IN THE COURT OF COMMON PLEAS, UNION COUNTY, OHIO
CRIMINAL DIVISION

STATE OF OHIO,

Plaintiff,

-vs-

Case No. «Case_Number»
Judge «Judge_Informal_Name»

«Defendant_Informal_Name»
Defendant

MOTION TO COMPEL
ELECTRONIC DEVICE PASSCODE

Now comes the State of Ohio and moves the court for an order compelling the production of a passcode necessary to unlock a digital device seized by the State under a Warrant to Search issued by this court on <<date of warrant>>.

A. A Search Warrant Was Issued Authorizing the Search and Seizure of an Electronic Device from the Defendant.

On <<date of warrant>> this court authorized the State of Ohio to both seize and search a smartphone from the defendant. (Ex. 1). This court recognized the probability of incriminating information being on the digital device and ordered its seizure. A search of digital information associated with a mobile device supported by probable cause is considered "reasonable" under the Fourth Amendment to the U.S. Constitution. *Riley v. California*, 573 U.S. 373,134 S.Ct. 2473 (2014); *Carpenter v. United States*, 585 U.S., 138 S.Ct. 2206 (2018); *State v. Smith*, 124 Ohio St. 3d. 163, 2009-Ohio-6426 (2009).

On <<date of seizure>> the State of Ohio executed the search warrant and seized a <<describe phone>> from the defendant <<defendant's name>>. The State has attempted to forensically examine the device but is prevented from doing so by the necessity of entering a password to the device. The device encrypts data, and the phone cannot be examined without a passcode or biometric data.[1] The defendant has declined to provide the passcode to law enforcement, though he admits knowing the passcode.

B. The Device Cannot be Searched Without the Passcode or Biometric Data

Obtaining a warrant to search a smartphone or other electronic device does not guarantee that law enforcement can access the device's data. Such devices encrypt their data and manufactures of these devices design them so it thwarts law enforcement's efforts to retrieve cell phone data. Apple and Google, which make the software in nearly all of the world's smartphones, encrypted their mobile software by default in 2014. Encryption scrambles data to make it unreadable until accessed with a special key, often a password.[2]

As reflected in the attached affidavit, law enforcement has attempted to gain access to the stored information using available forensic technology but cannot do so without the passcode. A passcode data is needed to access the device to execute the search warrant.

C. The Compelled Production of the Passcode or Use of Biometric Data to Unlock the Phone Does Not Violate the Fifth Amendment.

[1] For all devices running iOS 8.0 and later versions, Apple is unable to perform an iOS device data extraction as the data typically sought by law enforcement is encrypted, and Apple does not possess the encryption key. All iPhone 6 and later device models are manufactured running iOS 8.0 or a later version of iOS. www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf (Accessed June 29, 2020).

[2] Nicas, J. (June 13, 2018), Apple to Close iPhone Security Hole That Law Enforcement Uses to Crack Devices. New York Times. https://www.nvtimes.com/2018/06/13/technology/apple-iphone-police.html (Accessed June 29, 2020).

The State seeks compel the production of information on the digital device, information which this court has ruled the State may have access The password, in and of itself, is not incriminating. The only fact that could be established by the compelled production of the passwords that the defendant knows it and can access the phone. The State is already in possession of this information.

U.S. Const. amend. V does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication incriminating. For the Fifth Amendment privilege against compelled self-incrimination to apply, what the government is must (among other things) be considered "testimonial," meaning that the compelled must use 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact." *Curico v. United States*, 354 U.S. 118, 77 S.Ct. 1145 (9157). Generally the government may not compel a criminal suspect to make an incriminating communication.

The privilege does not, however, ordinarily "protect a suspect from being compelled . . . to produce 'real or physical evidence.'" *Pennsylvania v. Muniz*, 496 U.S. 582. For example, the government may force a suspect to give a blood sample or a handwriting exemplar, stand in a lineup, or even provide a voice exemplar, because, although these acts can furnish incriminating information, they do not require the suspect to "disclose any knowledge he might have" or "speak his guilt." To be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself. *Doe v. United States*, 487 U.S. 201, 210 (1988).

"The only fact conveyed by compelling a defendant to enter the password to an encrypted electronic device is that the defendant knows the password and can therefore access the device," *Commonwealth v. Jones*, 481 Mass. 540 (2018) (The superior court abused its discretion in

denying the Commonwealth's renewed motion to compel defendant to decrypt his cell phone because the Commonwealth proved that defendant knew the password beyond a reasonable doubt for the foregone conclusion exception to apply; Defendant's knowledge of the password was a foregone conclusion and not subject to the protections of the Fifth Amendment and art. 12 because his possession of the phone at the time of his arrest, his prior statement to police characterizing the phone's number as his number, and the phone's subscriber information proved beyond a reasonable doubt he knew the password.").

What the government must establish to overcome a Fifth Amendment objection is merely "that the suspect's knowledge of the passcode is a foregone conclusion, not that the contents of the device are a foregone conclusion." *Id*.

The Fifth Amendment privilege does shield documents from being disclosed pursuant to compulsion, even if their contents are incriminating. *United States v. Hubbell*, 530 U.S. 27, 35-36 (2000). This is because "the creation of those documents was not 'compelled' within the meaning of the privilege." *Id*.

D. The 'Foregone Conclusion' Doctrine is Applicable Here; The State Can Establish Beyond a Reasonable Doubt that the Suspect Knows the Passcode and Can Access the Phone.

The foregone conclusion doctrine teaches that when the testimonial aspect of a compelled act "adds little or nothing to the sum total of the Government's information," any implied testimony is a "foregone conclusion" and compelling it does not violate the Fifth Amendment. *Fisher v. United States*, 425 U.S. 391 (1976). Here the State can establish that the accused knows the password. As set out in the attached affidavit, the defendant has admitted:

1. The cellular telephone is his, and;
2. That he regularly uses the cellphone, and;

3. That he knows the passcode to the cellular telephone, and;

4. «Other facts»

In *Commonwealth v. Gelfgatt*, 468 Mass. 512, 514-15 (2014) the court noted, on the day of his arrest, investigators seized several encrypted devices from his home and interviewed the defendant, who asserted that he could decrypt them. Id. at 516-17. The defendant's act of entering the passwords would be a testimonial act of production, because it would implicitly acknowledge his "ownership and control of the computers and their contents." Id. at 522. But, the court continued, the defendant had acknowledged as much in his statement to the police; thus, any facts implied by his entering the passwords were foregone conclusions. Id. at 523-24. In doing so, the court commented that the "foregone conclusion" exception would apply where law enforcement already knew "(1) the existence of the evidence demanded; (2) the possession or control of that evidence by the defendant; and (3) the authenticity of the evidence." *Id.* at 522 (citing *Fisher*, 425 U.S. at 410-13).

A New Jersey appellate division court addressed this issue, concluding as follows under the facts of the case:

"However, by producing the passcodes, [the] defendant is not implicitly conveying any information the State does not already possess. Defendant is not telling the government something it does not already know. Therefore, the implicit facts conveyed by the act of producing the passcodes is a 'foregone conclusion' and compelled disclosure of the passcodes does not violate defendant's Fifth Amendment right against self-incrimination."

See, *In re M.W.*, 5th Dist. Licking No. 2018 CA 0021, 2018-Ohio-5227, citing *State v. Andrews*, 197 A.3d 200, 457 N.J. Super. 14, 2018 N.J. Super. LEXIS 159, 2018 WL 5985982 (Nov. 15, 2018), at 5.

E. Conclusion

"[T]he public ... has a right to every [person's] evidence.' *United States v. Nixon*, 418 U.S. 683, 709-710 (1974) (quoting *Branzburg v. Hayes*, 408 U.S. 665, 688 (1972)). Under the federal and Ohio constitutions, the privilege generally protects individuals only from having to make statements or perform acts that are compelled, incriminating and testimonial.

Where the only fact that a suspect would implicitly be asserting is '"a foregone conclusion," such that the suspect "adds little or nothing to the sum total of the State's information by conceding it. Under these circumstances the statement loses its testimonial nature and "no constitutional rights are touched. The question is not of testimony but of surrender." *In re Harris*, 221 U.S. 274, 279 (1911); *Fisher v. United States*, 425 U.S. 391, 411, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976).

Wherefore, the State of Ohio respectfully requests this Court issue an Order compelling the production of the passcode for the electronic device.

Respectfully submitted,

DAVID W. PHILLIPS
UNION COUNTY PROSECUTING ATTORNEY

_____

By: «First_Chair_Informal_Name»
(«First_Chair_Attorney_Number»)
249 West Fifth Street
Marysville, Ohio 43040
(937) 645-4190
(937) 645-4191

CERTIFICATE OF SERVICE