge Westmore also noted that the agents' request for permission to compel persons at the scene to provide passcodes to their respective electronic digital devices, if granted, would violate the subjects' Fifth Amendment's self-incrimination protections. As discussed below, Judge Westmore was probably right as to this conclusion.

As noted by Westmore, individuals have had the ability to lock their personal electronic and digital devices for decades, using numeric or alphanumeric passcodes to open them. Although yet to have a published decision directly on point from either the United States Supreme Court or any California court, lower appellate court case law from other jurisdictions tells us that a person cannot be compelled to provide a passcode to a digital device under the Fifth Amendment (absent an exception) because the act of providing law enforcement with one's passcode constitutes a "testimonial communication."[2]

These cases tell us that a physical act is "testimonial" when the act is a communication that "itself, explicitly or implicitly, relate[s] a factual assertion or disclose[s] information."[3] Providing law enforcement with a passcode has consistently been held to be testimonial because it reflects "[t]he expression of the contents of an individual's mind. …"[4]

This rule grew out of a long line of cases dealing with various governmental agencies attempting to force criminal suspects to provide access to private—potentially incriminating—documents or records, typically contained in a suspect's bank accounts or other document repositories.[5]

In sharp contrast to this rule, however, it is recognized that the Fifth Amendment does not prevent a criminal suspect from being required to provide "real or physical" evidence, such as a blood sample[6] or handwriting exemplars,[7] or to stand in a live lineup in front of witnesses wearing certain items of clothing and repeating phrases

continued on page 6

SELF-INCRIMINATION from page 5

spoken by the perpetrator of the crime.[8] None of these forms of evidence fall into the category of a testimonial communication.

Biometric Features

Judge Westmore did not stop with passcodes, however. As previously noted, the agents who applied for the search warrant in this case also asked for authority to compel individuals present at the residence to use certain biometric features, such as pressing a finger or a thumb on the screen of their digital devices, or using facial or iris recognition, if necessary, to unlock the digital or electronic devices found at the scene. As so aptly noted by Westmore:

> Today, technology has provided citizens with shortcuts to entering passcodes by utilizing biometric features. The question, then, is whether a suspect can be compelled to use his finger, thumb, iris, or other biometric feature to unlock a digital device.[9]

In declining to issue the warrant, Westmore specifically differentiated this request from those cases upholding the requirement that a suspect provide real or physical evidence, while at the same time finding fatal similarities to those cases compelling a suspect to provide his or her passcode. In so finding, she specifically held "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."[10] On this issue, Judge Westmore—ignoring significant case law to the contrary—is probably wrong.

In finding the forced use of one's biometric features to be testimonial, and thus implicating the Fifth Amendment, Westmore cites a single case in support of her conclusion on this issue from another federal district (trial level) court located in Illinois: *In re Application for a Search Warrant*.[11]

The Illinois court did in fact rule that the Fifth Amendment privilege barred the compelled use by the defendant of his fingerprint to unlock a cellphone because the act of pressing his finger to the cellphone's screen produced the contents of the phone. As reasoned by the Illinois court:

> With a touch of a finger, a suspect is [in effect] 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.[12]

As authority for this argument, both the Illinois court and Judge Westmore cite a federal Eleventh Circuit Court of Appeals decision that held that a witness' "act of production itself could qualify as testimonial if conceding the existence, possession and control, and authenticity of the documents tended to incriminate them."[13] The Eleventh Circuit in turn cites the U.S. Supreme Court decision of *Fisher v. United States*, which refers to this concept as the "implicit authentication" rationale.[14] The only problem with going down this path is that *In re Application for a Search Warrant* is a passcode case dealing with the compelled decryption of a computer's hard drive contents. *Fisher* is neither a passcode nor a biometric feature case and involves the issue of a government-issued subpoena for a criminal defendant's personal records. Neither case discusses the lawfulness of requiring a person to open his or her digital or electronic devices using biometric features.

Totally ignored by Judge Westmore is a comprehensive and relatively recent discussion of this issue by the Minnesota Supreme Court in *Minnesota v. Diamond*.[15] In noting the issue to be one of first impression, the Minnesota Supreme Court held that a suspect's act of providing a fingerprint to the police to unlock a cellphone was in fact *not* a testimonial communication. This is because the compelled act of providing a fingerprint elicited only physical evidence from the defendant's body not the contents of his mind. Thus, by not constituting a testimonial communication, the compelled use of a biometric feature to open the defendant's cellphone did not violate the Fifth Amendment privilege against self-incrimination.[16]

Westmore also ignored the findings of a Virginia state case entitled *Commonwealth of Virginia v. Baust*, even though she cited the case in her decision. *Baust* involved a situation where police seized the defendant's cellphone from his home pursuant to a search warrant but were unable to examine its contents because it was locked and encrypted. The Government filed a motion seeking to compel the defendant to either produce his passcode or provide his fingerprint, either of which would unlock the phone. The court denied the motion as to the passcode, holding that compelled disclosure would be testimonial and thus barred by the Fifth Amendment. However, the court granted the motion as to the fingerprint.

In upholding this ruling, the Virginia appellate court noted that the Fifth Amendment does not prohibit compelling a defendant to exhibit and permit the

continued on page 7

SELF-INCRIMINATION from page 6

government to document physical characteristics such as submitting to fingerprinting, standing for a photograph, making a voice recording, or providing a blood sample. The court found this to be no different than requiring a defendant to use his biometric features to unlock a cellphone. After pointing out that the production of a fingerprint, unlike a passcode, did not require the defendant to communicate any knowledge and is thus not testimonial, the court concluded that the defendant could be compelled to unlock the phone via his fingerprint consistent with the Fifth Amendment.[17]

California

California courts, of course, are not required to adopt either theory, as everything cited above is considered to be "persuasive" and not controlling in California.[18] In analyzing the above authority, however, it would seem that Judge Westmore, in failing to take into consideration any case decision above the level of a federal district court, chose to follow the minority opinion when it comes to the issue of whether it violates a person's Fifth Amendment right when he or she is in possession of an electronic or digital device and compelled to use available biometric features to unlock that device.

Potential Exceptions

If, however, Judge Westmore's opinion is to be adopted, one or more of several available exceptions to the rule might be argued, depending upon the circumstances.

First and foremost, what has been referred to as the "foregone conclusion" doctrine should be considered. Under this rule, the Fifth Amendment does not protect an act of production (e.g., using one's biometric feature to open a cellphone) when any potentially testimonial component of that act of production—such as the existence, custody, and authenticity of evidence—is a "foregone conclusion" and "adds little or nothing to the sum total of the Government's information."[19] Looking at the other side of this coin while trying to decipher what it means, it has been noted that "[t]he foregone conclusion doctrine [ ] does not apply when the Government cannot show prior knowledge of the existence or the whereabouts of the documents ultimately produced in response to a subpoena."[20]

Noting that "[t]oday's mobile phones are not comparable to other storage equipment, be it physical or digital, and are entitled to greater privacy protection," Judge Westmore held that the foregone conclusion exception did not apply to the instant case.[21] Given the fact that search warrants for the contents of digital and electronic devices are seldom able to predict, other than in general terms, what it is that a law enforcement officer expects to find, Westmore was probably correct in holding that this exception does not generally apply to circumstances such as are present here.

Another exception that might apply is when a suspect consensually provides a passcode or agrees to apply the necessary biometric feature to unlock a digital or electronic device. A "free and voluntary" consent has long since been recognized as a substitute for a search warrant or exigent circumstances.[22] Despite it being one's Fifth Amendment self-incrimination rights a suspect would be waving, as opposed to a Fourth Amendment search and seizure right, it is not likely a court would require a full-blown *Miranda*[23] admonishment and wavier in order to secure such a consent. This is because asking for consent to search a container of any sort has never required more than the subject's non-coerced acquiescence and does not involve the type of situation *Miranda* was intended to address, i.e., an in-custody interrogation.[24]

Lastly, it can be argued that anyone who is already subject to a parole or probation waiver of his or her Fourth Amendment search and seizure rights might also be compelled to provide passcodes and/or to apply the necessary biometric features to open his or her electronic devices. This is, as of yet, an undecided issue that will necessarily hinge on whether a court finds that a Fourth Amendment waiver can constitutionally be extended to situations where it is a person's Fifth Amendment self-incrimination rights that are at issue. It would help in this argument for prosecutors, when appropriate, to request upon conviction that a defendant agree to cooperate as a condition of his or her probation when access to digital or electronic devices is requested by law enforcement, specifically waiving his or her Fifth Amendment testimonial rights as are applicable to the issue here.[25]

Conclusion

How California courts will evaluate all the above has yet to be decided. But the law provided here will—at the very least—get a prosecutor's foot in the door, hopefully leading to a favorable decision.

In the meantime, this entire issue is one ripe for U.S. Supreme Court consideration, from deciding whether passcodes are indeed entitled to Fifth Amendment protection under the theory that they constitute a testimonial

continued on page 8

SELF-INCRIMINATION from page 7

communication, to how biometric features relate to the problem. Governmental-forced access to the vast amounts of private information typically contained in electronic devices being a rapidly developing area of the law, we can probably expect, or at least hope for, some Supreme Court guidance in the not too distant future.

ENDNOTES

1. *In re Search of a Residence in Oakland, California* (N.D.Cal. 2019) 2019 WL 176937.
2. See also *United States v. Kirschner* (Mich. 2010) 823 F. Supp.2d 665; *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011* (11th Cir. 2012) 670 F.3d 1335, 1346; *Commonwealth v. Baust* (Va. Cir. Ct. 2014) 89 Va. Cir. 267.
3. *Doe v. United States* (1988) 487 U.S. 201, 210.
4. *Residence in Oakland*, *supra,* at 2; citing the dissenting opinion in *Doe, supra*, at 219–220.
5. E.g., see *Doe*, *supra*, at 206–219; *Fisher v. United States* (1976) 425 U.S. 391; *State v. Alexander* (Minn. 1979) 281 N.W.2d 349; *Boyd v. United States* (1886) 116 U.S. 616.
6. *Residence in Oakland*, *supra,* at 3, citing *Schmerber v. California* (1966) 384 U.S. 757.
7. *Gilbert v. California* (1967) 388 U.S. 263.
8. *United States v. Wade* (1967) 388 U.S. 218.
9. *Residence in Oakland*, *supra*, at 2.
10. *Id.* at 3.
11. *In re Application for a Search Warrant* (N.D.Ill. 2017) 236 F.Supp.3d 1066.
12. *Id.* at 1073.
13. *Subpoena Duces Tecum Dated Mar. 25, 2011*, *supra*, at 1343.
14. *Fisher, supra,* at 412, fn. 2.
15. *Minnesota v. Diamond* (Minn. 2018) 905 N.W.2d 870.
16. *Id.* at 878.
17. *Baust, supra*, at 4.
18. *Raven v. Deukmejian* (1990) 52 Cal.3d 336, 352; *People v. Wade* (2016) 63 Cal.4th 137, 141.
19. *Fisher, supra*, at 411.
20. *Residence in Oakland*, *supra*, at 4, citing *United States v. Hubbell* (2000) 530 U.S. 27, 43; see also *United States v. Bright* (9th Cir. 2010) 596 F.3d 683; *United States v. Apple Mac Pro Computer, John Doe, et al.* (3rd Cir. 2017) 851 F.3d 238; *Kirschner*, *supra*, at 668–669.
21. *Residence in Oakland, supra*, at 4, citing *Riley v. California* (2014) 573 U.S. ___; 134 S.Ct. 2473, 2475, 2489.
22. See *Bumper v. North Carolina* (1968) 391 U.S. 543, 548.
23. *Miranda v. Arizona* (1966) 384 U.S. 436.
24. *Id.* at 445; see also *Arizona v. Mauro* (1987) 481 U.S. 520, 529–530.
25. See *In re Q.R.* (2017) 7 Cal.App.5th 1231; *In re George F.* (2016) 248 Cal.App.4th 734.

Robert C. Phillips is a retired San Diego County deputy district attorney and the author of Miranda and the Law, *a CDAA monograph originally published in 1999 and updated in 2017.*

The CDAA Anatomical Model Lending Library

Do you have a case involving strangulation, pediatric abusive head trauma, domestic violence, or physical abuse? These are just a few examples of crimes for which demonstrations using anatomical models at trial could be beneficial. Show your jury exactly what happened to the victim. All models are available at no cost to your office.

Anatomical models are expensive and usually cost-prohibitive for most prosecutors. They are items that would be "great to have for my case but no time to figure out how to get one." Civil attorneys use them regularly in their cases with remarkable success. Granted, not every criminal case warrants them, but it is time prosecutors embrace their use.

CDAA's anatomical models can be sent to any prosecutor in California. They will arrive in a protective case with a pre-paid UPS shipping label to return to CDAA when you are finished. The models can be used for in-house prosecutor and investigator training, expert preparation, and as demonstration evidence. Anatomical models should not be admitted into evidence, but they are useful to illustrate and enhance oral testimony.

Why Use an Anatomical Model?

- A prosecutor is a teacher. Where visible injuries are involved, the jury or judge (fact finder) seldom understands the consequence of a severe injury and is resistant to learning. It can be repugnant and boring. Where there is no visible injury–like perhaps in a strangulation or sexual assault case–the fact finder can be skeptical and unable to process the significance of internal organ and vascular damage.
- A prosecutor is a student. Understanding injuries is imperative to presenting your case. Using your expert to teach you helps your expert and you establish a way to educate the fact finder in court.
- Expert witnesses typically develop more authority in the eyes of the fact finder because they are teaching using the anatomical model, not lecturing. When an expert becomes a teacher, it is harder for the defense attorney to accuse the expert of not being objective.
- Videos or photos present facts from one perspective. Anatomical models are 3-D and engage the jury because they can be rotated, touched, and opened. Engaging visuals provide clarity and understanding. Fact finders are more likely to retain what they learn during deliberation when information is visual and clear.

Click HERE to see all the models available!