In *In re Search Warrant No. 5165*, 2020 WL 3581608 (E.D. Ky. July 2, 2020), Magistrate Judge Matthew A. Stinnett ruled that compelled biometrics scans of all individuals present at the scene of a warrant search violated those individuals' Fourth Amendment rights and held that the government may compel certain individuals to unlock devices using biometrics pursuant to a search warrant without violating those individuals' Fifth Amendment rights but may not compel production of a passcode.

As part of a search warrant, the United States sought to search a premises belonging to a target individual and seized electronic devices found there. The U.S. also sought to compel any individuals present on the premises to provide their biometrics — physical features unique to an individual, such as fingerprints, facial features, or iris demarcations — to unlock electronic devices on the premises. The court addressed whether such compulsion was permitted under the Fourth and Fifth Amendments. *Id.* at *1–*2.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." *Id.* at *2 (quoting U.S. Const. amend. IV). The parties did not dispute that a warrant was needed to seize and search the electronic devices, and the court had previously ruled that probable cause existed to do so. The only question was under what circumstances, if any, the government could compel any individual, whether a target or bystander, to provide biometrics in the execution of a search warrant for electronic devices.

The court and the parties agreed that law enforcement's search of the electronic devices themselves would be compliant with the Fourth Amendment if the devices were unsecured or if law enforcement accessed them without the assistance of the suspect. However, compelling biometrics went beyond the scope of seizing and searching electronic devices and could be viewed as analogous to fingerprinting an individual. Therefore, the court had to determine (1) whether capturing physical characteristics of an individual was a search, and (2) if so, what burden must the government meet to capture such individual physical characteristics.

Magistrate Judge Stinnett noted that the Supreme Court had addressed the first question, holding that taking a fingerprint is a search. *Id.* at *3 (citing *Hayes v. Florida*, 470 U.S. 811, 816–17 (1985)). *Hayes* set forth three requirements for obtaining fingerprints at the scene of a search warrant execution, which a D.C. district court reframed to determine when the government can compel the use of an individual's biometric features to unlock an electronic device. *Id.* at *3 (citing *Matter of Search of [Redacted] Washington, D.C.*, 317 F. Supp. 3d 523 (D.D.C. 2018)). The reformulated test required that (1) the procedure was carried out with dispatch and in the immediate vicinity of the premises to be searched, and, at the time of the compulsion, the government had both (2) reasonable suspicion that the individual had committed a criminal act related to the same subject matter covered by the warrant and (3) reasonable suspicion that the individual's biometrics would unlock the device. *Id.* at *4 (citing *Matter of Search of [Redacted] Washington, D.C.*, 317 F. Supp. 3d at 531).

Magistrate Judge Stinnett then reviewed a set of hypotheticals explored by the parties in briefing and argument of the case. First, he determined that when executing a search warrant for an electronic device, if the government has reasonable suspicion that a device is controlled by the target, officers on the scene may compel that target to provide biometrics to unlock the device. On

the other hand, officers on the scene could not *necessarily* compel a bystander to provide biometrics. For example, the government may have reasonable suspicion of a roommate's criminal act and the ability to unlock a device. Thus they could compel biometrics from this individual. The same could not be said for the hypothetical mail carrier present during the execution of the search. *Id.* at *4–*5.

Rejecting the probable cause standard articulated by other courts, Magistrate Judge Stinnett found that "when attempting to unlock devices during execution of a search warrant, the government may compel an individual's biometrics if there exists reasonable suspicion to believe that the individual has committed a criminal act for which the warrant authorizes an evidentiary search, *and* that the individual's biometric features will unlock the device." *Id.* at *5 (emphasis in original). The search warrant at issue was thus overbroad by applying to all individuals present.

Magistrate Judge Stinnett then turned to the Fifth Amendment, which provides that "[n]o person ... shall be compelled in any criminal case to be a witness against himself." *Id.* At *6 (citing **U.S. Const. amend. V**). He concluded that privilege against self-incrimination does not apply to providing biometrics to law enforcement in order to unlock an electronic device.

The Fifth Amendment privilege applies only when there is (1) compelled, (2) incriminating (3) testimony. Magistrate Judge Stinnett reasoned that obtaining biometrics to access a device is clearly compelled conduct and, for the sake of the instant opinion, assumed it would be incriminating. However, to be testimonial, a communication must "explicitly or implicitly, relate to a factual assertion or disclose information." *Id.* at *8 (citing *Doe v. United States*, 487 U.S. 201, 210 (1988)). Based on the "act of production" doctrine, producing items is testimonial when that production "reveals the contents of the target's thoughts or impressions." *Id.* (citing *Fisher v. United States*, 425 U.S. 391 (1976)). The Supreme Court's analysis focuses on the lock versus key distinction, wherein the court determines whether the act of production is more similar to revealing the combination to a safe or to the surrender of a lockbox key. The former is testimonial; the latter is not. *Id.* at *9.

The Magistrate Judge determined that given the Supreme Court's analysis, the only reasonable conclusion was that biometrics are a physical item that can be produced without mental impressions, communications, or admissions of *mens rea.* Compelling a target to unlock a device using these means "sheds no light on his actual intent or state of mind." *Id.* at *10 (quoting ***Doe I*, 487 U.S. 201, 216 (1988)**). Biometrics were analogous to key in the lock-versus-key test.

On the other hand, a passcode was no different from a combination lock and is thus afforded Fifth Amendment protection. While passcodes and biometrics both perform the function of unlocking a device, "biometrics are not passcodes." *Id.* at *12. Precedent emphasized that the act of production doctrine applies only when the act compelled "make[s] extensive use of 'the contents of [the target's] own mind.' " *Id.* (quoting *United States v. Hubbell*, 530 U.S. 27, 43 (2000)). Passcodes do reveal the contents of the target's mind; biometrics do not.

While recognizing that other courts deemed it "absurd" that a defendant's compelled production of password-protected information would hinge on whether the information was protected by biometrics or by a password, Magistrate Judge Stinnett found that precedent required that result. "[E]ven when presented with legal questions impacted by changing technology that has triggered

significant modifications of individuals' behavior, a lower court cannot ignore or rewrite the constitutional principles the Supreme Court has articulated. Rather, this Court's job is to interpret and apply those precedents as faithfully as possible." *Id.* at *14 (quoting *Matter of Search of [Redacted] Washington, D.C.*, 317 F. Supp. 3d at 539–40).