Mobile Devices and the Fifth Amendment

By Jaret Langston, Dale W. Callahan, and Joseph Popinski –ISSA Fellow, North Alabama Chapter

The authors review relevant court cases concerning searches of mobile devices, the basis of their rulings, and how multi-factor authentication implementations that employ a knowledge-based factor would provide Fifth Amendment protections with the security of multi-factor authentication and ease of use of biometrics.

Abstract

Multi-factor authentication (MFA) provides additional security to protect data and systems from theft and cyber attack. While this is accurate, MFA can have a privacy impact on mobile devices because of the Fifth Amendment and law enforcement searches. Mobile devices protected by biometrics alone are not covered by Fifth Amendment protections (with a few court case exceptions). Knowledge-based authentication factors, such as passwords and pin codes, are considered testimony and covered by the Fifth Amendment, as held in several court cases. In "Smartphones Need Two-Factor," the authors confirmed that data stored on smartphones warrants the use of MFA to unlock smartphones [1]. In this article we review relevant court cases concerning searches of mobile devices, the basis of their rulings, and how MFA implementations, like Facial Recognition with Image Signaling (FRIS), that employ a knowledge-based factor would provide Fifth Amendment protections with the security of MFA and ease of use of biometrics.

The US Constitution restricts the actions of the US government and protects the rights of its citizens, and the 5th Amendment to the Constitution protects one from self-incrimination. As technology advances, the application of laws evolves to address the new technologies. The advancement of mobile computing resulted in mobile phones containing more detailed personal information about the owner than anyone ever envisioned.

This advancement complicates the searching of mobile devices by law enforcement since it is almost impossible to gather just the needed evidence without exposing copious amounts of personal information unrelated to the case. Herein we examine several court cases where precedent has been set and continues to evolve for approved and denied search requests of mobile devices and how multi-factor authentication (MFA) can affect them.

Authentication factors

To understand the court case positions, one must understand authentication and authentication factors. Authentication is the process of verifying someone is who he or she claims to be. In this process, the person in question provides a piece of information that, when compared to a known good value, will either confirm the claim or prove it false. The authentication information provided by the claimant is an authentication factor. There are three types of authentication factors: something you know (knowledge based, i.e., passcode, pin code, password), something you are (biometrics, i.e., fingerprint, face, voice), and something you have (possession based,

i.e., ATM card, ID badge). In this article, we are looking at knowledge- and biometric-based authentication factors.

Legal precedence

Court cases have been decided and set precedence for 5th Amendment legal protections provided to knowledge- and biometric-based authentication factors. To protect an action with the 5th Amendment as self-incrimination, the action must constitute some form of testimony. In order to be "testimonial," an accused's oral or written communication or act must itself, explicitly or implicitly, relate a factual assertion or disclose information [2].

Pass codes and passwords

Court cases consistently find pass codes and passwords do require mental effort and are testimonial in nature. This protects them under the 5th Amendment. In *Doe v. United States*, the United States Supreme Court found that forcing the defendant to recall a combination to a wall safe would be testimonial and a violation of the 5th Amendment [2][3].

In *Commonwealth v. Baust* the court stated that when a phone is locked with a PIN code or password, the subject could not be compelled to reveal the PIN/password even if the state had a warrant to search the phone [4]. The US District Court for the District of Columbia determined a passcode produced would be the product of one's mind and is testimonial [3].

The foregone conclusion doctrine is an exception used to coerce the production of pass codes and passwords. In 2016 a Florida district court applied it and indicated the state did not have to establish possession, authenticity, or location of the phone to force the suspect to produce his passcode. The state simply had to show that the phone could be associated with the suspect [5]. This is in contradiction to a strict application of the doctrine as seen in *Matter of Residence in Oakland, California* [6].

Biometrics

The use of biometrics to unlock smartphones is not seemingly settled like the use of passcodes when it comes to 5th Amendment protections. There are cases where it has been allowed and denied, each presenting compelling arguments for the decisions. In "Cell Phones and the 5th Amendment Right against Self-incrimination," Michelle Nunes states that in cases of biometrics used to unlock phones, the main question to ask is does the act require a testimonial communication [3. Several cases found using biometrics is not an act requiring testimonial communication.

In 2018, the United States District Court for the District of Columbia held that producing a fingerprint to unlock a phone does not require mental effort and because of that it does not violate the 5th Amendment protections [3][7]. In *State v. Diamond*, the Minnesota Supreme Court ruled that providing biometrics to unlock a phone is not testimonial communication and therefore not a 5th Amendment violation [8]. And in *Commonwealth v. Baust*, the court held that using a fingerprint to unlock a phone does not require any mental process and is non-testimonial [4]. The court in *Florida v. Stahl* (2016) determined having an iPhone unlocked with a fingerprint was not a protected act [5]. Dritz concludes the ruling in *State v. Diamond* left Minnesota residents vulnerable to mobile phone searches unless they disable biometric authentication and used PIN or Password authentication [9].

Other cases resulted in just the opposite. In *Matter of Residence in Oakland, California*, the court denied the government request to use biometrics to unlock a phone, and in the process noted several reasons. The court states that submitting a fingerprint as physical evidence is not the same as sub-

mitting a fingerprint to unlock a phone. They conclude the biometric feature is used the same way as a passcode to lock the phone and the two are therefore equivalent. If they are equivalent and a person cannot be forced to reveal a passcode, then she cannot be forced to unlock the phone with biometrics [6]. The court also states that unlocking the phone via biometrics indicates it belongs to the individual or at least had some control over the phone. The act of unlocking it via biometrics then is testifying about ownership and/or control of the phone. In *Schmerber v. California*, the court noted physiological responses used in a polygraph exam are considered testimony and would violate the 5th Amendment [10]. And in *Matter of Residence in Oakland, California*, the court stated that biometric features are analogous to the physiological responses used in a polygraph exam and therefore would violate the 5th Amendment [6].

The forgone conclusion doctrine can require subjects to divulge certain information that might otherwise be covered by the 5th Amendment. In *Matter of Residence in Oakland, California*, the government requested to access smart phones found during a premises search by having all persons present during the search attempt to unlock them with biometrics [6]. The forgone conclusion doctrine states that surrendering materials that could incriminate oneself is not the same as testimony that could incriminate oneself [11]. However, the government must show prior knowledge of the materials' content and specific location. If this cannot be done, then the forgone conclusion doctrine cannot be used to compel one to unlock the phone with biometrics or passcodes [6]. Here the court determined the doctrine did not apply and denied the request.

These contradictory rulings on biometrics will eventually result in a Supreme Court case as pass codes and passwords have already done.

New authentication process

Currently, mobile devices have few options for multi-factor authentication to unlock them. Self-contained options are biometric (finger print, voice recognition, facial recognition) and pass code (password/pin). These utilize knowledge-based and biometric-based factors. Non-self-contained options could be an external device detected by near frequency communication (NFC) or connected by Bluetooth, combined with biometric or pass code. These would utilize either a something-you-have factor and a biometric factor or a something-you-have factor and a something-you-know factor.

These options require users to carry additional equipment and/or take multiple actions for authentication. The Facial Recognition with Image Signaling (FRIS) process utilizes a biometric factor (facial recognition) and a something you know factor [12]. With FRIS the something-you-know factor is an object the user identified during the registration process for the mobile device. When the user registered her face for authentication, she also held an object in the image frame and selected it on the screen as the secret object. The object chosen should be one the user normally has with her (a ring, watch, bracelet, etc.) When the user unlocks her mobile device, she holds the object where the mobile device camera can see her face and the object at the same time. Since this object is not designed to identify someone, and only the user knows it must be included for authentication, it is a knowledge-based factor. Using the FRIS process for authentication requires the user to execute a single action for unlocking the mobile device and does not require additional equipment [13].

Attorney opinion

Attorney R. Scott Estes, P.C., reviewed the existing authentication processes and the new FRIS process. He concurred the best option for smartphone 5th Amendment protections is using an authentication process that includes a knowledge-based factor like FRIS process [14].

Conclusion

Mobile devices contain more personal data about our lives than any other single tool we use. Multi-factor authentication is a better option for protecting access to these mobile devices than single-factor authentication commonly used today. Court cases have yielded mixed results for biometric authentication, while knowledge-based authentication has resulted in almost complete protection under the 5th Amendment. With this we conclude that implementing MFA for mobile devices that contain a knowledge-based factor, like FRIS, provides the best protection against self-incrimination under the 5th Amendment related to unlocking mobile devices for search and seizure.

References

1. Langston, J.A., Callahan, Dale W., Popinski, Joseph, "Smartphones Need Two-Factor," in *eForensics Magazine File System Forensics*. 2019. p. 19.
2. Doe v. United States, 487 U.S. 201 (1988). Justia Opinion Summary and Annotations [cited 2019 7/12/2019] – https://supreme.justia.com/cases/federal/us/487/201/.
3. Nunes, M., "Cell Phones and the 5th Amendment Right against Self-Incrimination," Campbell Law Observer. 2019, Campbell Law School.
4. Commonwealth v. Baust, in Va. Cir. 2014. p. 267.
5. State v. Stahl, in So. 3d. 2016, Fla: Dist. Court of Appeals, 2nd Dist. p. 124.
6. Matter of Residence in Oakland, California, in F. Supp. 3d. 2019, Dist. Court, ND California. p. 1010.

7. Matter of Search of [redacted] WA, DC, in F. Supp. 3d. 2018, Dist. Court, Dist. of Columbia. p. 523.
8. State v. Diamond, in NW 2d. 2018, Minn: Supreme Court. p. 870.
9. Dritz, J., "Unlocking Fifth Amendment Considerations in State v. Diamond," Minnesota Law Review, 2018. 102.
10. Schmerber v. California, in US. 1966, Supreme Court. p. 757.
11. In re Grand Jury Subpoena Duces Tecum, in F. 3d. 2012, Court of Appeals, 11th Circuit. p. 1335.
12. Langston, J.A. "Smartphones and 2FA" in Proceedings of the Alabama Cyber Now Conference. 2019. Birmingham, AL.
13. Langston, J.A., Callahan, Dale W., Popinski, Joseph, "Facial Recognition with Image Signaling: Process and Design." Not Yet Published, 2019.
14. R. Scott Estes, P.C., "FRIS Process Review," J. Langston, Editor. 2019.
15. Fifth Amendment. [cited 2019 July 12, 2019] – https://www.law.cornell.edu/constitution/fifth_amendment.
16. Boyd v. United States, in US. 1886, Supreme Court. p. 616.
17. US v. Kirschner, in F. Supp. 2d. 2010, Dist. Court, ED Michigan. p. 665.
18. Keidi Kuffel, K.R. "Face ID is Unavailable. Try Again Later— Can Law Enforcement Force a Suspect to Unlock Their Phone by Face ID or Fingerprint?" Cyberspace Law Committee Newsletter, 2019. February 2019.
19. LLP, R.S., "Recent Rulings Indicate Fifth Amendment May Join Fourth Amendment as Critical Consideration in Courts' Efforts to Apply Constitutional Protections to Smartphones and Other New Technology," in Lexology. 2019.

About the Authors

Jaret A. Langston, MsEng., is a credentialed course instructor at The University of Alabama at Birmingham. He is an Interdisciplinary Engineering PhD candidate with the UAB School of Engineering. His research interests are systems security, applied machine learning, and data science. He can be reached at jlangsto@uab.edu.

Dale W. Callahan, PhD, is the Associate Dean at The University of Alabama Birmingham, with the UAB School of Engineering. He served as Associate Editor of IEEE Transactions on Education from 2006 to 2008. Contact him at dcallahan@uab.edu.

Joseph Popinski, PhD, retired, is an ad hoc faculty member at the University of Alabama in Birmingham in the School of Engineering. He currently supports several professional organizations and can be reached at jpopinski3@aol.com.