No. 127968

IN THE
SUPREME COURT OF ILLINOIS

PEOPLE OF THE STATE OF ILLINOIS, Plaintiff-Appellee, v. KEIRON K. SNEED, Defendant-Appellant.	))))))))))	On Appeal from the Appellate Court of Illinois, Fourth Judicial District, No. 4-21-0180 There on Appeal from the the Circuit Court of the Sixth Judicial Circuit, DeWitt County, Illinois, No. 21 CF 13 The Honorable Karle E. Koritz, Judge Presiding.

BRIEF OF PLAINTIFF-APPELLEE PEOPLE OF THE STATE OF ILLINOIS

KWAME RAOUL
Attorney General of Illinois

JANE ELINOR NOTZ
Solicitor General

KATHERINE M. DOERSCH
Criminal Appeals Division Chief

JOSHUA M. SCHNEIDER
Assistant Attorney General
100 West Randolph Street, 12th Floor
Chicago, Illinois 60601-3218
(773) 590-7123
eserve.criminalappeals@ilag.gov

Counsel for Plaintiff-Appellee
People of the State of Illinois

ORAL ARGUMENT REQUESTED

E-FILED
11/29/2022 8:18 AM
CYNTHIA A. GRANT
SUPREME COURT CLERK

TABLE OF CONTENTS

Page(s)

POINTS AND AUTHORITIES

NATURE OF THE ACTION

In February 2021, defendant was charged with forgery. C5.[1] Police obtained a warrant to search defendant's cell phone for evidence of that offense, Sec. C3, then moved to compel him to enter the phone's passcode so that they could execute the warrant, C12-18. After the trial court denied the motion to compel, R45, the People filed a certificate of impairment, C31, and appealed, C33. The Illinois Appellate Court reversed the trial court's order, A30, ¶ 108, and defendant now appeals from that judgment. No question is raised on the charging instrument.

ISSUES PRESENTED FOR REVIEW

1. Whether the order denying the People's motion to compel defendant to enter the phone's passcode so that police could search the phone was appealable under Illinois Supreme Court Rule 604(a)(1) because it had the substantive effect of quashing the warrant and suppressing any evidence contained on the phone, and the People certified that it impaired their case.

2. Whether compelling defendant to enter the phone's passcode comports with the Fifth Amendment because entering the passcode implicitly admits only to his ability to access the phone, which is a foregone conclusion where he already identified the phone as his.

---

[1] Citations to the common law record appear as "C__," to the report of proceedings as "R__," to defendant's brief as "Def. Br. __," and to defendant's appendix as "A__." Citations to the four-page secured record appear as "Sec. C__," with page numbers referring to the pages in the order that they appear.

JURISDICTION

On March 30, 2022, this Court allowed defendant's petition for leave to appeal. Accordingly, this Court has jurisdiction under Supreme Court Rules 315 and 612(b).

STATEMENT OF FACTS

In February 2021, defendant and his wife, Allora Spurling Sneed (Spurling), R6, were charged with forging two Dairy Queen paychecks, C5-7. Police arrested them pursuant to arrest warrants, R8-9; C10, and seized one cell phone from each of them, R9-10; Sec. C1. When defendant and Spurling were later released on bond, defendant provided a phone number on the bond sheet that matched the number for the phone that police had seized from him during arrest. R9; C11. Defendant later provided the same phone number on a sworn affidavit of assets and liabilities that he filed to obtain appointed counsel. *Compare* C11, *with* C20.

The next month, Clinton Police Detective Todd Ummel filed a sworn complaint for a search warrant to search defendant's and Spurling's phones, which police still possessed, for evidence of the forgery and transmission of Dairy Queen paychecks. Sec. C1. According to the complaint, in January 2021, the bookkeeper for the Dairy Queen in Clinton, Illinois, contacted the Clinton Police Department. *Id.* She had discovered a paycheck made out to defendant, who did not work at Dairy Queen but whose wife, Spurling, did. *Id.* The paycheck had been cashed using mobile deposit, which allows checks

to be deposited using a cell phone. *Id.* The bookkeeper texted Spurling about the forged paycheck, and Spurling claimed that she "didn't know anything about it" and "guess[ed] it wasn't meant to happen for real." *Id.* Spurling continued that defendant "didn't think it would actually work because it wasn't real." *Id.* She claimed that "[h]e never got the money" and "d[id]n't have a card for that bank or anything," and asked whether "there [was] any way to call the bank and get the money back cuz [*sic*] he didn't get it." *Id.*

Ummel scheduled an interview with Spurling, but she did not appear. Sec. C2. She claimed that she missed the interview because she had been exposed to COVID-19, and they rescheduled. *Id.* Spurling did not appear for the rescheduled interview either, and further attempts to contact her were unsuccessful. *Id.* A few weeks later, the Dairy Queen bookkeeper discovered a second forged paycheck that was made payable to defendant and cashed via mobile deposit. *Id.* Ummel then sought to search defendant's cell phone for evidence that he had used the phone to deposit the forged paychecks, such as photographs of the paychecks, messages communicated through the phone's text messaging application or other messaging applications like Facebook or WhatsApp, emails, and mobile application notifications. *Id.* The trial court found probable cause to believe that such evidence was on defendant's phone and issued the search warrant on March 1, 2021. Sec. C3.

When police discovered that defendant's phone was passcode-protected, R7-8; C12-13, the People moved to compel defendant to "provide the passcode

or enter the passcode to his phone seized by Clinton Police," C19; *see* C12-19. The motion alleged that defendant could be so compelled because the testimony implicit in the act of producing or entering the passcode was already a foregone conclusion, and thus not privileged under the Fifth Amendment. C13-17, 19.

At the hearing on the motion, Ummel testified to the facts that were provided in the sworn complaint for the warrant, *see* R4-6, of which the trial court took judicial notice, R17, and further testified that both forged paychecks made out to defendant and deposited using a mobile device had been endorsed using defendant's name, R6-7. Ummel noted that the phone number that defendant had provided on the bond sheet matched the number of the phone seized from him during arrest, R9, and testified that police had been unable to access the phone because it was protected by a passcode that defendant refused to provide, R7-8. The Clinton Police Department did not have the ability to bypass the phone's passcode-protection. R8. Ummel was not aware of any outside agency that would assist in decrypting the phone; he explained that although the Illinois State Police (ISP) sometimes assisted with such matters, they usually would not assist unless the case involved narcotics. *Id.* Ummel was cautious about simply entering possible passcodes into the phone because too many failed attempts might result in permanently locking the device. *Id.*

Defendant cross-examined Ummel about his knowledge of the contents of the locked phone and Ummel's attempts to obtain evidence of the crimes from other sources. R10-12. Ummel did not know for certain that the evidence identified in the warrant would be found on the phone. R11. He had not yet compared the signatures on the backs of the endorsed checks to defendant's signature, and he had not subpoenaed the bank in which the paychecks were deposited for related bank records or defendant's cell phone carrier for copies of his text messages. R10-12.

The trial court denied the motion to compel. R45. The court applied the "foregone conclusion" test, under which "production of incriminating testimonial evidence" may be compelled if "the existence, possession, and authenticity of the evidence is a foregone conclusion that adds little or nothing to the sum total of the State's information." R40. The court found that that the act of producing defendant's password is testimonial because it would admit "that the phone belonged to the defendant and that he was capable of accessing it." R39. The court further found that this "implied statement of fact communicated by disclosure of the pass code provides no further evidence than already exists" because "the phone was found on the [d]efendant" and he "listed the phone number associated with the phone as his own phone number on the bond sheet." *Id.* But, the court explained, it was bound by *People v. Spicer*, 2019 IL App (3d) 170814, which held that the focus of the foregone conclusion test when considering compelled production

of a phone's passcode is "on the information the pass code protects, which, in this case, would be the contents of the cell phone." R40-41. The court suggested that "perhaps the better-reasoned argument" is that the foregone conclusion test should focus on the passcode being produced, R41, but followed *Spicer* to hold that the People had failed to satisfy the foregone conclusion test by showing that the existence, possession, and authenticity of the files contained on the phone were a foregone conclusion, R44-45.

The People filed a certificate of substantial impairment, asserting that the trial court's order "substantially impairs the People's ability to prosecute this cause" because it "prevents [them] from acquiring evidence pursuant to a search warrant," and therefore had the substantive effect of quashing the search warrant and suppressing evidence. C31. The People then filed a notice of appeal. C33.

The appellate court reversed. A4-5, ¶ 2. The court first held that it had jurisdiction under Supreme Court Rule 604(a)(1) because the order denying the motion to compel defendant to enter the phone's passcode had the substantive effect of suppressing the evidence contained on the phone. A10-11, ¶¶ 32-34. The appellate court then held that "requiring defendant to provide entry or the passcode to the phone does not compel him to provide testimony within the meaning of the [F]ifth [A]mendment" because there was no dispute that the phone was his. A19-20, ¶¶ 61, 63. And even if it did compel testimony, defendant could be compelled to enter the passcode under

the foregone conclusion test because the existence of the passcode, defendant's possession of the passcode, and authenticity of the passcode were all foregone conclusions. A29-30, ¶¶ 98-102.

STANDARDS OF REVIEW

Whether the appellate court had jurisdiction under Supreme Court Rule 604(a)(1) is a question of law that this Court reviews de novo, as is any question regarding the proper interpretation of the rule. *People v. Salem*, 2016 IL 118693, ¶ 11.

Whether compelling defendant to enter a phone's passcode into the phone comports with the Fifth Amendment is a question of law that this Court reviews de novo. *In re A.W.*, 231 Ill. 2d 92, 106 (2008) (standard for reviewing alleged violations of Fifth Amendment right is de novo). Factual findings made by the trial court in the course of analyzing defendant's Fifth Amendment challenge will be reversed only if they are against the manifest weight of the evidence. *People v. Salamon*, 2022 IL 125722, ¶ 75.

ARGUMENT

I. The Order Denying the People's Motion to Compel Defendant to Unlock His Phone Was Appealable Under Rule 604(a)(1).

The People may appeal from an order that has the "substantive effect" of "quashing an arrest or search warrant" or "suppressing evidence." Ill. S. Ct. R. 604(a)(1). The order denying the People's motion to compel defendant to enter the passcode into the phone that police seized from him so that police could execute the warrant to search the phone was appealable under Rule

604(a)(1) because it had the substantive effect of quashing the search warrant. Although that alone sufficed to render the order appealable, the order was also appealable because it had the effect of suppressing any evidence contained on the phone.

A. The order had the substantive effect of quashing the warrant to search the phone seized from defendant.

The order had the substantive effect of quashing the warrant to search the phone because it prevented police from executing the warrant — that is, from conducting the search authorized by the warrant. *Cf. People v. York*, 29 Ill. 2d 68, 72 (1963) ("The purpose of the [search] warrant is to authorize the officer to conduct the search[.]"); *People v. Carter*, 2016 IL App (3d) 140958, ¶ 27 (search warrant is executed when search is conducted). Therefore, it was appealable by the plain terms of Rule 604(a)(1).

The People moved to compel defendant to "enter the passcode to his phone seized by Clinton Police," C19; *see* C12, because the phone was "protected by pass[code], preventing law enforcement from searching [it] pursuant to the issued search warrant," C12-13. Ummel testified that the phone was passcode-protected, and that Clinton Police were unable to bypass that passcode-protection. R7-8. Nor was Ummel aware of any outside assistance that they could enlist to bypass the protection; the ISP, the outside agency that sometimes assisted with bypassing passcode-protection, assisted only in narcotics cases. R8. Without the technological capabilities necessary to bypass the passcode-protection, the only avenue left was blindly

attempting to guess the passcode through trial and error, which risked locking the phone permanently if police did not get lucky within an unknown but limited number of attempts. *Id.*[2] Because the record establishes that police could execute the search warrant only if defendant entered the phone's passcode, which he refused to do voluntarily, the order denying the motion to compel him to enter the passcode prevented the execution of the warrant.

It is true that the order did not also "prevent the State from pursuing other avenues to obtain the evidence it sought," Def. Br. 11, but the option of pursuing an investigation through means other than the execution of a particular search warrant is irrelevant to whether an order denying a motion to compel has the substantive effect of quashing the warrant. Otherwise, even an order that explicitly quashes a search warrant would not have the substantive effect of quashing the warrant because it would not prevent police from pursuing their investigation in other ways.

Similarly irrelevant is the trial court's "acknowledg[ment] [of] the continued validity of the search warrant" that its order prevented police from executing. Def. Br. 11. Appealability under Rule 604(a)(1) is contingent on an order's "substantive effect." *See People v. Keith*, 148 Ill. 2d 32, 39 (1992)

---

[2] For example, if the phone has a six-digit passcode, Ummel's first guess would have a one-in-a-million chance of succeeding. *See* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L. Rev. 989, 1000 (April 2018). If his first guess was wrong, he could have as few as nine more chances to guess correctly before the phone's contents become permanently inaccessible. *See id.* (current iPhones have feature that permanently erases phone's contents after ten failed attempts to enter passcode).

("[T]he substantive effect of the court's order, not the label of the motion, controls appealability under Rule 604(a)(1)."). Although defendant characterizes the order as "limit[ing] only the *means* by which the State could pursue the search warrant," Def. Br. 10 (emphasis in original), the order excluded the only means by which Clinton Police could execute the search warrant: compelling defendant to enter the phone's passcode.

Defendant relies on *In re K.E.F.*, 235 Ill. 2d 530 (2009), and *People v. Lee*, 2020 IL App (5th) 180570, but those cases did not deal with search warrants. Rather, they addressed the admissibility of evidence that prosecutors had already obtained. *See K.E.F.*, 235 Ill. 2d at 539; *Lee*, 2020 IL App (5th) 180570, ¶¶ 5-6. Under Rule 604(a)(1), it is enough that the order here had the substantive effect of quashing a warrant, and these cases are inapposite.

In any event, even under the logic of those cases, the order here was appealable. In *K.E.F.* and *Lee*, the prosecution argued that evidentiary rulings had the effect of suppressing evidence, but courts found that the rulings barred the prosecution only from presenting evidence about the charged offenses through its preferred means but left other, equally viable means available. In *K.E.F.*, the prosecution sought to present the victim's prior statements about the respondent's offenses but, "for reasons that quite frankly def[ied] comprehension," refused to even attempt to lay the foundation necessary to do so. 235 Ill. 2d at 539. Similarly, under the order

at issue in *Lee*, the prosecution was prevented from presenting information about the charged sexual offenses through the three victims' prior statements, 2020 IL App (5th) 180570, ¶¶ 5-6, but was free to present that same information through their live testimony, which the prosecution conceded it could do if it wished, *id.* ¶ 9. Because "admissibility of the evidence in question was a matter entirely within the State's control," the orders in *K.E.F.* and *Lee* excluding the prior statements for lack of foundation did not have the effect of suppressing evidence. *K.E.F.*, 234 Ill. 2d at 540; *see Lee*, 2020 IL App (5th) 180570, ¶ 14 ("[W]hile the recorded statements could possibly be more compelling than [the victims'] in-court testimony, they are not the only means available to the State to present the relevant information to the jury.").

K.E.F. and *Lee* are inapposite because, unless defendant is compelled to enter his password, the People do not have any means of accessing the evidence contained on defendant's phone. Thus, unlike in those cases, the execution of the search warrant here cannot be deemed "a matter entirely within the State's control." *K.E.F.*, 234 Ill. 2d at 540. If Clinton Police had the ability to bypass the phone's passcode-protection but refused to do so, then the trial court's refusal to compel defendant to enter the passcode would merely limit the means by which they could execute the warrant. But Clinton Police *cannot* execute the warrant unless defendant enters the passcode, which he has refused to do. Therefore, the order denying the

motion to compel defendant to enter the phone's passcode had the substantive effect of quashing the warrant. *See People v. Hollingsworth*, 2022 IL App (4th) 190329-U, ¶ 28 (order denying motion to compel entry of phone's passcode had substantive effect of quashing warrant to search phone's contents).[3]

B. The order also had the substantive effect of suppressing any evidence contained on the phone.

The order also had the substantive effect of suppressing evidence because it prevented information accessible only through the phone from being presented at trial. *See People v. Drum*, 194 Ill. 2d 485, 492 (2000) (order has substantive effect of suppressing evidence if it "prevents [the] information from being presented to the fact finder"). Clinton Police established probable cause to search the phone for a variety of evidence related to defendant's deposit of fraudulent checks, such as photographs of the paychecks reflecting that they were taken by the phone's camera and messages communicated through the phone's text messaging application or other messaging applications like Facebook or WhatsApp that might be stored only on the phone. Sec. C3. Accordingly, the order preventing police from searching the phone and discovering that evidence necessarily prevents the prosecution from presenting that evidence at trial. *See Hollingsworth*, 2022 IL App (4th) 190329-U, ¶ 27 (order denying motion to compel defendant

[3] A copy of this nonprecedential order is available at https://tinyurl.com/2m6ajhcp. *See* Ill. S. Ct. R. 23(e)(1).

to unlock phone had substantive effect of suppressing evidence contained on phone because it prevented execution of search warrant and therefore discovery of evidence on phone); *see also People v. Smith*, 399 Ill. App. 3d 534, 536-38 (3d Dist. 2010) (order quashing subpoena duces tecum to police department for "any and all statements" made by defendant police officers during internal investigation had substantive effect of suppressing those statements).

C. The certificate of impairment conclusively establishes impairment to the People's case.

To appeal from an order that has one of the requisite substantive effects under Rule 604(a)(1), the People must certify that the order substantially impairs their ability to prosecute the case. *People v. Young*, 82 Ill. 2d 234, 247 (1980). But the certification requirement creates no independent grounds for jurisdictional challenges. *Id.* ("Our intention in requiring this certification is not to formulate a standard by which courts may determine the appealability of a particular order."). Rather, it directs the People to consider the prosecutorial necessity of seeking review of an interlocutory order. *See id.* at 247-48. Accordingly, the Court "rel[ies] solely upon the good-faith evaluation by the prosecutor of the impact of the [appealable] order in his case." *Id.* at 247. Courts thus have consistently rejected defendants' attempts to challenge the validity of a certificate of substantial impairment. *See Keith*, 148 Ill. 2d at 39-40 (rejecting defendant's jurisdictional challenge that prosecution was insufficiently impaired by

otherwise appealable interlocutory order); *People v. Turner*, 367 Ill. App. 3d 490, 495-96 (2d Dist. 2006) (same); *People v. Jackson*, 269 Ill. App. 3d 851, 854 (1st Dist. 1995) (same); *People v. Davis*, 117 Ill. App. 3d 98, 99 (4th Dist. 1983) (same).

After the trial court denied the motion to compel, the prosecutor evaluated the effect of that order on his ability to prosecute the case and filed a certificate asserting that the order "substantially impairs the People's ability to prosecute this cause" because it "prevents [them] from acquiring evidence pursuant to a search warrant," and therefore has the substantive effect of quashing the search warrant and suppressing evidence. C31. Defendant's disagreement with the prosecutor's evaluation of the challenged order's effect on the People's case presents no valid jurisdictional challenge.

II. Compelling Defendant to Enter the Passcode to Unlock His Cell Phone Comports with the Fifth Amendment Under the Foregone Conclusion Test.

The appellate court correctly held that defendant may be compelled to enter the passcode to the phone seized from him during arrest. Although the act of entering the passcode will implicitly admit that the passcode exists, that defendant possesses it, and that the passcode is authentic (in the sense that it is the passcode that unlocks the phone), those facts are already a foregone conclusion in this case and therefore insufficiently testimonial to be privileged under the test used to evaluate Fifth Amendment challenges.

The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const., amend. V.;

see Ill. Const. 1970, art. I, § 10 ("No person shall be compelled in a criminal case to give evidence against himself[.]"). Although the Fifth Amendment and the Illinois Constitution are not phrased identically, with the former describing the privilege against self-incrimination as a protection against "be[ing] a witness against [one]self" and the latter as a protection against "giv[ing] evidence against [one]self," this Court has held that "[t]he two provisions differ in semantics rather than in substance." *People ex rel. Hanrahan v. Power*, 54 Ill. 2d 154, 160 (1973). "There is nothing in the proceedings of the constitutional convention to indicate an intention to provide, in article I, section 10, protections against self-incrimination broader than those of the Constitution of the United States." *People v. Rolfingsmeyer*, 101 Ill. 2d 137, 142 (1984). To the contrary, those proceedings "reflect[ ] a general recognition and acceptance of the interpretations by the United States Supreme Court" and an intent "that the existing state of the law would remain unchanged," *id.* (internal quotation marks omitted), with "the existing state of the law at that time [being] lockstep of identical or nearly identical language," *People v. Caballes*, 221 Ill. 2d 282, 293-94 (2006). Accordingly, to the extent defendant asks this Court to interpret the Illinois provision as "applying more expansively" than the federal provision, Def. Br. 19, he has failed to provide "the substantial grounds necessary for this court to depart from the federal interpretation of the self-incrimination clause." *Relsolelo v. Fisk*, 198 Ill. 2d 142, 150 (2001) ("virtually identical" self-

incrimination clauses are to be interpreted in lockstep absent substantial grounds to depart from federal interpretation).

The Fifth Amendment privilege against compelled self-incrimination "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* that is incriminating." *Fisher v. United States*, 425 U.S. 391, 408 (1976) (emphasis added); *see Hiibel v. Sixth Judicial Dist. Ct.*, 542 U.S. 177, 189 (2004) ("To qualify for the Fifth Amendment privilege, a communication must be testimonial, incriminating, and compelled."). If an act is not "sufficiently testimonial for purposes of the privilege," then a person may be compelled to perform that act. *Fisher*, 425 U.S. at 411-12.

Accordingly, the first step in determining whether defendant may be compelled to enter the phone's passcode is to determine whether that act is testimonial at all, such that it would implicate the Fifth Amendment privilege. If the act of entering the passcode is testimonial, then the next step is to determine whether the testimony implicit in the act is a "foregone conclusion," meaning that it "adds little or nothing to the sum total of the Government's information" and therefore is insufficiently testimonial to be privileged. *Id.*

A. The compelled act of entering a phone's passcode implicates the Fifth Amendment privilege because its performance implicitly asserts facts about the passcode.

An act is "testimonial" if it "relates either express or implied assertions of fact or belief." *United States v. Hubbell*, 530 U.S. 27, 35 (2000). If the act of entering a phone's passcode does not "'speak [one's] guilt'" in this way, then it is not testimonial and no further analysis is required, *Doe v. United States* (*Doe II*), 487 U.S. 201, 210-11 (1988) (quoting *United States v. Wade*, 388 U.S. 218, 222-23 (1967)), for it is "the attempt to force [the accused] 'to disclose the contents of his own mind' that implicates the Self-Incrimination Clause," *id.* (quoting *Curcio v. United States*, 354 U.S. 118, 128 (1957)) (internal citation omitted).

The question whether an act is testimonial "do[es] not lend [itself] to categorical answers," but "depend[s] on the facts and circumstances" of the case. *Fisher*, 425 U.S. at 410. Generally, acts of exhibiting physical characteristics of one's body for examination, such as by submitting to fingerprinting, photography, or measurements, are not testimonial because "[t]he act of exhibiting such characteristics is not the same as a sworn communication by a witness that relates either express or implied assertions of fact or belief." *Hubbell*, 530 U.S. at 35; *Wade*, 388 U.S. at 222-23 ("compulsion of the accused to exhibit his physical characteristics" is "not compulsion to disclose any knowledge he might have"). In contrast, "[t]here are very few instances in which a verbal statement, either oral or written, will not convey information or assert facts." *Doe II*, 487 U.S. at 213. "The

vast majority of verbal statements thus will be testimonial and, to that extent at least, will fall within the privilege." *Id.* at 213-14.

All other acts — that is, acts that produce evidence other than nontestimonial physical characteristics or testimonial verbal statements — are testimonial only to the extent that performing them "implicitly communicate[s] statements of fact." *Hubbell*, 530 U.S. at 36 (internal quotation marks omitted). When determining whether a compelled act is testimonial, the proper focus is on the factual assertions implicit in the performance of the act itself, not the contents of any evidence that the act produces. *See id.* at 40 ("The 'compelled testimony' that is relevant in this case is not to be found in the contents of the documents produced in response to the subpoena. It is, rather, the testimony inherent in the act of producing those documents."); *Fisher*, 425 U.S. at 409-10 (focusing on "communicative aspects" of "[t]he act of producing evidence . . . wholly aside from the contents of the [evidence] produced"); *see also In re Grand Jury Subpoena Duces Tecum No. 00114*, 164 Ill. App. 3d 344, 353 (2d Dist. 1987) (recognizing that *Fisher* and *United States v. Doe (Doe I)*, 465 U.S. 605 (1984), "shifted the emphasis from the contents of the [evidence produced] to the testimonial act of production").

Applying this analysis, the United States Supreme Court concluded that the "testimonial aspect" of a compelled act that produces evidence "does nothing more than establish the existence, authenticity, and custody of the

items that are produced." *Hubbell*, 530 U.S. at 40-41. In other words, when a person complies with an order to produce evidence, he implicitly asserts three facts: (1) the evidence he was ordered to produce exists, (2) he possesses or controls that evidence, and (3) the evidence he produced is authentic, meaning it is the evidence that he was ordered to produce. *See Fisher*, 425 U.S. at 410; *Doe II*, 487 U.S. at 209. Those three facts are implicitly asserted because they are the facts that must be true for the person to have performed the act as ordered. *See* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767, 779 (2019) ("A person can be successfully ordered to do only what he has sufficient knowledge to do."). A person cannot have produced the ordered evidence unless that evidence exists. Nor can a person have produced the ordered evidence unless he possesses or controls it. And a person cannot have produced the ordered evidence unless the evidence he produced is actually the evidence he was ordered to produce. Although other facts may be inferred from the act of producing the ordered evidence — for example, that the person possessed the evidence at a particular time in the past or obtained it from a particular person or in a particular way — those facts are not implicitly asserted through the performance of the act because they are not necessary prerequisites for the act to be performed. Such facts might be true or they might not; the performance of the act itself provides no guarantee.

1. Entering a phone's passcode is testimonial because it implicitly admits to knowledge of the phone's passcode.

When a person performs the act of entering a passcode into a phone, thereby unlocking it, he implicitly admits that he knows the passcode to unlock the phone. *See Commonwealth v. Jones*, 117 N.E.3d 702, 710 (Mass. 2019) ("In the context of compelled decryption, 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."); *Spicer*, 2019 IL App (3d) 170814, ¶¶ 19, 21 ("forcing a person to reveal a passcode results in implied factual statements" by requiring person "to use his mind and demonstrate . . . that he could access his phone" (internal quotation marks omitted)); *G.A.Q.L. v. State*, 257 So. 3d 1058, 1062 (Fla. Dist. Ct. App. 2018) ("The very act of revealing a password asserts a fact: that the defendant knows the password."); *United States v. Apple Mac Pro Computer*, 851 F.3d 238, 428 n.7 (3d Cir. 2017) ("[T]he fact . . . that is implicit in the act of providing the password for the devices is 'I, John Doe, know the password for these devices.'"); *see also* Kerr, *supra*, at 779 ("Entering a password is testimonial because it communicates a simple statement: 'I know the password.'").[4]

[4] Although the appellate court held that "requiring defendant to provide entry or the passcode to the phone does not compel him to provide testimony within the meaning of the [F]ifth [A]mendment," A20, ¶ 63, its reasoning appears to have been that the act was *insufficiently* testimonial (as the People argue here), for the court distinguished the act of entering a passcode from the act of producing hundreds of documents based on the extent that the

Consistent with *Fisher*, *Doe I*, and *Hubbell*, courts have articulated this admission that a person knows a phone's passcode as three component factual assertions: (1) the passcode exists, (2) the person who entered the passcode possesses the passcode, and (3) the passcode that the person entered is authentic (meaning that it is the passcode that unlocks the phone). *See State v. Andrews*, 234 A.3d 1254, 1274 (N.J. 2020) (act of producing passcodes to unlock phones entails admissions of "the passcodes' existence, possession, and authentication"); *State v. Johnson*, 576 S.W.3d 205, 225-226 (Mo. Ct. App. 2019) (act of producing passcode admits "the existence of the passcode, its possession or control by [the person producing it], and the passcode's authenticity"); *State v. Stahl*, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016) (act of producing passcode to phone implicitly admits "that the *passcode* exists, is within the accused's possession or control, and is authentic" (emphasis in original)); *see also Reynolds v. State*, 516 P.3d 249, 254 (Okla. Crim. App. 2022) (production of password to DVR system implicitly admits existence, possession, and authenticity of password); *Commonwealth v. Davis*, 220 A.3d 534, 555 (Pa. 2019) (Baer, J., dissenting) (entering password

---

two acts requires a person to disclose his knowledge of facts unknown to the government, *see* A19-20, ¶¶ 59, 61 (relying on *United States Oloyede*, 933 F.3d 202, 309 (4th Cir. 2019), for proposition that suspect may be compelled to enter passcode without disclosing it where "no dispute exists that the suspect owns the phone"). In other words, although the appellate court purported to first hold that entry of a passcode is nontestimonial and then hold in the alternative that it is permissible under the foregone conclusion test, its rationale for holding that entry of a passcode is nontestimonial is consistent with that of the foregone conclusion test. *See infra* § II.B.

into computer implicitly admits "that the password exists, that [the person] has possession and control of the password, and that the password is authentic, as it will decrypt the encrypted computer files"). Thus articulated, the testimonial aspects of a compelled act of producing a passcode can be analyzed like the testimonial aspects of a compelled act to produce anything else.[5]

2. Contrary to defendant's argument, entering a phone's passcode does not admit anything about the phone's contents.

Although the act of entering a phone's passcode is testimonial, it is not testimonial to the extent that defendant asserts. One might infer a variety of

[5] The one distinction between the act of producing a passcode and the act of producing a document arises when a person produces a passcode by disclosing its substance rather than entering it. This is the distinction that *Hubbell* drew between "surrender[ing] the key to a strongbox" and "telling an inquisitor the combination to a wall safe." 530 U.S. at 43. When a person produces a key to a locked box, he admits that the key exists, that he possesses it, and that the key he produced is the key that unlocks the box. Similarly, when a person is compelled to produce a passcode by entering it, he asserts that the passcode exists, he possesses it, and that the passcode he entered is the passcode that unlocks the device. *See* R39. In contrast, the act of producing a passcode by disclosing it to police, rather than by entering it, is analogous to telling police the combination to a locked box; by telling police the combination, a person tells them not only that the combination exists, he possesses it, and the combination is authentic, which all may have been foregone conclusions, but the actual digits making up the combination, which were not. Because the People's motion to compel sought an order that defendant either enter the passcode or produce it to police, compliance with that order would not require that defendant disclose the passcode and the Court need not resolve whether revealing a passcode is sufficiently testimonial to be privileged where entering the passcode would not be. Accordingly, for the purposes of this brief, the People's discussion of the act of producing a passcode refers to the act of producing a passcode by entering it into an encrypted device, rather than by disclosing it.

facts other than the existence, possession, and authenticity of a phone's passcode from a person's entry of that passcode — that the phone is registered in the person's name, the person used the phone to make certain phone calls or send certain text messages, or the person knows what files are stored on the phone — but none of those facts *must* be true for the person to have entered the passcode and therefore none is impliedly asserted by the mere act of entering the passcode. *See* Kerr, *supra*, at 779 (author who knows passcode to his sister's phone but "ha[s] no idea what files might be stored [there]" could be compelled to enter phone's passcode, but doing so would admit only that he knew that phone's passcode, not that he knew what files lay beyond it). Thus, providing a passcode is not "testimonial" on the ground that it communicates such information.

Defendant thus errs in relying on *Seo v. State*, 148 N.E.3d 952 (Ind. 2020), to argue that the act of entering a phone's passcode admits something about the phone's contents, Def. Br. 24, 35, because *Seo* conflated entering a phone's passcode with producing files from the phone. *Seo* considered a suspect's challenge to an order compelling her to "unlock" her phone, which police had seized, so that police could search the phone's contents. 148 N.E.3d at 954. But when *Seo* considered the facts implicitly asserted by the act of entering the passcode, the court incorrectly failed to focus its analysis on that act. *See supra* p. 18. Instead, *Seo* built a chain of analogies that led it to analyze the testimonial implications of a different act entirely: the act of

producing files from the phone. First, *Seo* recharacterized the act of entering a phone's passcode as "the act of producing an unlocked smartphone." *Id.* at 957. *Seo* then drew an analogy to the act of producing physical documents, analogized physical documents to electronic files, and concluded that the act of entering a passcode into a phone is the same as the act of producing files from a locked phone. *Id.* Accordingly, *Seo* held, compelling a suspect to enter a phone's passcode "communicates to the State, at a minimum, that (1) the suspect knows the password; (2) the files on the device exist; and (3) the suspect possesses those files." *Id.*

Seo's holding regarding the testimony implicit in the act of entering a phone's passcode is incorrect because *Seo* analyzed the testimonial implications of the wrong act. The root of *Seo*'s error lies in its initial recharacterization of the act of entering a passcode into a phone already possessed by police (which the suspect had been ordered to perform) as an act of producing an unlocked phone to police (which she had not).[6] Producing an unlocked phone to police cannot be characterized as entering a passcode into

---

[6] *Seo*'s conclusion would be wrong even if this recharacterization was valid, for producing an unlocked phone would not admit that "the files on the device exist" and "the suspect possesses those files." 148 N.E.3d at 957. If one accepts the analogy that *Seo* drew between the act of producing an unlocked phone and the act of producing documents, *see id.* — that is, if one conducts the analysis by substituting an unlocked phone for documents — then the act of producing an unlocked smartphone admits nothing about the phone's contents, just as the act of producing documents admits nothing about the documents' contents. *See Hubbell*, 530 U.S. at 40 (testimony relevant to act of producing documents "is not to be found in the contents of the documents produced" but "in the act of producing those documents").

a phone that is already in the possession of police. Producing an unlocked phone to police admits to the existence, possession, and authenticity of the phone that the person was ordered to produce, *see Hubbell*, 530 U.S. at 40-41, whereas entering a passcode into a phone that police already possess admits only to the person's knowledge of the phone's passcode, *see supra* § II.A.1.

The error in *Seo*'s conclusion that entering a phone's passcode implicitly admits that "the files on the device exist" and "the suspect possesses those files," 148 N.E.3d at 957, becomes clear once focus is returned to the compelled act at issue. Entering a phone's passcode cannot admit that "the files" exist because the act is not dependent on the existence of files; a person who knows a phone's passcode can enter it whether the phone contains lots of files, the particular files police think it contains, or no files at all. Similarly, a person can enter a phone's passcode without possessing any of the files contained on the phone or even being aware that such files exist. *See* Kerr, *supra*, at 779.

At bottom, a phone is a container. Entering the passcode does nothing more than open the container. And the testimony implicit in producing *access to* a container and the testimony implicit in producing *contents of* a container are distinct. Suppose that police obtain a warrant to search a suspect's home for drugs but cannot execute the warrant because he lives in an impregnable bunker. If they obtain an order compelling the suspect to unlock the steel door to his bunker, then his compliance with that order will

implicitly admit that the key exists, he possesses it, and he used it to unlock the door. But unlocking the door will *not* admit that there are drugs in the bunker. If police instead obtain an order compelling the suspect to produce the drugs they believe are hidden inside his locked bunker, then his compliance with *that* order will admit not only that the key to the bunker exists, he possesses it, and he used it to unlock the bunker, but that the *drugs* exist and the suspect possesses *them*. An order to unlock a phone by entering its passcode is equivalent to the first order to unlock a door by using its key; compliance says nothing what may lie beyond the barrier.

In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012), confirms this distinction between the testimony implicit in unlocking a device and the testimony implicit in producing the contents of a locked device. In that case, the accused was ordered to produce the "unencrypted contents" of hard drives and "any and all containers or folders thereon." *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1339. The Eleventh Circuit focused on the testimony inherent in the act of producing hidden files, *id.* at 1342, and concluded that complying with the order to decrypt and produce files not only would admit the accused's ability to access the encrypted portions of the drives — that is, to unlock the door to the bunker — but also "would be tantamount to testimony by [the accused] of his knowledge of the existence and location of potentially incriminating files" and "of his possession, control, and access to"

those files. *Id.* at 1346. In other words, because the government demanded the production of files, compliance would implicitly admit the existence, possession, and authenticity of any files produced. *Id.*

Applying this same analysis, when the government demands the production of a passcode, compliance will implicitly admit the existence, possession, and authenticity of the passcode produced. *See supra* § II.A.1. But producing a passcode by entering it into a phone does not admit the existence, possession, and authenticity of any files that might be stored on the phone because the act of entering a phone's passcode produces no files. Only the act of producing files from the locked phone would implicitly testify to the existence, possession, and authenticity of such files. Thus, although the act of entering a phone's passcode is testimonial, it is not testimonial to the extent that defendant asserts.

B. Compelling defendant to enter the phone's passcode is not sufficiently testimonial to be privileged because the facts that it would implicitly admit are foregone conclusions.

An act that is testimonial because it implicitly asserts certain facts is not "sufficiently testimonial for the purposes of the privilege" if those facts are a "foregone conclusion," such that the implicit factual assertions "add[ ] little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411-12. In such cases, "the Government is in no way relying on the 'truthtelling' of the [person compelled to act]" to establish the facts implicitly asserted by the act, and so the act does not "rise[ ] to the level of

testimony within the protection of the Fifth Amendment." *Id.* at 411 (quoting 8 J. Wigmore, Evidence § 2264, p. 380 (1961)).

Fisher and *Hubbell* illustrate the application of the foregone conclusion test. In both cases, the compelled act was the act of producing documents, *Fisher*, 425 U.S at 394; *Hubbell*, 530 U.S. at 31, which would have implicitly asserted that the documents existed, were possessed by the suspects, and were authentic, *Hubbell*, 530 U.S. at 36-37. In *Fisher*, the compelled act of producing certain tax documents was permissible because the existence, possession, and authenticity of those documents were a foregone conclusion; the government already knew that the documents existed and were in the suspects' possession, *Fisher*, 425 U.S. at 394, 411; *Hubbell*, 530 U.S. at 44, and could "independently confirm" the documents' authenticity after they were produced by consulting the accountants who created them, *Hubbell*, 530 U.S. at 44-45; *see Fisher*, 425 U.S. at 411-12. In contrast, in *Hubbell*, the compelled act of producing 11 broad categories of documents was impermissible because the government had no "prior knowledge of either the existence or whereabouts" of the documents, 530 U.S. at 45, but relied entirely on the assertions implicit in the suspect's act of production "to identify potential sources of information and to produce those sources," *id.* at 41. *Fisher* and *Hubbell* thus illustrate that a compelled act does not violate the Fifth Amendment if the government possesses independent knowledge of the assertions of fact implied by the performance of the act.

Defendant nevertheless argues that he cannot be compelled to enter the phone's passcode because phone passcodes, unlike other evidence, are absolutely privileged under the Fifth Amendment and therefore not subject to the foregone conclusion test. In the alternative, he argues that application of the foregone conclusion test to the compelled entry of a phone's passcode should focus on the contents of the phone being unlocked rather than the testimony implicit in the compelled act of unlocking the phone. But defendant is incorrect on both accounts. Phone passcodes are not uniquely privileged under the Fifth Amendment, and the foregone conclusion test focuses solely on the testimony implicit in the performance of a compelled act, not on the evidence that the act might subsequently allow police to discover.

1. Foregone conclusion analysis applies to the compelled entry of phone passcodes.

Defendant argues that the foregone conclusion test should not be "extended" to the compelled entry of phone passcodes because the production of passcodes is not like the production of documents to which the Supreme Court has "historically" applied the analysis. Def. Br. 25-26, 28. But passcodes have no characteristics requiring that they be uniquely privileged under the Fifth Amendment.

"While the Court in *Fisher* and *Doe* [*I*] did not purport to announce a universal test for determining the scope of privilege," it created the foregone conclusion test by "appl[ying] basic Fifth Amendment principles." *Doe II*, 487 U.S. at 209. Accordingly, the Supreme Court has repeatedly described the

foregone conclusion test in broad terms applicable to all compelled acts that produce evidence. *See Balt. City Dep't of Soc. Servs. v. Bouknight*, 493 U.S. 549, 555 (1990) ("[T]he act of complying with the government's demand testifies to the existence, possession, or authenticity of the *things* produced." (emphasis added)); *Hubbell*, 530 U.S. at 40-41 (response to compelled act of production "does nothing more than establish the existence, authenticity and custody of *items* that are produced" (emphasis added)). And the Supreme Court has recognized that the test may be applied to compelled acts beyond the production of documents. *See Bouknight*, 493 U.S. at 554-55 (holding that compelled production of child was not privileged because child's authenticity (*i.e.*, identity) could be confirmed independently of assertion of authenticity implicit in compelled act); *see also United States v. Patane*, 542 U.S. 630, 644 n.7 (2004) (noting that "there is a reasonable argument" under rationale of foregone conclusion test that defendant could have been compelled to produce handgun because he had already admitted to possessing it (citing, *inter alia*, *Hubbell* 53 U.S. at 42-45; *Bouknight*, 493 U.S. at 554-56; and *Fisher*, 425 U.S. 391, generally)).

Thus, nothing in the nature or history of the foregone conclusion test suggests that it does not apply to all compelled acts that produce evidence, including acts of producing passcodes. Accordingly, courts in Illinois and elsewhere have regularly evaluated Fifth Amendment challenges to the compelled production of passcodes by applying the foregone conclusion test.

See Hollingsworth, 2022 IL App (4th) 190329-U, ¶¶ 33-39; *Spicer*, 2019 IL App (3d) 170814, ¶¶ 15-23; *see also*, *e.g.*, *Reynolds*, 516 P.3d at 252-54; *Andrews*, 234 A.3d at 1273; *Seo*, 148 N.E.3d at 955; *Johnson*, 576 S.W.3d at 225-226; *Jones*, 117 N.E.3d at 709-10; *G.A.Q.L.*, 257 So. 3d at 1063; *Apple Mac Pro Computer*, 851 F.3d at 247; *United States v. Gavegnano*, 305 F. App'x 954, 956 (4th Cir. 2009).

One outlier, *Commonwealth v. Davis*, 220 A.3d 534 (Pa. 2019), held that the foregone conclusion test is inapplicable to the production of passcodes, but *Davis*'s reasoning is unsound. *Davis* reasoned that the cases in which the Supreme Court applied the test concerned production of "business or financial records," which *Davis* asserted are "a unique category of material" for Fifth Amendment purposes. *Id.* at 549. But *Davis* did not identify the unique characteristics of business or financial records that it believed render compelled acts of producing of such documents subject to less protection under the Fifth Amendment than compelled acts of producing other kinds of evidence. *See id.* And although *Davis* suggested that the foregone conclusion test does not apply to acts of producing passcodes because such acts reveal "information arrived at as a result of using one's mind," *id.* at 550, this suggestion rests on a fundamental misunderstanding of the test.

Contrary to the *Davis* court's suggestion, a person may be compelled to perform an act that implicitly admits to facts within the person's knowledge — or, as *Davis* put it, reveals "information arrived at as a result of using

one's mind," *id.* at 550 — so long as the facts to which the act implicitly admits are a foregone conclusion. *Fisher*, 425 U.S. at 411-12. Were the foregone conclusion test inapplicable whenever a compelled act revealed "information arrived at as a result of using one's mind," then *Fisher* would have disallowed the compelled production of tax documents at issue in that case, for the gathering and production of specific documents cannot be performed by unthinking physical reflex but instead requires the use of one's mind.

Nor is it significant, as defendant claims, that "[m]odern phones and computers contain an extraordinary amount of information" compared to physical documents. Def. Br. 28. For the purposes of the Fifth Amendment, a phone is simply a container and the passcode the key that unlocks it. *See supra* pp. 25-26. The testimony implicit in unlocking a container is the same whether the container is very small, holding only a few pages, or very large, holding an entire library: that the key exists, the person possesses it, and the person used it to unlock the container. *See Hubbell*, 530 U.S. at 40-41; *Fisher*, 425 U.S. at 410. If the Fifth Amendment privilege turned on the potential volume of incriminating evidence that would be exposed by a compelled act, then a person who filed simple tax returns and lived in a small apartment could be compelled to produce his tax documents for inspection and unlock his door to allow a search, but a person who filed voluminous tax returns and lived in a mansion could not. The Fifth Amendment's focus on a

compelled act's testimonial content rather than its evidentiary consequences prevents such absurd and unjust outcomes.

At bottom, defendant's concern that unlocking a phone so that police can execute a warrant to search its contents will provide "broad access to the phone in its entirety," Def. Br. 26 — that it will allow police to review too much private information — amounts to a challenge to the scope of the search authorized by the warrant as unreasonable under the Fourth Amendment. Unless the incriminating evidence in question is compelled testimony, "its protection stems from other sources — the Fourth Amendment's protection against seizures without warrant or probable cause and against subpoenas which suffer from too much indefiniteness or breadth in the things required to be particularly described." *Fisher*, 425 U.S. at 401 (internal quotation marks omitted). A suspect is free to move to quash the warrant under the Fourth Amendment if he believes it defective in these ways; defendant has not challenged the validity of the warrant to search the phone seized from him on any ground.

But "the Fifth Amendment protects against 'compelled self-incrimination, not [the disclosure of] private information,'" and does not "serve as a general protector of privacy — a word not mentioned in its text and a concept directly addressed in the Fourth Amendment." *Fisher*, 425 U.S. at 401 (quoting and altering *United States v. Nobles*, 422 U.S. 225, 233 n.7 (1975)). To the extent that the privilege against self-incrimination

"serves privacy interests," it does so only "[w]ithin the limits imposed by the language of the Fifth Amendment." *Id.* at 399. But "the [Supreme] Court has never on any ground, personal privacy included, applied the Fifth Amendment to prevent the otherwise proper acquisition or use of evidence which, in the Court's view, did not involve compelled testimonial self-incrimination of some sort." *Id.*; *see Doe I*, 465 U.S. at 618 (O'Connor, J., concurring) (writing separately to "make explicit what is implicit in the analysis of [the majority] opinion: that the Fifth Amendment provides absolutely no protection for the contents of private papers of any kind"). The Fifth Amendment privilege therefore does not shield incriminating evidence from discovery on the ground that the suspect stored it in some private place. *See Harris*, 221 U.S. at 279-80 ("The right not to be compelled to be a witness against oneself is not a right to appropriate property that might tell one's story."); *Reynolds*, 516 P.3d at 254 ("There is simply no right for one to construct impenetrable enclaves, whether concrete or digital, to evade a magistrate's finding of probable cause and order to seize evidence or contraband attendant to the enforcement of the law.").

Accordingly, defendant's reliance on *Carpenter v. United States*, 138 S. Ct. 2206 (2018), is misplaced. *Carpenter* considered the Fourth Amendment implications of a "new phenomenon" — "the ability to chronicle a person's past movements through the record of his cell phone signals" — and concluded that "an individual maintains a legitimate expectation of privacy

in the record of his physical movements as captured through [cell-site location information]." *Id.* at 2216-17. *Carpenter* cautioned against "uncritically extend[ing] existing precedents" to "new concerns wrought by digital technology," *id.* at 2222, but applied the usual Fourth Amendment analysis to cell-tower location information to determine whether it was subject to a reasonable expectation of privacy, *see id.* at 2217-19. *Carpenter*'s warning concerned applications of old precedent given that the Fourth Amendment protects expectations of privacy that change over time as societal expectations change with the advancement of technology. *See id.* at 2217; *see also*, *e.g.*, *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (applying usual Fourth Amendment test of "whether the individual has an expectation of privacy that society is prepared to recognize as reasonable" to use of thermal imaging to look through walls of homes).

In contrast, the Fifth Amendment takes no regard of changing standards of reasonableness, *see Fisher*, 425 U.S. at 400 ("[T]he Fifth Amendment's strictures, unlike the Fourth's, are not removed by showing reasonableness."), but focuses narrowly on whether a person will be compelled to provide testimony, *id.* at 408; *Hubbell*, 530 U.S. at 34. Because the act of unlocking a container implicitly makes the same testimonial statements whether the container holds physical documents or electronic files, the fact that technological advancements have increased the types and volume of material that may be stored inside a container, though significant

under the Fourth Amendment, *see Riley v. California*, 573 U.S. 373, 385-86 (2014), is irrelevant for Fifth Amendment purposes.

Finally, there is no merit to defendant's argument that the foregone conclusion test is "unworkable" as applied to the entry of a passcode. Def. Br. 26-27. Defendant notes that applying the foregone conclusion test to resolve whether a person may be compelled to enter a phone's passcode would not resolve whether the person could be compelled to unlock any passcode-protected applications subsequently discovered while searching the phone. *Id.* But answering that separate question simply requires applying the foregone conclusion test to the separate compelled act of unlocking the application to determine whether the facts implicit in that act — that the application's passcode exists, the person possesses it, and the person used it to unlock the application — are foregone conclusions. Similarly, the fact that a suspect may be compelled to unlock the door to a house that he shares with roommates because his ability to do so is a foregone conclusion does not answer the separate question of whether he may be compelled to unlock the door to any particular bedroom inside the house. Defendant's hypothetical does not identify a problem with applying the foregone conclusion test to entry of a phone's passcode, but illustrates the limited scope of access that any given application of the test allows.

2. A phone's contents are irrelevant to whether a person may be compelled to enter the phone's password under the foregone conclusion test.

A person may be compelled to perform an act as long as the facts implicitly asserted by performing the act are a foregone conclusion. *Fisher*, 425 U.S. at 411-12. As discussed, when a person enters a phone's passcode, the person implicitly asserts three facts: that the passcode exists, the person knows the passcode, and the passcode that the person entered is the passcode that unlocks the phone. *See supra* § II.A.1. Therefore, a person may be compelled to enter a phone's passcode as long as those three facts are a foregone conclusion. *See Andrews*, 234 A.3d at 1274; *Johnson*, 576 S.W.3d at 226; *Stahl*, 206 So. 3d at 136; *Reynolds*, 516 P.3d at 254; *see also Jones*, 117 N.E.3d at 711. Because entering a phone's passcode does not implicitly assert any facts about the phone's contents, *see supra* § II.A.2, no fact about those contents need be a foregone conclusion.

Defendant argues that analysis of the compelled entry of a phone's passcode under the foregone conclusion test should "focus on the evidence the State is seeking by unlocking the phone" because the government's reason for compelling the act is to provide access to files on the phone. Def. Br. 31 (citing *Spicer*, 2019 IL App (3d) 170814, ¶ 21). But the Fifth Amendment privilege protects people from being compelled to give incriminating testimony, regardless of the reasons for compulsion, and so the government's reason for compelling the performance is irrelevant to the testimony implicit in performing the act. For example, when the government obtained the order

to compel the suspects in *Fisher* to produce tax documents, presumably it was because the government sought incriminating information written in those documents. Yet *Fisher* nonetheless held that the suspects could be compelled to produce the documents because the facts implicitly asserted by doing so were a foregone conclusion, even though the contents of the documents might not be. 425 U.S. at 411-13. Thus, the fact that an order to compel the entry of a phone's passcode is motivated by the hope that it will provide access to incriminating evidence provides no reason to shift the focus of the foregone conclusion test from the testimony implicit in entering the passcode to the contents of the phone.

Nor would a proper application of the foregone conclusion test "'swallow the protections of the Fifth Amendment'" by "subject[ing] all passcode protected phones to compulsion purely on the fact they have a passcode." Def. Br. 29 (quoting *G.A.Q.L.*, 257 So. 3d at 1063). As an initial matter, this argument is factually incorrect; although the existence of a phone's passcode is a foregone conclusion whenever a phone requires a passcode to unlock it, *G.A.Q.L.*, 257 So. 3d at 1063, that foregone conclusion is insufficient to compel someone to enter a phone's passcode because the person's possession of the passcode and the passcode's authenticity must also be foregone conclusions. *See supra* § II.A.1. But the broader argument — that if people may be compelled to enter passcodes whenever the testimony implicit in doing so is a foregone conclusion, then people will be required to

enter passcodes too much — expresses a policy preference, not a constitutional basis to shift the focus of the foregone conclusion test from the testimony implicit in the compelled act.

For example, the fact that the existence of phone's passcode will always be a foregone conclusion if the phone is passcode-protected (and in that sense is "tautological," Def. Br. 29) does not suggest that the foregone conclusion test cannot apply as usual to phone passcodes, but instead suggests merely that the test's application is straightforward in that respect. *See Fisher*, 425 U.S. at 411 (accused may be compelled to submit handwriting exemplar even though doing so would "admit his ability to write" because that fact "would be a near truism"); *Butcher v. Bailey*, 753 F.2d 465, 469 (6th Cir. 1985) (applying foregone conclusion test to debtor's personal records and finding possession a foregone conclusion because it "border[s] on tautology" that one has control of one's own personal records).

Moreover, the Supreme Court's established framework for evaluating assertions of the Fifth Amendment privilege cannot be discarded on the ground that its faithful application often results in outcomes that are unfavorable to parties asserting the privilege. If applying the foregone conclusion test often results in people being compelled to unlock their phones, that fact does not show that the test is being applied improperly; it shows that many assertions of privilege are meritless.

Defendant relies on *Pollard v. State*, 287 So. 3d 649 (Fla. Dist. Ct. App. 2019), to argue that the nature of the act of producing a phone's passcode requires shifting the focus of the foregone conclusion test from the phone's passcode to the phone's contents because otherwise the compelled production of a passcode could never satisfy the foregone conclusion test. Def. Br. 29-30 (citing *Pollard*, 287 So. 2d at 656). *Pollard* reasoned that the foregone conclusion test requires that "[t]he state must have sufficient proof of authenticity *before* it can compel the password's production," and therefore the fact that a password's authenticity can be conclusively established after production by observing that its entry unlocked the phone is insufficient. *Id.* at 656 (emphasis in original). But *Pollard* misunderstood what it means for the authenticity of evidence to be a foregone conclusion.

Authenticity is a foregone conclusion if the government's ability to authenticate the evidence produced, independent of the assertion of authenticity implicit in the act of production, is a foregone conclusion. *See United States v. Greenfield*, 831 F.3d 106, 118-19 (2d Cir. 2016) (authenticity is foregone conclusion if "the Government can prove that it is a foregone conclusion that the [evidence] . . . could be authenticated by the Government independent of [the person's] production of [it] when the [order] was issued"); *In re Grand Jury Subpoena Dated April 18, 2003*, 383 F.3d 905, 912 (9th Cir. 2004) (similar); *United States v. Stone*, 976 F.2d 909, 911-12 (4th Cir. 1992)

(similar); *United States v. Clark*, 847 F.2d 1467, 1473 (10th Cir. 1988) (similar); *United States v. Rue*, 819 F.2d 1488, 1494 (8th Cir. 1987) (similar).

For example, it was not a foregone conclusion in *Fisher* that whatever the taxpayers eventually produced in response to the order to produce their tax documents would in fact be those documents. But the authenticity of the tax documents was nonetheless a foregone conclusion because, once the documents were produced, the government "could independently confirm their . . . authenticity through the accountants who created them." *Hubbell*, 530 U.S. at 44-45. Similarly, in *Bouknight*, a mother could not assert privilege against an order that she produce her child, Maurice, "upon the theory that compliance would assert that the child produced is in fact Maurice" because "the State could readily establish" whether the child produced was Maurice. 493 U.S. at 555 (citing *Fisher*, 425 U.S. at 411); *see also Rue*, 819 F.2d at 1494 (authenticity of physician's patient cards was foregone conclusion because cards could be independently authenticated "by comparing the contents of the patient cards with information from other documents whose authenticity is already established . . . or from information provided by the patients themselves").

In the case of a phone's passcode, authenticity is a foregone conclusion because police have the ability to authenticate the passcode by examining the phone after the passcode has been entered; "[i]f the phone or computer is accessible once the passcode or key has been entered, the passcode or key is

authentic." *Stahl*, 206 So. 3d at 136. In other words, phone passcodes are self-authenticating, in that their interaction with the world establishes their authenticity independently from any implicit assertion of authenticity. *Id.*; *Andrews*, 234 A.3d at 1275 ("passcodes self-authenticate by providing access to the cellphones' contents"); *cf. Fisher*, 425 U.S. at 411 (accused may be compelled to submit handwriting exemplar even though doing so "impliedly asserts that the exemplar is his writing" because that fact is "self-evident"). Thus, nothing about the nature of passcodes renders Supreme Court's established foregone conclusion test inapplicable; the compelled act of producing a passcode is susceptible to the same foregone conclusion analysis just like a compelled act of producing anything else.

3. Defendant may be compelled to enter the passcode to the phone seized from him under the foregone conclusion test because the existence, possession, and authenticity of that passcode are foregone conclusions.

Applying the foregone conclusion test to the facts of this case, defendant may be compelled to enter the passcode to the phone seized from him by police because the three facts that would be implicitly asserted through that act — the existence of the passcode, his possession of the passcode, and the authenticity of the passcode, *see supra* § II.A.1 — are all foregone conclusions. The trial court found as much, reasoning that "the implied statement of fact communicated by disclosure of the pass code," which the trial court identified as "that the phone belongs to the defendant and he was capable of accessing it," would "provide no further evidence than

already exists." R39. Defendant fails to show that this factual finding is against the manifest weight of the evidence. *See Doe I*, 465 U.S. at 613-14 & n.11 (trial court's findings with respect to whether facts implicit in performance of compelled act are foregone conclusions are factual determinations because they "essentially rest[ ] on determinations of fact").

And it is not. The trial court reasonably found it a foregone conclusion that the phone's passcode exists because the phone is passcode-protected. R7-8; *see Andrews*, 234 A.3d at 1275. The trial court also reasonably found it a foregone conclusion that defendant possesses the passcode to the phone because the phone was seized from him, R7, 9-10, and he previously identified the number to the phone as his own phone number in court filings, R9; C11, C20. *See Andrews*, 234 A.3d at 1275. And it is a foregone conclusion that if defendant is compelled to enter the phone's passcode, police will be able to authenticate the passcode that he enters without relying on the assertion of authenticity implicit in his act of entering it by examining the phone to see if it is unlocked; if the phone is unlocked after defendant enters the passcode, then police will know that the passcode was authentic. *See Andrews*, 234 A.3d at 1275; *see supra* pp. 41-42. Because all of the facts that would be implicitly asserted by defendant's entry of the phone's passcode are foregone conclusions, the appellate court correctly held that, consistent with the Fifth Amendment, defendant may be compelled to enter the passcode to the phone.

* * *

In sum, the appellate court correctly held that defendant may be compelled to enter the phone's passcode because, although testimonial, the facts to which entering the phone's passcode would implicitly testify — that the passcode exists, defendant possesses it, and the passcode defendant enters is the passcode to the phone — are all foregone conclusions and therefore unprivileged.

CONCLUSION

For these reasons, the People of the State of Illinois respectfully request that this Court affirm the judgment of the appellate court.

November 29, 2022

Respectfully submitted,

KWAME RAOUL
Attorney General of Illinois

JANE ELINOR NOTZ
Solicitor General

KATHERINE M. DOERSCH
Criminal Appeals Division Chief

JOSHUA M. SCHNEIDER
Assistant Attorney General
100 West Randolph Street, 12th Floor
Chicago, Illinois 60601-3218
(773) 590-7123
eserve.criminalappeals@atg.state.il.us

Counsel for Respondent-Appellee
People of the State of Illinois

RULE 341(c) CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rules 341(a) and (b). The length of this brief, excluding the pages containing the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service, and those matters to be appended to the brief under Rule 342(a), is 11,319 words.

/s/ Joshua M. Schneider
JOSHUA M. SCHNEIDER
Assistant Attorney General

PROOF OF FILING AND SERVICE

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct. On November 29, 2022, the foregoing **Brief of Plaintiff-Appellee People of the State of Illinois** was filed with the Clerk of the Supreme Court of Illinois, using the Court's electronic filing system, which provided service to the following:

Joshua Scanlon
Assistant Appellate Defendant
Office of the State Appellate Defender
Fourth Judicial District
400 West Monroe Street, Suite 303
Springfield, Illinois 62704
4thdistrict.eserve@osad.state.il.us

Daniel Markwell
DeWitt County State's Attorney
201 West Washington Street
Clinton, Illinois, 61727
dmarkwell@dewittcountyill.com

David J. Robinson
State's Attorney Appellate Prosecutor
725 South Second Street
Springfield, Illinois 61704
4thdistrict@ilsaap.org

Rebecca K. Glenberg
Roger Baldwin Found. of ACLU
150 N. Michigan Ave, Ste. 600
Chicago, Illinois 60601
rglenberg@aclu-il.org

/s/ Joshua M. Schneider
JOSHUA M. SCHNEIDER
Assistant Attorney General