Filed: 2/27/2019 11:06 AM

IN THE
INDIANA SUPREME COURT

No. 18S-CR-595

KATELIN EUNJOO SEO, *Appellant-Defendant*, v. STATE OF INDIANA, *Appellee-Plaintiff*.	Appeal from the Hamilton Superior Court, No. 29D01-1708-MC-5640, The Honorable Steven R. Nation, Judge.

STATE'S RESPONSE TO BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION OF INDIANA

CURTIS T. HILL, JR.
Attorney General
Attorney No. 13999-20

ELLEN H. MEILAENDER
Deputy Attorney General
Attorney No. 22468-64

OFFICE OF THE ATTORNEY GENERAL
Indiana Government Center South
302 West Washington Street, Fifth Floor
Indianapolis, Indiana 46204-2770
317-233-3548 (telephone)
Ellen.Meilaender@atg.in.gov

Attorneys for Appellee

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

ARGUMENT

An order to unlock a cell phone compels no testimonial assertion about the contents of the phone and does not violate the Fifth Amendment where the person's knowledge of the passcode is a foregone conclusion.

Defendant has not been compelled to disclose or reveal the contents of her mind; she was ordered to perform the act of unlocking her phone, not to disclose her password to the government orally or in writing. And Amici erroneously oversimply Fifth Amendment jurisprudence in suggesting that any "use" of the mind in the compelled performance of an act of production always constitutes a Fifth Amendment violation (Amici Br. at 9-11).[1] A person must use his mind in order to provide a handwriting exemplar, but this act is not protected by the Fifth Amendment. *See Gilbert v. California*, 388 U.S. 263, 266-67 (1967). Any act of producing documents in compliance with a subpoena would require the use of one's mind, but it does not violate the Fifth Amendment when the foregone conclusion doctrine is satisfied. *Fisher v. United States*, 425 U.S. 391, 410-11 (1976); *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1345-46 (11th Cir. 2012). Even the classic example of compelled behavior that does not implicate the Fifth Amendment—being forced to surrender the key to a strongbox—requires the person to use his mind. He must recollect or remember where he has stored or hidden the key in order to retrieve it and use it to unlock the strongbox.

[1] The State notes that Amici do not make any argument that it would implicate the Fifth Amendment to require a person to unlock a device by means of biometric measures, which involve only the display of a physical feature, such as a fingerprint or a face.

In the context of compelled acts of production, the Fifth Amendment analysis does not turn on whether some minimal use of the mind is involved but rather on whether, and what, factual assertions the person has been required to communicate by performing the act.[2] *See also State v. Diamond*, 905 N.W.2d 870, 877 n.8 (Minn. 2018) (stating that "the focus of the inquiry is not only whether the content comes from the mind, but also whether the content from the mind has 'testimonial significance'") (citing *Doe v. United States*, 487 U.S. 201, 211 n.10 (1988) ("In order to be privileged, it is not enough that the compelled communication is sought for its content. The content itself must have testimonial significance.")).

Defendant has been ordered to do the functional equivalent of providing her key to unlock a container so that the police may execute their search warrant. She has not been required to show the police where the evidence they seek is located nor has she been required to make any explicit or implicit factual assertions regarding anything the police may find inside that container. *See Doe*, 487 U.S. at 214-16 (compelling a person to sign a consent form authorizing a bank to release information was not testimonial because it did not make any admissions regarding anything the bank might release nor did it show the government where the evidence they sought was located). In *United States v. Green*, 272 F.3d 748, 753 (5th

[2] Even outside the context of compelled acts of production, it is an oversimplification of Fifth Amendment law to assert that any compelled use of the mind or compelled disclosure of potentially-incriminating information automatically runs afoul of the Fifth Amendment. For example, individuals may be compelled to stop and report to law enforcement, providing statutorily-required information, when they are involved in a personal injury or property damage accident. *California v. Byers*, 402 U.S. 424, 427-34 (1971).

Cir. 2001), relied on by Amici, the defendant was compelled to disclose the locations of his gun cases to law enforcement, not just to unlock the cases. Similarly, in *Curcio*, the government was seeking to compel the defendant to disclose the location of the evidence the government was seeking. *Curcio v. United States*, 354 U.S. 118, 118-19, 125 (1957). Defendant has not been compelled to show or tell the police where on her phone the evidence they seek may be found. Her mind has not been co-opted to perform the government's investigation for it; she has simply been compelled to provide the key to unlock the premises so that the government may carry out its investigation on its own.

This compelled act of production receives Fifth Amendment protection only to the extent that the act itself implicitly conveys a factual assertion that is not a foregone conclusion. *Fisher*, 425 U.S. at 410-11; *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 612-15 (Mass. 2014). And the implicit factual assertion in this case is not the password itself (which is Defendant's asserted "contents of the mind") but the knowledge of the password. The Fifth Amendment is implicated not because Defendant is compelled to remember her password but because she is compelled to implicitly assert that she knows the password, which implicitly admits that she owns or has the capability to use the phone.

The State has never suggested that the foregone conclusion doctrine has any applicability outside the context of compelled acts of production. The State agrees that a defendant could not be compelled to admit his guilt even if the State had evidence definitively proving he committed the crime, nor could he be compelled to

tell the police where the murder weapon was located even if it was a foregone conclusion that he was the murderer. But it does not follow from that premise that the foregone conclusion doctrine has no applicability outside the specific facts of *Fisher* or even that it is applicable only to the production of business or financial records. The foregone conclusion doctrine, which is part of the act of production doctrine, is the appropriate legal framework under which to consider the Fifth Amendment issue raised in this case.

The Supreme Court has never limited the foregone conclusion doctrine to only the production of business or financial records (Amici Br. at 12-16).[3] Amici do not provide any theoretical reason or argument to explain why the doctrine must be limited to business and financial records. And, in fact, courts around the country have understood the foregone conclusion analysis to be the appropriate legal doctrine to apply when deciding whether a person may be compelled to disclose a

[3] Amici advance this argument for the first time. Defendant did not argue that the foregone conclusion doctrine was wholly inapplicable to this case before the trial court, in her Brief of Appellant filed in the Court of Appeals, or in any response to the State's transfer petition.

password or unlock a device.[4] Those that have ruled against the government have generally done so because they concluded the government had not or could not satisfy the doctrine and establish the requisite foregone conclusion, not because they held that the doctrine was not the correct legal doctrine under which to consider the issue.[5] *See In re Grand Jury Subpoena*, 670 F.3d at 1345-49; *SEC v. Huang*, 2015 WL 5611644, at *3-4 (E.D. Pa. Sept. 23, 2015); *G.A.Q.L. v. State*, 257 So. 3d 1058, 1063-65 (Fla. Dist. Ct. App. 2018).

Finally, Amici argue that to satisfy the foregone conclusion doctrine, the State must identify with reasonable particularity the specific items stored on the device, but this argument is premised on a doctrinal error (Amici Br. at 17-22). It is the implicit testimonial assertion inherent in the compelled act that must be the foregone conclusion, not the evidence that the State is searching for pursuant to the

---

[4] *See, e.g.*, *United States v. Apple MacPro Computer*, 851 F.3d 238, 246-48 (3rd Cir. 2017), *cert. denied*; *In re Grand Jury Subpoena*, 670 F.3d at 1342-49; *In re Search of a Residence in Aptos, California*, 2018 WL 1400401, at *5-12 (N.D. Cal. March 20, 2018); *United States v. Spencer*, 2018 WL 1964588, at *1-4 (N.D. Cal. March 20, 2018); *United States v. Friscosu*, 841 F. Supp. 2d 1232, 1236-37 (D. Colo. 2012); *SEC v. Huang*, 2015 WL 5611644, at *3-4 (E.D. Pa. Sept. 23, 2015); *In re Grand Jury Subpoena to Sebastian Boucher* (*Boucher II*), 2009 WL 424718, at *2-4 (D. Vermont Feb. 19, 2009); *G.A.Q.L. v. State*, 257 So. 3d 1058, 1063-65 (Fla. Dist. Ct. App. 2018); *State v. Stahl*, 206 So. 3d 124, 132-37 (Fla. Dist. Ct. App. 2016); *Gelfgatt*, 11 N.E.3d at 612-16; *In re Grand Jury Investigation*, 88 N.E.3d 1178, 1180-82 (Mass. App. Ct. 2017); *State v. Andrews*, 197 A.3d 200, 204-09 (N.J. Super. Ct. App. Div. 2018); *Commonwealth v. Davis*, 176 A.3d 869, 874-76 (Pa. Super. Ct. 2017).

[5] The district court decision in *Kirschner* is simply silent with respect to the foregone conclusion doctrine. It does not contain any foregone conclusion analysis, but it also does not contain any assertion or analysis affirmatively rejecting the applicability of the doctrine to this context. *United States v. Kirschner*, 823 F. Supp. 2d 665, 668-69 (E.D. Mich. 2010).

warrant. Amici never explain how the act of unlocking a device makes any testimonial assertion about the evidence existing on the phone.

The fact that the material on the phone is the object of the search, the thing that the State is ultimately seeking, does not make the material on the phone the object of the Fifth Amendment's foregone conclusion inquiry. The materials existing on Defendant's phone are not protected by the Fifth Amendment—everything existing on the phone was created voluntarily by Defendant without any government compulsion.[6] *See Hubbell v. United States*, 530 U.S. 27, 35-36 (2000); *United States v. Doe*, 465 U.S. 605, 610-12 & n.10 (1984); *see also Andresen v. Maryland*, 427 U.S. 463, 471-77 (1976) (no Fifth Amendment privilege attaches to voluntarily-created private papers). Even if those materials contain incriminating testimonial statements, the government did not compel Defendant to write or say or do those things. Thus, Amici are wrong to assert that "digital devices" have "Fifth Amendment protection" that would be extinguished (Amici Br. at 8). The Fifth Amendment does not protect digital devices, just as it does not protect homes or automobiles; it protects people from being compelled to make incriminating testimonial statements. The substance of the material on the phone becomes

[6] Notably, Amici make no effort to support or defend Judge Mathias' idiosyncratic view that documents cease to exist when they are encrypted and are therefore created anew through decryption. It was by viewing the compelled decryption as the compelled creation of the material itself on the phone that Judge Mathias could view the material on the phone as the testimony Defendant was being compelled to make.

relevant to a Fifth Amendment inquiry only if Defendant is being compelled to make any testimonial assertion about the substance of that material.

When a defendant produces documents in response to a subpoena, he is making testimonial assertions about the existence and substance of those documents; that is why, in that context, the existence and substance of the documents must be a foregone conclusion. For example, if the State ordered Defendant to produce copies of all the text messages she sent to D.S. in 2017, the act of complying with that order would inherently admit both that she sent text messages to D.S. during that time frame and that the documents she produced constituted the specific messages that she sent. Those facts would therefore need to be a foregone conclusion before the State could compel her to implicitly admit them.

But the order in this case does not compel Defendant to locate and produce any specific documents for the State. It only requires her to unlock her phone, *i.e.*, to produce the key, so that the State may conduct its judicially-authorized search. Complying with that order does not compel Defendant to make any testimonial assertions regarding the contents of the phone. Admitting that she knows the password to the phone, *i.e.*, admitting that she possesses the key to the phone, does not implicitly admit that there are any text messages to D.S. on the phone or that she is the person who sent any such messages that might be found there. Defendant is not being required to admit her guilt by affirming the authenticity of anything found on the phone. Therefore, the contents of the phone do not need to be a foregone conclusion; the State does not need to identify with particularity what it

believes exists on the phone in order to avoid a Fifth Amendment problem.[7] The only implicit factual assertion she makes by complying with this order is that she knows the password, and, by extension, that she owns or has the capability to use the phone. Thus, what the State must identify with particularity is Defendant's knowledge of the password and use of the phone. That is the object of the foregone conclusion inquiry because that is the only thing that falls within the ambit of the Fifth Amendment privilege under this factual scenario.

* * *

The rule sought by the State is narrow and limited (Amici Br. at 8, 22). The Fourth Amendment protects people's significant privacy rights in the contents of their phones or computers from unwarranted government intrusion, and it will continue to do so if the State prevails in this case. The State's ability to compel a person to unlock her device comes into play only after the Fourth Amendment's requirements have been satisfied and the State has established a legal right to view the contents of the device. And even then, it is not true that every password-protected device becomes subject to compelled unlocking. It is only if the State can prove that it already knows and can independently establish a specific person's connection to a specific device that the foregone conclusion doctrine would permit

[7] Of course, under the Fourth Amendment, a valid search warrant must describe with sufficient specificity the evidence that that is sought. *See Figert v. State*, 686 N.E.2d 827, 829-30 (Ind. 1997) (stating that a warrant is facially valid when it describes "with sufficient particularity" the "things to be seized" and the places to be searched). Thus, the State cannot obtain a search warrant unless it can assert with sufficient specificity what evidence it has probable cause to believe exists in the location to be searched.

the State to compel that person to use his password to unlock that device. To fall outside the protection of the Fifth Amendment privilege, it is not enough for the State to show that the existence of a password is a foregone conclusion; it is the specific individual's knowledge of the password/ability to unlock the phone that must be the foregone conclusion.

Where advancing technology has skewed the careful balancing of individual's privacy interests and society's effective law enforcement interests to the detriment of the individual, the Supreme Court has modified Fourth Amendment doctrine so that people's privacy interests continue to receive robust protection and the equilibrium is restored. *See, e.g.*, *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014). But in this context, it is the State, not the individual, who has been placed at the mercy of advancing technology. *See* Brief of Amicus Curiae States at 19-23.[8] Even when the careful Fourth Amendment balancing has concluded that the individual's privacy interests must give way, modern technology allows the individual to unilaterally thwart the weighty societal interest merely because he now stores materials in digital form on a password-protected computer or phone rather than in physical form in a locked file cabinet or desk drawer. The limited application of the foregone conclusion doctrine at issue here does nothing more than prevent new technology from converting the Fifth Amendment into a trump card over the Fourth Amendment.

[8] And this has serious consequences for the ability to investigate and prosecute crimes, particularly crimes in which digital evidence on phones or computers is pervasive and critical, such as possession of child pornography.

CONCLUSION

This Court should hold that the order to unlock the cell phone does not violate the Fifth Amendment under the foregone conclusion doctrine.

Respectfully submitted,

CURTIS T. HILL, JR.
Attorney General
Attorney No. 13999-20

By: /s/ Ellen H. Meilaender
Ellen H. Meilaender
Deputy Attorney General
Attorney No. 22468-64

OFFICE OF THE ATTORNEY GENERAL
Indiana Government Center South
302 West Washington Street, Fifth Floor
Indianapolis, Indiana 46204-2770
317-233-3548 (telephone)
Ellen.Meilaender@atg.in.gov

Attorneys for Appellee

CERTIFICATE OF WORD COUNT

I verify that this brief, as governed by Indiana Appellate Rule 44(C), contains no more than 4,200 words, according to the word count function of the Microsoft Word word-processing program used to prepare it.

/s/ Ellen H. Meilaender
Ellen H. Meilaender

CERTIFICATE OF SERVICE

I certify that on February 27, 2019, the foregoing document was electronically filed using the Indiana E-filing System ("IEFS"). I further certify that on February 27, 2019, the foregoing was served upon opposing and amicus counsel, via IEFS, addressed as follows:

William J. Webster
courts@webstergarino.com

Carla V. Garino
courts@webstergarino.com

Kenneth J. Falk
kfalk@aclu-in.org

Kevin S. Smith
ksmith@cchalaw.com

/s/ Ellen H. Meilaender
Ellen H. Meilaender