Police Cannot Force Some Phone Unlocks

February 2019

Article Source : http://www.patc.com/weeklyarticles/2019_searchresidence_chapman.shtml

©2019 Jim Chapman, Attorney, Public Agency Training Council

In In the Matter of the Search of a Residence in Oakland, California, ___ F. Supp. 3d___, 2018 WL 176937 (N.D. Cal. Jan. 10, 2019), a United States Magistrate Judge in the United States District Court for the Northern District of California issued a ruling that is contrary to most rulings across the United States. Unlike other judges, United States Magistrate Judge Kandis Westmore held that law enforcement officers cannot force people to unlock their smartphones using their face, eyes, or fingerprints because such an act is testimonial for purposes of the Fifth Amendment, and the Fifth Amendment prohibits law enforcement officials from compelling a person to testify against himself.

In this case, the Government was investigating two individuals believed to be involved in extortion in violation of 18 U.S.C. § 875(d). According to the Government, the suspects allegedly used Facebook Messenger to communicate with a victim in which they threatened to distribute an embarrassing video of him if he did not pay them. The Government submitted an application for a search and seizure warrant to seize various items presumed to be located at a residence in Oakland, California ("Subject Premises") connected to the two named suspects. The application further requested the authority to seize various items, including electronic devices such as mobile telephones and computers ("digital devices"). Upon review, Magistrate Judge Westmore found that there were sufficient facts to support a finding of probable cause to conduct a search of the Subject Premises.

However, the Government also sought the authority to compel any individual present at the time of the search to press a finger (including a thumb) or utilize other biometric features, such as facial or iris recognition, for the purposes of unlocking the digital devices found in order to permit a search of the contents as authorized by the search warrant. Magistrate Judge Westmore found that the Government's request ran afoul of the Fourth Amendment and the Fifth Amendment and denied that portion of the search warrant application.

As for the Fourth Amendment, Magistrate Judge Westmore held that the request to search the Subject Premises was proper, but the request to search any and all electronic devices found during the search and to use the phones' biometric features to retrieve data from the phones was overbroad. Magistrate Judge Westmore noted that the Fourth Amendment protects the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures. The basic purpose of this Amendment is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials. After reviewing the warrant application, Magistrate Judge Westmore concluded that there were sufficient facts in the affidavit to believe that evidence of the crime would be found at the Subject Premises,

and so, the Government had probable cause to conduct a lawful search, so long as it comported with the Fourth Amendment.

On the other hand, Magistrate Judge Westmore concluded that the Government's request for an order that would allow agents executing the warrant to compel any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features was overbroad. Although there were two suspects identified in the affidavit, the request was not limited to a particular person or to a particular device. Therefore, Magistrate Judge Westmore found that the warrant application did not establish sufficient probable cause to compel any person who happened to be at the Subject Premises at the time of the search to provide a finger, thumb, or other biometric feature to potentially unlock any unspecified digital device that may be seized during the otherwise lawful search.

Furthermore, Magistrate Judge Westmore found that the Government's request to search and seize all digital devices at the Subject Premises was similarly overbroad. The Government cannot be permitted to search and seize a mobile phone or other device that is on a non-suspect's person simply because they are present during an otherwise lawful search because, to do so, would violate the Fourth Amendment's reasonableness requirement. In other words, Magistrate Judge Westmore determined that such a request was too broad to comport with the Fourth Amendment's requirements.

As for the Fifth Amendment, Magistrate Judge Westmore stated that, even if probable cause existed to seize devices located during a lawful search based on a reasonable belief that they belong to a suspect, probable cause does not permit the Government to compel a suspect to waive rights otherwise afforded by the Constitution, including the Fifth Amendment right against self-incrimination. The Fifth Amendment provides that no person shall be compelled in any criminal case to be a witness against himself. The proper inquiry is whether an act would require the compulsion of a testimonial communication that is incriminating. Magistrate Judge Westmore opined that the issue is whether the use of a suspect's biometric feature to potentially unlock an electronic device is testimonial under the Fifth Amendment.

Unlike other federal judges across the country, Magistrate Judge Westmore held that use of a suspect's biometric features to unlock a smart phone was testimonial under the Fifth Amendment. In reaching this conclusion, Magistrate Judge Westmore noted that courts have an obligation to safeguard constitutional rights and cannot permit those rights to be diminished merely due to the advancement of technology. Citizens do not contemplate waiving their civil rights when using new technology, and the United States Supreme Court has concluded that, to find otherwise, would leave individuals at the mercy of advancing technology.

In addition, Magistrate Judge Westmore stated that users have had the ability to lock their electronic devices by using an alpha-numeric code for decades and that 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. Testimony is not restricted to verbal or written communications. Acts that imply assertions of fact can constitute testimonial communication for the purposes of the Fifth Amendment. Specifically, a witness's act of production itself could qualify as testimonial if conceding the existence, possession and control, and authenticity of the documents tended to incriminate them.

Magistrate Judge Westmore acknowledged that 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. But a distinction has emerged, often expressed in different ways, in 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.

Magistrate Judge Westmore found that utilizing a biometric feature to unlock an electronic device is not akin to submitting to fingerprinting or a DNA swab because it differed in two fundamental ways. First, the Government conceded that a finger, thumb, or other biometric feature may be used to unlock a device in lieu of a passcode. 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 acknowledged, 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.

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. This feature is, no doubt, a security feature to ensure that someone without the passcode cannot readily access the contents of the phone. In fact, the Government expressed some urgency with the need to compel the use of the biometric features to bypass the need to enter a passcode. This urgency appeared to be rooted in the Government's inability to compel the production of the passcode under the current jurisprudence. It followed, 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.

Second, requiring someone to affix their finger or thumb to a digital device is fundamentally different than requiring a suspect to submit to fingerprinting. 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 to 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.

Magistrate Judge Westmore also found it noteworthy that many smartphone applications provide access to personal, private information—including medical records and financial accounts—and allow users to utilize biometric features in lieu of passcodes to access those records. Therefore, Magistrate Judge Westmore determined that a phone's 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.

Magistrate Judge Westmore sympathized with the Government's interest in accessing the contents of any electronic devices that it might lawfully seize. Nevertheless, Magistrate Judge Westmore asserted that there were other ways that the Government could access the contents of those devices that do not trample on the Fifth Amendment. For example, the Government could obtain any Facebook Messenger communications from Facebook under the Stored Communications Act or a warrant based on probable cause. While it may be more expedient to circumvent Facebook and to attempt to gain access by infringing on the Fifth Amendment's privilege against self-incrimination, Magistrate Judge Westmore held that it was both an abuse of power to do so and that it was unconstitutional to do so, and the fact that the Government may never be able to access the complete contents of a digital device otherwise did not affect the analysis.

Accordingly, Magistrate Judge Westmore denied the Government's warrant application and held that the Government may not compel or otherwise utilize fingers, thumbs, facial recognition, optical/iris, or any other biometric feature to unlock electronic devices. Instead, the Government could only seize those digital devices that law enforcement reasonably believed are owned and/or possessed by the two suspects named in the affidavit.