The Complexities of Compelling Facial Biometrics

BY BENNY FORER

> **You use a glass mirror to see your face; you use works of art to see your soul.**
>
> *—George Bernard Shaw*

Our physical features are often the defining objective criteria by which we are judged, evaluated, and assessed by other members in society. Specifically, identity and the way a person appears to others is fundamental to the criminal justice system and prosecutions. Issues dealing with identification methods—whether in court,[1] via lineup, six-pack, or other manners—have been grappled with and contemplated over time and have largely dealt with suggestibility or lack of reliability of an identification. In this new age of technology, however, issues have taken a new and different form: Whether an individual can be compelled to display his or her physical features for evidentiary or access purposes.

Modern technological innovations and conveniences have given rise to this new and unique issue. The ubiquity of technology and society's obsessiveness with electronic devices[3] have given courts pause when dealing with privacy rights and when and how the government can access an individual's device(s). Innovations designed to provide the user with a better experience are also capable of being exploited by the government.

In an effort to make devices more user-friendly, while simultaneously making security a priority, manufacturers have migrated toward using biometrics to secure those devices.[4] Facial recognition, in particular, is offered on many mobile devices, including Apple and Android, and provide the benefit of secure control over your own device. For example, Apple maintains that "The probability that a random person in the population could look at your iPhone or iPad Pro and unlock it using Face ID is approximately 1 in 1,000,000 with a single enrolled appearance."[5] Essentially, Face ID has the effect of securing a device so that it can only be used by the authorized user and possessor.

The complexity of electronic devices, along with more restrictive laws,[6] has generated unremitting difficulties for detectives and prosecutors who need to access necessary and pertinent data contained on a suspect's device(s). Constant manufacturer software updates initiate a mirroring response from forensic software companies to create tools that enable access to those devices. When these tools are out of date or reach a point of inaccessibility, investigations are hampered and stall.[7] These issues apply even if a well-crafted search warrant authorizes access.

"Compelled Decryption of Devices," an article by James Laughlin in *Prosecutor's Brief,* addressed the issues of compelling access to an electronic device.[8] The article discussed the issues pertaining to compelling an individual to supply law enforcement with information, with a particular focus on the compulsion of a password to access these devices. The difficulty is that forcing someone to provide or enter a password for a device gives rise to Fifth Amendment issues of self-incrimination. This article will discuss the issue of compelling biometrics, i.e., requiring an individual to provide their *face* for the purposes of unlocking a device.

The Fifth Amendment provides that "… nor shall be compelled in any criminal case to be a witness against himself." The courts have interpreted this clause as having three distinct requirements. First, that an individual be compelled; second, that the compulsion be of testimonial significance; and third, that it be incriminating.[9] Compelling an individual to provide biometric information contends with whether or not compelling a person's physical features to be displayed in relation to the device is protected by the right against self-incrimination.

Interestingly, issues of physical compulsion are not new, and the law appears settled in this area. As any prosecutor knows, an individual can be compelled to provide a DNA sample,[10] a blood sample,[11] saliva,[12] urine,[13] breath,[14] a haircut or shave,[15] etcetera.[16] The source of these holdings is longstanding. In 1910, the U.S. Supreme Court decided in *Holt v. United States* whether a defendant can be compelled to try on a shirt that was alleged to have been worn by the murderer. The court denied the defendant's motion under the Fifth Amendment and stated:

> Another objection is based upon an extravagant extension of the Fifth Amendment … the 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

continued on page 11

FACIAL BIOMETRICS from page 10

> him, not an exclusion of his body as evidence when it may be material."[17]

This case and its progeny established that physical compulsion is not testimonial because it does not compel the suspect to reveal or disclose information or content that is unknown. Thus, in 1966, the United States Supreme Court in *Schmerber v. California* found that a compelled blood draw did not violate the defendant's Fifth Amendment rights because it was not testimonial.[18] Similarly, a physical lineup that required an utterance[19] and a grand jury demand for a voice exemplar[20] did not violate either defendant's rights for the same reason.

Notwithstanding the various court-stated positions on physical compulsions, courts have begun evaluating electronic devices differently.[21] A district court in Nevada was recently presented with the issue of compelled biometrics—specifically, facial identification. In *USA v. Wright*, the defendant was under investigation for possibly possessing child pornography.[22] The defendant was located and arrested for failing to register as a sex offender. Seeking to obtain evidence of further offenses, the detectives Mirandized the defendant. The defendant invoked his right to counsel and questioning was terminated. However, the defendant was ordered to remove his glasses and his cellular phone was held up to his face, which unlocked the device. Subsequently, a warrant to search the device was obtained and it was searched. No items of relevance were located on this device.[23]

In this matter, there was no dispute between the parties that the evidence was obtained by compulsion, and that it would be incriminating. The issue was whether compelling the defendant to provide his face to unlock his cellular device was testimonial. In holding that it was, the court found that obtaining facial identification for the purpose of unlocking a device reveals the contents of the individual's mind. The court briefly discussed the various federal district court cases that have resolved similar issues (e.g., fingerprint recognition) and found the testimonial cases to be more compelling.[24]

Thus, the court held that a biometric feature is the functional equivalent of a passcode, which if compelled, would be testimonial. Necessarily, this position must disregard the prior U.S. Supreme Court history that maintains this would be "an extravagant extension of the fifth amendment." Material evidence that is contained on a person's body has no privacy rights and is admissible evidence regardless of how incriminating it may be. The use of a defendant's face is not for its communicative qualities, rather for identifying physical qualities.

There is a common thread in the line of cases cited above: The compelled acts required pertain to a physical

continued on page 12

HUMAN TRAFFICKING from page 9

do represent the interests of victims throughout the proceedings," they wrote. "This advocacy on behalf of trafficking victims is a great comfort to survivors, many of whom feel they have never had anyone 'on their side.'"[4]

Further elements of the white paper include "toolbox ideas" throughout each chapter containing useful tips that can be incorporated by prosecutor offices. The report also highlights the many myths and misconceptions of human trafficking, including distinguishing it from prostitution and smuggling. In addition to Stephan and Patrick, other contributors to the white paper include CDAA President and Alameda County District Attorney Nancy O'Malley; Los Angeles County District Attorney Jackie Lacey; Alessandra P. Serrano, chief of the Criminal Division of the United States Attorney's Office District of the Virgin Islands, and Nicole Roth and Mary Ellen Barrett, San Diego County deputy district attorneys.

ENDNOTES

1. National District Attorneys Association, *National Human Trafficking Prosecution Best Practices Guide* (2020) <https://mcusercontent.com/c922c7933b72f97867304b913/files/624cc7ff-9446-4380-b93f-3ffa5ecac220/20200100_National_Human_Trafficking_Prosecution_Best_Practices_Guide_White_Paper_NDAA_Womens_Prosecutor_Section_Patrick_Stephan.pdf> (accessed Feb. 11, 2020).
2. *Id.* at p. 21.
3. Ami Carpenter and Jamie Gates, *The Nature and Extent of Gang Involvement in Sex Trafficking in San Diego County* (2016) San Diego, CA: University of San Diego and Point Loma Nazarene University <https://www.ncjrs.gov/pdffiles1/nij/grants/249857.pdf> (accessed Feb. 11, 2020).
4. NDAA, *Human Trafficking Prosecution Guide, supra,* at p. 34.

Brian Heaton is CDAA's managing editor. Prior to joining CDAA in January 2016, he spent five years as a journalist, covering technology and the law for a variety of public sector-centered trade publications, including Government Technology *and* Governing *magazines. Heaton earned his Juris Doctor from Western New England University School of Law in 2003.*