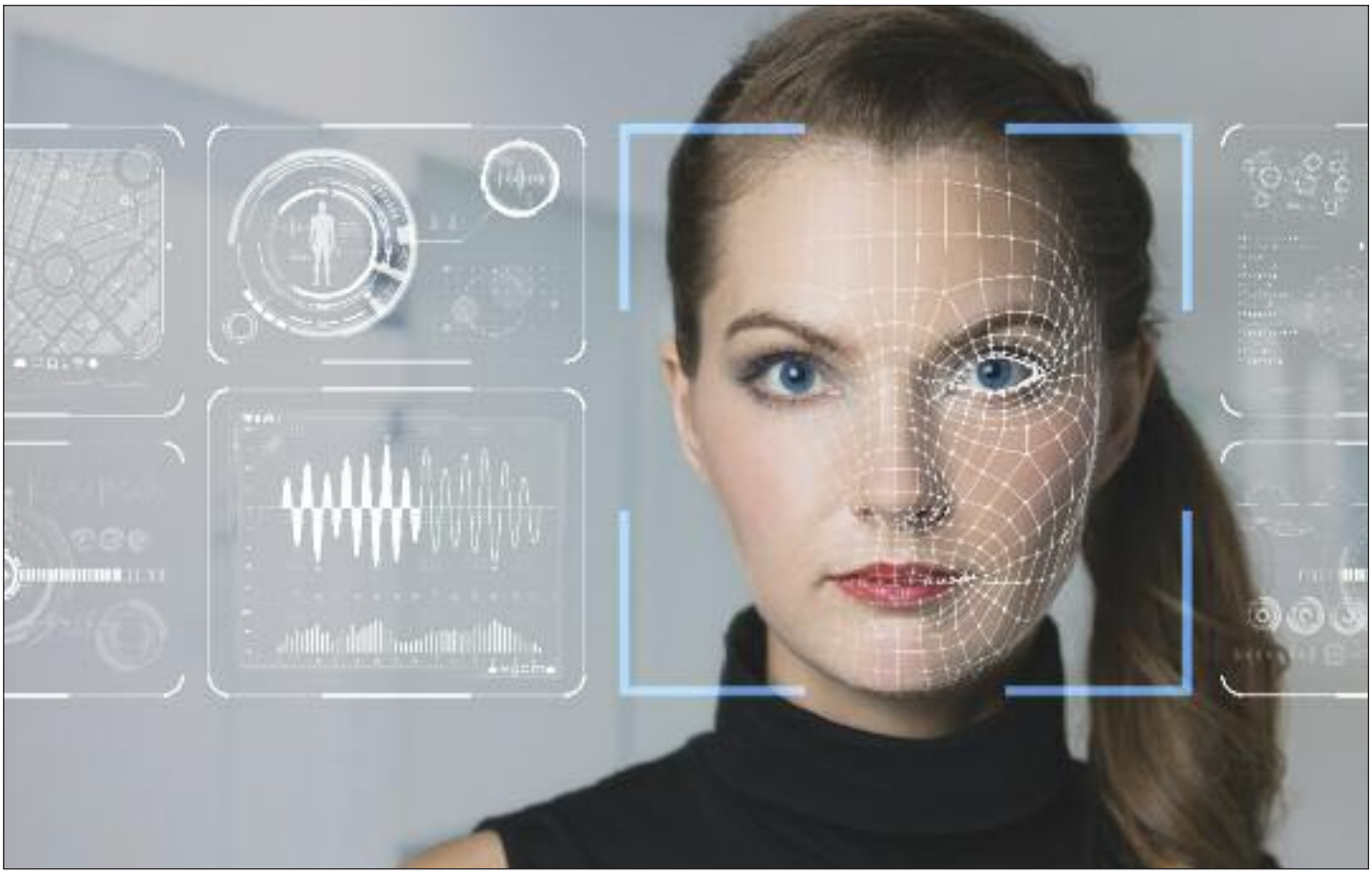
SPRING/SUMMER 2018

common DEFENSE

A member publication of Kentucky Defense Counsel, Inc.



BIOMETRICS AND THE CONSTITUTION: EXPLORING HOW THE DEVELOPMENT OF TECHNOLOGY IMPACTS OUR CIVIL LIBERTIES

By Olivia Amlung
Adams, Stepner, Woltermann & Dusing, PLLC
Covington

The evolution of technology repeatedly creates the need for a complete reevaluation of how our constitutional rights are protected from governmental intrusion. Courts are forced to apply holdings and analyses to facts which, at the time of the original decision, were technologically unimaginable. A mere ten to fifteen years ago, police could only obtain minimal information from the search of a cell phone. At that time, a cell phone search would likely only reveal a few saved phone numbers and phone owner's highest Snake score. But in 2007, when Apple rolled out its first iPhone commercial, our society unknowingly commenced a new era of legal conundrums stemming from the exponential popularity that these "smart" phones would soon gain. Today, with the simple touch of a button, the contents of a phone can provide the most personal details of a phone owner's life—bank transactions, complete location and tracking details, call history, health information, and more. Given the unimaginable amount of information that can be found on a phone, individuals are increasingly motivated to shield their data from prying eyes.

In 2013, consumers were given the opportunity to purchase the first generation of mass-produced biometric authentication technology — Apple's Touch ID. Touch ID and similar programs allow users to gain access to their phone with a quick scan of their unique fingerprint. Four years later, Apple rolled out its newest and most innovative biometric technology yet—the iPhone X. Customers willing to spend the near $1,000 for a new phone are able to make use of a slew of cutting-edge features, the most innovative of which is "Face ID." Similar to Touch ID, Face ID eliminates the need for manual passcode entry by using biometric authentication to allow a user to gain access to his or her electronic device.[1]

What is Biometric Authentication?

Biometric authentication involves use of a biometric identifier, simply described as a person's unique biological data or physical feature, to confirm a person's identity for security purposes. Biometric identifiers can include a person's fingerprint, their voice, or even their facial features. When the user of an electronic device stores a biometric identifier, the identifier becomes a unique passcode for access. Only the individual possessing the unique, biometric identifier can gain access to the device.

Face ID, a form of biometric authentication, allows users to unlock their phones with nothing more than a quick glance at their screen. Face ID maps the geometry of the user's face to create a secure passcode of sorts which prevents anyone other than the user from accessing the contents of the phone. Using a 3-D map created by more than 30,000 infrared dots projected onto a person's face, Face ID detects and matches the user's face to unlock their phone without the need for the device passcode. When a face is detected, Face ID is intended to confirm attention and intent to unlock by detecting that the user's eyes are open and directed at the device. The technology is purported to be fool-proof when it comes to photos and masks, and the feature allegedly cannot be used when an individual's eyes are closed (i.e., when a phone is placed in front of a sleeping individual's face).[2]

Why Are Biometric Authentication Programs Legally Significant?

While new features such as Face ID are advertised to dramatically enhance iPhone security and protect against prying eyes, this technology may inadvertently provide law enforcement with an easier way to access users' personal information. By casually placing a phone in front of an individual's face, an officer can acquire a plethora of information about that individual and his or her connection with a potential piece of evidence. These phones are often guarded with Fort Knox-style security features and can even contain sophisticated mechanisms which will automatically erase the contents after a certain number of incorrect password entries. While some agencies possess the ability to hack into a locked phone and search its contents, most local law enforcement agencies stick with the easiest method of entry—convincing the device's owner to provide the means of access. If an individual refuses to provide the digits of a passcode or refuses to cooperate while officers physically force his or her finger to a scanner, the task of obtaining access can be daunting. But with Face ID, this objective is much easier to achieve. With one glance, officers can quickly unlock the phone, gain access to its contents, and, for the purposes of this article, accomplish the most significant task: learning who owns and uses that phone. When an individual possesses the approved biometric passcode for a device, he or she simultaneously demonstrates control and ownership of that same information.

Similar to the questions raised by Apple's earlier Touch ID technology, Face ID raises concerns over an individual's constitutional right against self-incrimination: Can an officer use an individual's face to unlock a cell phone *without* his or her permission? Can a court *order* an individual to unlock a phone via this method? Unlocking a phone is now as easy as casually flashing it in front of an individual's face—but when does that split-second act become a violation of someone's civil liberties and constitutional rights?

Imagine This Hypothetical

An officer pulls over a vehicle on the highway for a traffic violation. There are three passengers in the backseat. The car smells

strongly of marijuana, and the officer notices multiple baggies of narcotics strewn around the vehicle. As all three backseat passengers exit the vehicle during their arrest on possession charges, the officer's partner notices an iPhone lying on the backseat floor. No one claims the phone, so the officer decides to make it easy for them. Recognizing that the phone is an iPhone X with Face ID technology, the officer places the phone in front of each passenger's face until the phone finally unlocks, thus identifying its owner.

Later, that phone is found to contain text messages relating to a murder which occurred in the area a month prior. The owner of the phone, who was identified by use of the Face ID feature, has now been indicted in relation to the murder.

So the question remains: when, if at all, did the officer's actions become a violation of that individual's civil liberties and/or her Fifth Amendment freedom from self-incrimination?

When Compelled Production of Biometrics Becomes Self-Incrimination

The first generation of smart phone security features prompted users to create a four-digit PIN enabling only those who know the four digits to access the phone's contents. For the reasons described below, this PIN was the epitome of security within the context of the Fifth Amendment. But, as technology companies continuously strive to create the most advanced security features and prevent prying eyes from accessing the phones of others, these companies may be inadvertently reducing their customers' security under the law.

After passcode protection became standard issue for all smartphones, Apple introduced Touch ID. As one would expect based on its name, Touch ID uses a biometric scanner to unlock the user's phone with the touch of a button. A user presses his or her finger to a touch sensor that rapidly scans for the unique pattern formed by the swirling ridges of the owner's fingertips. Access is only granted if the print matches. Since the unveiling of Touch ID in late 2013, courts across the nation have been asked to evaluate whether the compelled production of a fingerprint, in the capacity of its use as a passcode, violates the Fifth Amendment. Now, with the introduction of Face ID, the analysis of forced biometric production is even more unsettled than before.

Understanding the Fifth Amendment in this Context

The question of when the Fifth Amendment can be used to protect an individual from following a government directive is by no means new. For over a century, courts have evaluated what law enforcement can and cannot do with regard to forcing individuals to manipulate, test, or produce pieces of evidence. As early as 1910, a criminal defendant raised Fifth Amendment concerns when the government sought to force him to wear a specific shirt at trial to demonstrate that it was, in fact, his shirt. In dismissing the defendant's challenges and compelling him to wear the clothing, the Supreme Court reasoned:

> [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.

Holt v. United States, 218 U.S. 245, 252-53 (1910). This concept still serves as the basis for assessing whether the act of producing certain evidence, when completed under government compulsion, is protected by the Fifth Amendment. When the State of California tried O.J. Simpson for murder, assistant prosecutor Christopher Darden was able to force Simpson to try on a glove during a murder trial. That infamous moment, resulting in the ever-popular mantra "if it doesn't fit, you must acquit," was not a violation of Simpson's Fifth Amendment rights because the act of putting on the glove was a mere use of his body as physical evidence. As the Supreme Court once explained, "[a] party is privileged from producing the evidence but not from its production." *Johnson v. United States*, 228 U.S. 457, 458 (1913). Essentially, the analysis can be summed up in one query—whether the forced action, and the evidence obtained therein, is testimonial or physical in nature. Testimonial acts are protected by the Fifth Amendment; mere physical acts are not.

While the question may seem straightforward, the analysis is far from simple. The U.S. Supreme Court has held that a physical act can become testimonial if it "tacitly concedes" that the produced materials exist and are in the possession or control of the individual. *Fisher v. United States*, 425 U.S. 391, 410 (1976). But the Court has neither drawn a clear line nor created a list of criteria explaining when an act stops being merely "physical" and ventures into "testimonial" territory. When the act becomes testimonial, the Fifth Amendment applies. In an effort to simplify this complex evaluation, Justice Stevens set forth a metaphor which would thereafter be relied upon to this day. He stated:

> A defendant can be compelled to produce material evidence that is incriminating. Fingerprints, blood samples, voice exemplars, handwriting specimens, or other items of physical evidence may be extracted from a defendant against his will. But can he be compelled to use his mind to assist the prosecution in convicting him of a crime? I think not. **He may in some cases**

But the Court has neither drawn a clear line nor created a list of criteria explaining when an act stops being merely "physical" and ventures into "testimonial" territory. When the act becomes testimonial, the Fifth Amendment applies.

be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe — by word or deed.

Doe v. United States, 487 U.S. 201, 219 (1988) (Stevens, J., dissenting) (emphasis added). While a dissent is not legally binding precedent, the majority opinion in *Doe* contained a footnote endorsing Justice Stevens' framework and clarified that its only disagreement was with his preferred outcome in the case. *Id.* at 210 n.9. The "combination versus key" metaphor was next relied upon by the Supreme Court in 2000, solidifying its place as the controlling analysis for Fifth Amendment protections. *United States v. Hubbell*, 530 U.S. 27, 43 (2000).

Thus, assessing whether biometric technology, such as Face ID, has Fifth Amendment implications begs one inquiry: whether the human face is more synonymous with a key to a strongbox or a combination to a wall safe.

Biometric Recognition: Key or Combination?

The Fifth Amendment's application to compelled biometric production has not been heavily litigated to date, presumably due to the technology's relative novelty. But there are two clear schools of thought emerging from the jurisdictions which have addressed the topic: the first gives all deference to the physical nature of biometrics, and the second relies heavily on the potential for derivation of implicit testimony. The former consistently holds there are no Fifth Amendment implications in forcing an individual to unlock his or her phone by finger touch—producing fingerprints is like producing a key to a strongbox. The latter, however, uses a case-by-case assessment to analyze the implicit testimony the physical act could provide—under certain circumstances, producing fingerprints can be as testimonial as producing the combination to a safe.

Those jurisdictions which rely solely on the inherent physical nature of fingerprint production find the fingerprints more synonymous with a "key to a strongbox" under Justice Steven's "key versus combination" metaphor. The rationale behind this "key theory" has been most recently enumerated by the Minnesota Supreme Court in *State v. Diamond*, 905 N.W.2d 870 (Minn. 2018), petition for cert. filed, (U.S. Apr. 3, 2018) (No. 17-8336). Relying on antiquated U.S. Supreme Court precedent regarding the absence of Fifth Amendment implications in mere physical acts of production, the *Diamond* court rejected the notion that production of a fingerprint is in any way testimonial. Id. at 874 (citing *United States v. Dionisio*, 410 U.S. 1, 7 (1973)(compelled production of voice exemplars did not violate the Fifth Amendment privilege against compulsory self-incrimination) and *United States v. Wade*, 388 U.S. 218, 222 (1967)(exhibiting a person for observation in a lineup by witnesses and using his voice as an identifying physical characteristic involved no compulsion of the accused to give evidence of a testimonial nature against himself)). According to those jurisdictions which have adopted this "key theory" approach, production of a fingerprint for Touch ID comparison is simply the production of a physical characteristic. This logic makes the act of producing a fingerprint to unlock a phone synonymous with forcing that same individual to be fingerprinted when booked into the county jail. A fingerprint is a fingerprint regardless of the motivation for its production.

In short, when asking whether compelled production of a fingerprint implicates the Fifth Amendment, the only answer the courts can provide thus far amounts to a whopping "it depends."

Alternatively, the second school of thought gives more flexibility to the self-incrimination assessment in the context of biometric production. This approach acknowledges the production of fingerprints can have testimonial implications; but the analysis also provides numerous caveats which may allow the government to render any testimonial value irrelevant and thereby circumvent the potential Fifth Amendment concerns. *See State v. Stahl*, 206 So. 3d 124, 133-34 (Fla. Dist. Ct. App. 2016); *see also In re Single-Family Home & Attached Garage*, No. 17 M 85, 2017 U.S. Dist. LEXIS 170184 (N.D. Ill. Feb. 21, 2017).

Following with Justice Stevens' framework, the second school of thought looks beyond the physical nature of a biometric identifier and instead focuses on the possibility of the implicit testimony being conveyed. It calls for a pure evaluation of the circumstances surrounding compelled production and an assessment of whether the production itself functions as a "key" or a "combination." If the government can "establish[], through independent means, the existence, possession, and authenticity of the [produced evidence]," the act of production serves as nothing more than a "key" to unlock the data because any testimonial value has been rendered a "foregone conclusion." *Stahl*, 206 So. 3d at 135 (citing *Fisher*, 425 U.S. at 411). In this instance, an individual can no longer fear self-incrimination because the government already possesses any information which the individual could implicitly convey (i.e., phone ownership and control).

In short, when asking whether compelled production of a fingerprint implicates the Fifth Amendment, the only answer the courts can provide thus far amounts to a whopping *"it depends."* It depends on the jurisdiction, it depends on the judge, and it most definitely depends on the surrounding circumstances. The limited case law addressing Touch ID and the Fifth Amendment is wholly unsettled, and it does not appear that judicial assessment of Face ID will be any different. If anything, the assessment is even more convoluted than

it has been with Touch ID and the production of fingerprints — what happens if Face ID and similar facial recognition programs can be deceived with high-resolution photos of the phone's suspected owner? Will the owners of phones still enjoy Fifth Amendment protection for the use of their likeness?

Until the Supreme Court takes up this issue, there is no way of knowing the outcome. Biometric authentication, regardless of the biometric identifier, may be a key or it may be a combination. Moving forward, the only certainty upon which we can rely is this: the more biometric technology develops, the less certain the law becomes. So, at this point, law enforcement should make it their practice to err on the side of caution when gaining access to a suspect's phone via compelled biometric authentication. If not, they could be exposing themselves to a flood of civil rights litigation alleging violations of the Fifth Amendment's protection against self-incrimination.

Predicting the Implications Under 42 U.S.C. § 1983

42 U.S.C. § 1983 imposes liability on a state actor who "causes to be subjected . . . any citizen . . . to the deprivation of any rights." In other words, under this section, "a public official is liable under § 1983 only if he causes the plaintiff to be subjected to a deprivation of his constitutional rights." *Baker v. McCollan*, 443 U.S. 137, 142 (1979)(internal quotation marks and citation omitted). Section 1983 does not afford individuals any new legal rights, but instead provides a cause of action for individuals who have suffered a violation of their already-existing rights—one such right being that against self-incrimination.

Admittedly, § 1983 actions alleging violation of an individual's right to be free from self-incrimination are, at this point, few and far between. However, that is not to say that such actions are unheard-of. Many jurisdictions, including the Sixth Circuit, have entertained actions brought under 42 U.S.C. § 1983 premised on a claim that an individual's right to be free from self-incrimination had been violated. In 2005, the Sixth Circuit expressly rejected a district court's determination that police officers may never be liable for violating someone's Fifth Amendment rights. *McKinley v. Mansfield*, 404 F.3d 418, 439 (6th Cir. 2005). Although it was a prosecutor who technically used the self-incriminating information during a criminal proceeding, the Sixth Circuit opined, "it is the person who wrongfully coerces or otherwise induces the involuntary statement who causes the violation of the [Fifth Amendment] privilege." Id. (citing *Williams v. Fedor*, 69 F. Supp. 2d 649, 676 (M.D. Pa. 1999), *aff'd without opinion*, 211 F.3d 1263 (3d Cir. 2000)). When such a violation occurs, liability attaches under § 1983.

Given the current air of uncertainty surrounding potential Fifth Amendment implications, officers who forcibly compel an individual to access his or her cell phone via biometric authentication *could* be exposing their agency to civil liability under § 1983. When faced with the execution of a valid search warrant, a criminal defense attorney may have no other choice than to attack the steps leading up to the search, or how officers first accessed the phone. With the vast amount of information stored on a person's cell phone, the stakes are high when it comes to keeping the government's prying eyes at bay. Both defendants and their attorneys are more motivated than ever to poke holes in law enforcement's access to electronically stored information. Obtaining a valid search warrant will often shield officers from § 1983 liability related to the Fourth Amendment protection from unreasonable searches and seizures. *See Hale v. Kart*, 396 F.3d 721, 725 (6th Cir. 2005) (holding officers who rely on a valid warrant are

Given the current air of uncertainty surrounding potential Fifth Amendment implications, officers who forcibly compel an individual to access his or her cell phone via biometric authentication could be exposing their agency to civil liability

generally insulated from liability pursuant to § 1983 for Fourth Amendment violations). However, it is crucial for police agencies to understand the mere existence of a valid search warrant will do nothing to refute allegations that officers violated an individual's Fifth Amendment rights while executing that warrant. *See United States v. Blank*, 459 F.2d 383, 386 (6th Cir. 1972) (holding a "valid search warrant does not 'compel' the defendant to do anything in Fifth Amendment terms"); *see also United States v. Billings*, No. 2:17-cr-122-NT, 2018 U.S. Dist. LEXIS 891, at *6 (D. Me. Jan. 3, 2018). A ticket to the amusement park is useless if the gates are locked and there is no other way inside.

Oftentimes, a police officer can merely ask for information and a defendant will begrudgingly oblige. But if police are met with opposition when asking for a phone's passcode or the use of a suspect's fingerprints for Touch ID access, it is advisable not to pursue the matter without the court's guidance. The same is true even if the phone could be accessed with one quick and seemingly innocent flash of a suspect's face to engage the facial recognition software. A valid search warrant is *not* guaranteed to protect an agency from liability; on the contrary, valid assertions of one's Fifth Amendment protections can negate a search warrant's effectiveness in certain circumstances. *See Blank, supra*. Until the Supreme Court, or even a majority of the nation's jurisdictions, addresses the use of biometric authentication and the potential Fifth Amendment implications therein, one cannot safely predict how a court will decide this type of § 1983 claim. Until then, police agencies, and the attorneys who represent them, should train their officers to err on the side of caution when dealing with the unique situations created by biometric authentication in an effort to avoid potential exposure to civil liability.

Conclusion

Think back to the hypothetical posed at the outset of this article which involved three individuals and an unclaimed cell phone in the back of a car. Under the current state of the law, were the officer's actions permissible under the Fifth Amendment? Could the officer hold up the cell phone to each individual's face until the phone finally unlocked? If not, do the individuals have a viable action under 42 U.S.C. § 1983? Maybe. Or maybe not. Until this matter is raised before and fully evaluated by our nation's highest courts, the legal world cannot know for sure.

The rapid pace of innovation in the world of technology creates a constant need for reevaluation of the Constitution's implications in the routine practices of law enforcement. Far too often, courts are forced to apply holdings and analyses to facts which were technologically unimaginable at the time a particular decision was rendered. In 1988, when Justice Stevens first made his "key versus combination" metaphor, it is unlikely he imagined this framework would be applied to the advanced technologies of biometric authentication which have become commonplace in our everyday cell phone use. The only certainty is this: as technology develops, courts must be prepared to adapt their precedent and begin to define how these developments impact the protection of our civil liberties.

[1] *For more information on biometric authentication, refer to the Human Interface Guidelines, Apple, Inc., found at https://developer.apple.com/ios/human-interface-guidelines/.*

[2] *For more information on Face ID and its function, refer to the Face ID Security Guide, Apple, Inc., found at https://apple.com/business/docs/FaceID_Security_Guide.pdf.*

Olivia Amlung is an associate attorney at Adams, Stepner, Woltermann & Dusing, PLLC, a full-service law firm located in Covington, Kentucky. Ms. Amlung is a member of the firm's General Litigation Practice Group. Her practice primarily focuses on claims involving personal injury, criminal defense, government litigation, and a variety of other civil litigation matters.

KentuckyDefenseCounsel

P.O. Box 127
Harrods Creek, KY 40027-0127