ELECTRONICALLY FILED APR 28, 2026 CLERK OF SUPREME COURT

IN THE SUPREME COURT OF IOWA
Supreme Court No. 26–0067
Polk County No. FECR391528

STATE OF IOWA,
Plaintiff-Appellant,

vs.

KASSANDRA MARIE LARSEN,
Defendant-Appellee.

APPEAL FROM THE IOWA DISTRICT COURT
FOR POLK COUNTY
THE HON SCOTT D. ROSENBERG, JUDGE

BRIEF OF APPELLANT

BRENNA BIRD
Attorney General of Iowa

LOUIS S. SLOVEN
Assistant Attorney General
Hoover State Office Building, 2nd Floor
Des Moines, Iowa 50319
(515) 281-5976
louie.sloven@ag.iowa.gov

KIMBERLY GRAHAM
Polk County Attorney

LEVI GROVE
Assistant Polk County Attorney

ATTORNEYS FOR PLAINTIFF–APPELLANT

TABLE OF CONTENTS

TABLE OF AUTHORITIES 4

STATEMENT OF THE ISSUE PRESENTED FOR REVIEW 8

ROUTING STATEMENT 9

NATURE OF THE CASE 10

STATEMENT OF THE FACTS 11

JURISDICTIONAL STATEMENT 17

ARGUMENT 17

I. Entering a passcode to unlock a phone is a non-testimonial act of production. The district court erred in ruling that it would violate Larsen's rights under the Fifth Amendment to compel that act, to enable the search authorized by warrant. 17

II. Even if unlocking a phone by entering a passcode has some testimonial significance, it only impliedly asserts facts that "add little or nothing." So the foregone-conclusion doctrine defeats Larsen's assertion of Fifth Amendment privilege... 37

A. The act of entering the passcode to unlock the phone (at most) only asserts one fact: the person knows the passcode. So the court may compel that act if Larsen's knowledge of that passcode is a foregone conclusion. 40

B. Contents of the device—incriminating or otherwise—are irrelevant to this analysis 44

1. The act of unlocking the phone makes no implied assertions about its contents. 44

2. Acts of production that are either non-testimonial or non-privileged via the foregone-conclusion doctrine may be compelled, even if the evidence to be produced is powerfully incriminating 46

C. Applying the foregone-conclusion doctrine to these facts will not expand it or cause it to swallow the privilege. This is a faithful application, not an expansion. 47

D. Any appeal to privacy interests is a smokescreen. The Fourth Amendment protects privacy interests. When the State obtains a search warrant, privacy gives way. 49

E. The Fifth Amendment does not enable a defendant to make real evidence "warrant-proof" by placing it in a locked safe or device, then asserting that the physical act of unlocking it is testimonial and privileged. 51

CONCLUSION 57

REQUEST FOR NONORAL SUBMISSION 57

CERTIFICATE OF COMPLIANCE 58

TABLE OF AUTHORITIES

Federal Cases

Andresen v. Maryland, 427 U.S. 463 (1976) 30

Boyd v. United States, 116 U.S. 616 (1886) 48

Curcio v. United States, 354 U.S. 118 (1957) 35

Doe v. United States, 487 U.S. 201 (1988) 24, 28, 46, 48, 49, 56

Fisher v. United States, 425 U.S. 391 (1976) 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, 36, 37, 38, 41, 44, 46, 47, 48, 50, 53, 56

Gilbert v. California, 388 U.S. 263 (1967) 24

In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012) 39, 44, 46

In re Grand Jury, 541 F.Supp. 1 (D.N.J. 1981) 29

In re Grand Jury, 680 F.2d 327 (3d Cir. 1982) 29

In re Harris, 221 U.S. 274 (1911) 26, 27, 41

Jaffee v. Richmond, 518 U.S. 1 (1996) 20

Schmerber v. California, 384 U.S. 757 (1966) 25

United States v. Apple MacPro Computer, 851 F.3d 238 (3d Cir. 2017) 38

United States v. Burr, 25 F. Cas. 30 (CC Va. 1807) 20

United States v. Burr, 25 F. Cas. 38 (CC Va. 1807) 20, 21, 36

United States v. Combs, No. 24-CR-542, 2025 WL 2211300 (S.D.N.Y. June 30, 2025) 41

United States v. Doe, 465 U.S. 605 (1984) 28, 29, 30, 31, 32, 36

United States v. Hubbell, 530 U.S. 27 (2000) .. 18, 19, 20, 22, 23, 30, 31, 33, 35, 36, 37, 38, 41, 46, 54

United States v. Nobles, 422 U.S. 225 (1975) 50

United States v. Payne, 99 F.4th 495 (9th Cir. 2024) 23

United States v. Shvartsman, 722 F.Supp.3d 276 (S.D.N.Y. 2024) 10, 13, 16, 39, 47, 48, 49, 56

United States v. Smith, 706 F.Supp.3d 404 (S.D.N.Y. 2023) 39, 41

United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018) 39

United States v. Wade, 388 U.S. 218 (1967) 24, 25

State Cases

Commonwealth v. Davis, 220 A.3d 534 (Pa. 2019)..... 39, 47, 51, 54, 55

Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014)..... 32, 38

Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019) 38, 41, 43, 45

Lamasters v. State, 821 N.W.2d 856 (Iowa 2012) 17

People v. Sneed, 230 N.E.3d 97 (Ill. 2023) ..16, 24, 32, 36, 38, 40, 42, 45, 46

Reynolds v. State, 516 P.3d 249 (Okla. Ct. Crim. App. 2022)..... 38, 42, 53

Seo v. State, 148 N.E.3d 952 (Ind. 2020)..... 39, 44, 46, 50

State v. Andrews, 234 A.3d 1254 (N.J. 2020) ... 32, 33, 38, 41, 42, 44, 49, 51

State v. Anywar, No. 23–0149, 2024 WL 3887198 (Iowa Ct. App. Aug. 21, 2024)..... 55

State v. Diamond, 905 N.W.2d 870 (Minn. 2018)..... 23, 24, 36

State v. Doolin, 942 N.W.2d 500 (Iowa 2020) 9

State v. Garcia, 350 So.3d 322 (Fla. 2022)..... 9, 52

State v. Johnson, 576 S.W.3d 205 (Mo. Ct. App. 2019) 38, 40, 45

State v. Liggins, 978 N.W.2d 406 (Iowa 2022) 17, 37

State v. Marchant, No. 24–1500, 2026 WL 380053 (Iowa Ct. App. Feb. 11, 2026) 55

State v. Pittman, 479 P.3d 1028 (Or. 2021) 41, 47, 51

State v. Roberson, 935 N.W.2d 813 (Wis. 2019) 9

State v. Stahl, 206 So.3d 124 (Fla. Dist. Ct. App. 2016) 38, 42, 45, 46

State v. Valdez, 552 P.3d 159 (Utah 2023) 39, 48

State Statutes

Iowa Code § 665.2(3) 14

Iowa Code § 665.4 14

Iowa Code § 665.5 14

State Rules

Iowa R. App. P. 6.1001(2)(c), (d), (f) 9, 10

Iowa R. App. P. 6.106(b) 17

Other Authorities

Akhil Reed Amar & Renee B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857 (1995) 49, 50

Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767 (2019) 41, 45, 51, 53

Orin S. Kerr, *Decryption Originalism: The Lessons of Burr*, 134 HARV. L. REV. 905 (2021) 21, 22

Gabriel Pell, *The 'Realness' Key to Compelled Passcode Production*, 115 J. CRIM. L. & CRIMINOLOGY 1 (2025) 35, 38

Lawful Access, U.S. DEP'T OF JUST. (Oct. 30, 2020), https://perma.cc/6VJV-2UMH 51

Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, U.N. OFFICE ON DRUGS & CRIME, at 32–33 (2015), https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf 54

STATEMENT OF THE ISSUES PRESENTED FOR REVIEW

I. The State obtained a search warrant that authorized a search of Larsen's phones. There was a pink iPhone that rang when officers called Larsen's phone number. There were also three phones in a safe in Larsen's living area. The State moved for an order compelling her to input passcodes to unlock each phone. Larsen resisted and claimed that the act of inputting a passcode was testimonial, incriminating, and could not be compelled under the Fifth Amendment. The district court denied the State's motion to compel and rejected its argument that entering a passcode to unlock a phone was a non-testimonial act of production. Did it err?

II. The State also argued the foregone-conclusion exception: that even if inputting the passcode to unlock a phone was a testimonial act of production, the act may still be compelled because the State could already prove the only fact that the act would impliedly assert: that Larsen knew that passcode. The district court found the foregone-conclusion doctrine was inapplicable, based on *Shvartsman*—which held that the doctrine did not enable a court to compel a person to make an oral/written statement to *reveal* their passcode. Did the district court err?

ROUTING STATEMENT

Retention by the Iowa Supreme Court is appropriate. This appeal raises an issue of first impression in Iowa's appellate courts, and an issue on which Iowa district courts have split: whether the Fifth Amendment prohibits courts from imposing contempt sanctions on the owner of a phone who refuses to input the passcode to open that phone, so that officers may execute a valid warrant to search its contents. *See* D0041, Reply-Attachment (11/7/25) (ruling on the same issue that reached the opposite result in *State v. Quintero*, FRCR387476); D0037, Motion to Compel (10/2/25), 5 n.2. This is also an issue of broad public importance, involving substantial questions of enunciating legal principles. The district court's ruling threatens to place all evidence in phones (or any other encrypted electronic storage) off limits to investigators with valid search warrants. *See State v. Garcia*, 350 So.3d 322, 324 n.3 (Fla. 2022) (explaining that inability to compel phone owner to use passcode to unlock the phone makes its contents "warrant-proof"). Any "categorical rules of exclusion . . . are the antithesis of justice because one of the major tenets in the administration of justice is the presentation of reliable, relevant evidence at trial." *See State v. Doolin*, 942 N.W.2d 500, 515 (Iowa 2020) (quoting *State v. Roberson*, 935 N.W.2d 813, 820–21 (Wis. 2019)). So retention is appropriate. *See* Iowa R. App. P. 6.1001(2)(c), (d), (f).

NATURE OF THE CASE

This is the State's appeal from a ruling that denied its motion to compel defendant Kassandra Marie Larsen to enter passcodes to unlock her phones so officers could search their contents, pursuant to valid warrants. The district court ruled that compelling Larsen to input her passcode to open any phone would violate the Fifth Amendment—in a way that compelling her to open it using biometrics would not—because a passcode "is testimonial in nature." *See* D0044, Ruling (12/1/25), 7–8. It also ruled that the foregone-conclusion doctrine did not apply to anything other than "non-verbal acts of production," out of "respect [for] the inviolability of the human personality and of the right of each individual to a private enclave where he may lead a private life." *See id.* at 9–10 (quoting *United States v. Shvartsman*, 722 F. Supp. 3d 276, 318–20 (S.D.N.Y. 2024)). So, despite the fact that the State already obtained a warrant with a magistrate's finding of probable cause to believe that Larsen's phones contained evidence of narcotics trafficking (involving the 300-plus grams of methamphetamine and thousands of dollars in cash found in the same safe, right next to her phones), the district court ruled that neither it nor the State had any power to compel Larsen to enter a passcode to unlock any phone so that it could be searched, nor any power to sanction her for refusing to do so. *See id.*; *accord* D0096, Re-Ruling (1/12/26).

The State appeals from that ruling. Ordering Larsen to *recite* or *reveal* the passcode to her phone might compel a testimonial communication. But ordering her to *open* any phone—whether that means inputting a passcode, or providing biometric identifiers, or doing any other act that grants access—would only compel a non-testimonial act of production. Alternatively, even if this act of production had some minimal testimonial value, a court could still compel the act under the foregone-conclusion doctrine, which emerged from *Fisher v. United States*. The Fifth Amendment does not give Larsen the power to place physical evidence beyond the reach of a warrant (or the trial process) by locking it up, then claiming a constitutional right to swallow the key.

STATEMENT OF THE FACTS

On May 1, 2025, detectives with the Mid-Iowa Narcotics Enforcement Task Force searched a residence that Larsen shared with two others. Larsen lived in the basement, and the two other residents lived upstairs. An affidavit from a detective laid out what they found in the basement area:

> Detectives located what was recognized as methamphetamine and drug paraphernalia in plain view . . . . Some of the methamphetamine was loose in different containers. Detectives also located functional digital scale with what appeared to be methamphetamine residue. I know digital scale[s] are an indispensable tool of the drug trade and are used in the measuring of controlled substances for distribution, including methamphetamine. Narcotics packaging was located throughout the basement as well wholly consistent with narcotics trafficking.

Also located in the basement was documentation for Larsen. Near a safe located in the basement, Detectives located an ID card for Larsen as well as a department of transportation form demonstrating her residency in the basement area of the residence.

After the safe was broken open, within the safe Detectives located two bags totaling over 300 grams of methamphetamine, over three thousand (3,000) dollars in U.S. currency, and female jewelry as well as three phones . . .

[. . .]

Additionally, within the safe, Detectives located a check issued to Sholley [another subject of the investigation, who lived upstairs in the same house]. The check appeared it was then signed over to Quillen [who lived upstairs, owned the house, and was married to Sholley] and was ultimately cashed by Larsen appearing to likely be in her possession last.

[. . .]

I asked Larsen what the combination to the safe in the basement and she stated she didn't know. Larsen did not state she was unaware of the safe located in the basement.

When asked about her phone, Larsen stated she believed her phone would be in the house. When asked what her phone looked like, so Detectives could identify hers, she stated she didn't know and it was a phone.

Larsen then stated she didn't currently have a working phone, but she has a Samsung with a broken screen and no case and [that] she also had an iPhone she lost a couple of days prior.

Larsen was asked if she could call or text on either of her phones and she stated, "no", and told Detectives there was no service. Larsen stated her phone number is 515-865-1744. I asked if I called that number which phone would it go to and she stated she didn't know. Her conduct was consistent with evasive actions which, based on my training and experience, are often an attempt to distance oneself from a phone containing evidence of guilt and law enforcement detection of its contents.

D0037, Attachment 4 (10/2/25), 8–10. When an officer dialed that number, a fourth phone (a pink iPhone in a black purse in the kitchen) began to ring. *See id.* at 10. Detectives told Larsen that "pursuant to the previously signed search warrant, she was . . . required to provide her passcode and/or face ID" to unlock her phones, so that they could be searched. Larsen refused. *See id.*

> Subsequently, while in custody on approximately 5/5/2025, while on a recorded phone call with Sholley, [Sholley] asked if Larsen had provided her passcode and she stated she had not. She also stated she had someone with the ability to delete everything off of her phone.

Id.; *accord* D0151, Transcript (11/10/25), 41:24–44:8 ("[I]t was either that she had someone that she needed to get the passcode to to erase the phone or that she had someone with the ability with the passcode to erase the phone.").

Detectives obtained another warrant to search the contents of those four phones (among others). *See* D0037, Attachment 3. That warrant granted "[a]uthority to compel individuals to apply . . . his/her finger prints and/or face to the biometric reader on any electronic device, or physically enter the security code . . . [thus] revealing said security code to law enforcement, for the purposes of unlocking and keeping the . . . device in an unlocked state." *Id.* at 1–3. Detectives presented Larsen (and her counsel) with that warrant and gave her opportunities to enter the passcodes that unlock those phones. She still refused. *See* D0151, Transcript, 39:20–40:8.

The State moved to compel Larsen to comply, or (if she continued to refuse) for the court to hold her in contempt until she chose to comply. *See* D0037, Motion to Compel, at 4–5 (citing Iowa Code §§ 665.2(3), 665.4, & 665.5). Larsen resisted. *See* D0040, Resistance (11/3/25). She argued there was insufficient proof that any of the three phones in the safe were hers (but she did not contest the proof that she was the owner of the pink iPhone that rang when her number was dialed). *See id.* at 1–3. She also argued that any order that compelled her to "render [any] cellphones into an unlocked state" would violate the Fifth Amendment and would not be permissible under the foregone-conclusion doctrine, as she "would be compelled to self-incriminate by communicating to the State (1) that she knows the password(s); (2) that she has control over the phone(s); (3) that any files found on the device(s) exist; and (4) that she possesses those files." *Id.* at 3–6. The State briefed the Fifth Amendment issue in its reply to that resistance. It argued that an order "to unlock a device" is an order to perform "a nontestimonial act that falls outside the scope of the Fifth Amendment privilege." *See* D0041, Reply, 3–14. It also argued "[e]ven if unlocking a device through . . . passcode entry is deemed testimonial, the foregone conclusion exception applies." *Id.* at 14–19.

At the hearing, a detective testified that it would remain impossible to search any of these phones unless somebody entered the passcode:

> [W]hen a phone is in a pre-unlocked state, meaning it has previously died or just had been restarted, most of the data, if almost all of the data, is encrypted. Once a phone has been unlocked the first time for say, like, you use your passcode for the first time, some of that data remains unencrypted. However, by the time we got Ms. Larsen's [pink iPhone], it had died. So then that part put it at basically pre-unlocked state, which almost has the phone completely encrypted.
>
> [. . .]
>
> If [the pink iPhone] has the most recent up to date iOS, . . . the newest update to the phone, there's an antitheft protection which requires both the passcode and biometrics. . . . Even if we could get a partial extraction, it would not be a full contents of the phone.

D0151, Transcript, 40:9–41:19; *accord id.* at 44:13–18 (confirming that all four phones "remain unaccessible" and still cannot be searched). The pink iPhone had a picture of Larsen and her children as the lock screen (which was the only thing that was visible/accessible when officers charged it and powered it on). *See id.* at 12:17–13:11. None of the phones from the safe had any personalized flair that identified a specific person as their owner or user. *See id.* at 49:3–15. But Larsen admitted that she had multiple cell phones, and those phones were found among other items that belonged to Larsen. *See id.* at 26:6–39:13 & 50:12–52:14.

The district court recognized that "[b]iometric features are comparable to blood samples, voice exemplars, or handwriting samples, which involve physical characteristics and require no cognitive effort." *See* D0044, Ruling, at 5–6. It also recognized that "entering a passcode is functionally equivalent

to using a biometric feature." *Id.* at 6 (citing *People v. Sneed*, 230 N.E.3d 97, 115 (Ill. 2023)). Still, it ruled that "[p]roviding a passcode orally by the defendant is testimonial in nature as it requires the defendant to use his or her thought process to make an oral expression." *See id.* at 8. It then held the foregone-conclusion doctrine "was inapplicable" for reasons identified in a block quote from *United States v. Shvartsman*, 722 F. Supp. 3d 276, 318–20 (S.D.N.Y. 2024). *See id.* at 8–10. So while it ordered that Larsen was "compelled to provide her biometrics . . . to open the phones," it ruled that she "cannot be compelled to provide the passcode to the phones in question." *See id.* at 11.

The State filed a motion to reconsider and amend. It reminded the court that "the State's request is not for any *oral* recitation of the passcode by [Larsen], but rather that she *physically enter* the code in the phones to unlock them." *See* D0095, Motion (12/5/25), at 2–5. It highlighted that this is either non-testimonial or permitted by the foregone conclusion doctrine, even under *Shvartsman*. *See id.* at 4–5 (quoting *Shvartsman*, 722 F. Supp. 3d at 319–20). And it reminded the court that "these devices still cannot be unlocked without both the passcode and the biometric data." *See id.* at 5–6. The district court denied the State's motion, without any explanation. *See* D0096, Re-Ruling (12/15/25).

JURISDICTIONAL STATEMENT

This Court has jurisdiction. The State timely filed an application for discretionary review. *See* D0097, ADR (1/12/26); Iowa R. App. P. 6.106(b). This Court granted it. *See* D0102, Order (2/12/26).

ARGUMENT

I. Entering a passcode to unlock a phone is a non-testimonial act of production. The district court erred in ruling that it would violate Larsen's rights under the Fifth Amendment to compel that act, to enable the search authorized by warrant.

Preservation of Error

Error was preserved. The district court considered and rejected the argument that entering a passcode to unlock a phone was a non-testimonial act of production, and thus an act that Larsen could be compelled to perform without violating the Fifth Amendment. *See* D0044, Ruling, at 2–8; *accord* D0095, Motion, at 2–4; D0096, Re-Ruling. That ruling preserved error. *See Lamasters v. State*, 821 N.W.2d 856, 864 (Iowa 2012).

Standard of Review

Rulings on constitutional claims are reviewed de novo. *See, e.g.*, *State v. Liggins*, 978 N.W.2d 406, 434 (Iowa 2022).

Merits

The Fifth Amendment provides a privilege against self-incrimination. But it only prohibits "the use of compulsion to extort communications from

a defendant"—it does not prohibit "compelling a person to engage in conduct that may be incriminating." *United States v. Hubbell*, 530 U.S. 27, 35 (2000).

> Thus, even though the act may provide incriminating evidence, a criminal suspect may be compelled to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording of his voice. . . . Similarly, the fact that incriminating evidence may be the byproduct of obedience to a regulatory requirement, such as filing an income tax return, maintaining required records, or reporting an accident, does not clothe such required conduct with the testimonial privilege.

Id. at 35–36 (citations omitted). And it is a "settled proposition that a person may be required to produce *specific documents* even though they contain incriminating assertions of fact or belief." *Id.* (emphasis added).

The privilege against self-incrimination only offers protection from compelled production if the act to be compelled is "the functional equivalent" of "being compelled to answer questions" about the "sources of potentially incriminating evidence." *See id.* at 43–44. In *Hubbell*, the United States Supreme Court held that a target of a grand jury investigation who invoked a Fifth Amendment privilege could not be compelled to find, assemble, and turn over incriminating documents, requested via a broad subpoena. It held that "[g]iven the breadth of the . . . 11 categories of documents called for . . . , the collection and production of the materials demanded was tantamount to answering a series of interrogatories asking a witness to disclose the existence and location of particular documents." *See id.* at 41. The act of production

became testimonial because it communicated a belief about each document and its responsiveness. That act of "identifying the hundreds of documents responsive to the requests in the subpoena" was the functional equivalent of answering questions about the contents of every document he possessed—so the act of creating that "catalog" of responsive documents was testimonial and could not be compelled. *See id.* at 41–42. Assembling those documents was testimonial because it "was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox"—which is a non-testimonial act of production that *can* be compelled. *See id.* at 43.

Here, the State did not seek to compel Larsen to identify evidence against her; it did not even seek to compel her to reveal the combination. It only sought to compel her to input her key to open the lock—which would be an act without testimonial value, like surrendering the key to a strongbox.

The original understanding of the Fifth Amendment privilege supports this view. In *Hubbell*, Justice Thomas voiced skepticism of the view that Fifth Amendment privilege did not extend to acts of production, since some founding-era definitions of "witness" include a "a person who gives or furnishes evidence." *See Hubbell*, 530 U.S. at 49–55. He cited a ruling by Chief Justice Marshall during the treason trial of Aaron Burr, on the scope of the Compulsory Process Clause of the Sixth Amendment: that it

"includes the right to secure papers—in addition to testimony—material to the defense." *See id.* at 54–55 (citing *United States v. Burr*, 25 F. Cas. 30, 34–35 (CC Va. 1807)). But that's the Sixth Amendment, and compulsory process to obtain "every man's evidence" is a right that *both* prosecution and defense had at common-law. *See Jaffee v. Richmond*, 518 U.S. 1, 9 & n.8 (1996); *cf. Burr*, 25 F. Cas. at 33 (noting purpose of Compulsory Process Clause is that "the prosecution and defence are placed by the law on equal ground"). That had little to do with a founding-era definition of "witness"—it was about the common-law/pragmatic understanding that any legal right "to compel the attendance of witnesses" should extend to compel "their bringing with them such papers as may be material" to the case. *See Burr*, 25 F. Cas. at 35.

The more pertinent part of *Burr* was the Chief Justice's ruling that a witness (Willie) could be compelled to testify to whether he knew the cipher that would decrypt a coded letter, over a claim of Fifth Amendment privilege. *See United States v. Burr*, 25 F. Cas. 38 (CC Va. 1807). The ruling begins with a now-familiar fixture of Fifth Amendment law: an invocation of the privilege requires the court to determine whether a direct answer may incriminate the witness by proving a "necessary and essential link in the chain of testimony, which would be sufficient to convict him of any crime." *See id.* at 39–41. If so, the witness may invoke the privilege and refuse to answer (provided that he

"say on oath that he cannot answer without accusing himself"). *See id.* But this question to Willie, as "precisely stated," could not do that—because it "refer[red] only to the present knowledge of the cipher." *Id.* at 40. This was particularly notable because any *past* knowledge of the contents of the letter could be incriminating. *See id.* (noting "[t]o know and conceal the treason of another is misprision of treason, and is punishable by law"—which meant "[i]f the letter in question contain evidence of treason" and "if the witness were acquainted with that treason when the letter was written [or copied], he may probably be guilty of misprision of treason"). Even so, the question about whether Willie was *currently* able to decipher the coded letter "may be answered without implicating the witness, because his present knowledge would not. . . justify the inference that his knowledge was acquired previous to this trial, or afford the means of proving that fact." *See id.*

"*Burr* supports the conclusion that a suspect can be compelled to disclose his password" through a court order to "decrypt a file or computer suspected of containing evidence." *See* Orin S. Kerr, *Decryption Originalism: The Lessons of Burr*, 134 HARV. L. REV. 905, 952–56 (2021). In *Burr*, it did not matter whether the answer "led to the discovery" of other evidence that could incriminate the witness—the privilege could only be invoked upon a finding that "[the] answer itself" may incriminate the witness. *See id.* at 953.

> This is an essential distinction. It seems obvious that Willie's testimony could be a causal link to evidence against him. Willie's testimony was needed to authenticate the letter, and authenticating the letter was needed to use it in court. Without Willie's authentication, [another witness who was thought to be able to decrypt the letter] could testify to the content of the letter but not its origins—and therefore its relevance. If the letter contained evidence of Willie's involvement in the treason, then Willie's act of authentication would therefore lead to the admission of evidence in the letter that would help prove his crimes. And yet neither counsel nor Chief Justice Marshall conceived of a merely causal approach to the incrimination test.

See id. Moreover, "[d]isclosing the cipher would have shed no more light on Willie's past state of knowledge of the letter's contents than admitting that he knew it." *See id.* at 955–56. Thus, *Burr* "supports the conclusion that disclosing a password in a search for evidence is not incriminating." *See id.*

> To be sure, disclosing a password may provide a causal link. Testimony about the password may allow the government to unlock the device. And unlocking the device may yield evidence. But the password *itself* is not evidence. In most cases, the password is entirely innocuous. It is a meaningless string of characters. Questioning a suspect about a password is merely a means to access evidence, not evidence itself, much like the questions posed to Willie to determine his knowledge of Burr's cipher to authenticate Burr's letter.

Id. at 954; *accord Hubbell*, 530 U.S. at 40 (explaining that applicability of privilege is only assessed by "the testimony inherent in the act of producing those documents," as opposed to "the contents of the documents"). So even *revealing* a password—not just inputting it—would be a non-testimonial act of production under *Burr* and *Hubbell*, and could thus be compelled.

There is broad (through not unanimous) agreement that compelled use of biometrics to unlock a device does not violate the Fifth Amendment because "turning over a key to a safe or a thumb to unlock a phone" doesn't require a defendant "to divulge the contents of his mind." *See United States v. Payne*, 99 F.4th 495, 511 (9th Cir. 2024) (citing *Hubbell*, 530 U.S. at 43). The district court agreed that providing biometrics was not testimonial. *See* D0044, Ruling, at 5–6 & 11. On that, it was correct—but all of that reasoning is equally applicable to the act of unlocking a device by inputting a passcode. A good example is *State v. Diamond*, where the Minnesota Supreme Court upheld a ruling that held the defendant in contempt until he complied with an order to provide a fingerprint to unlock a cellphone, because "providing a fingerprint to unlock a cellphone is *not* a testimonial communication under the Fifth Amendment." *See State v. Diamond*, 905 N.W.2d 870, 872–73, 875 (Minn. 2018). It explained there was no "communicative testimony inherent in providing the fingerprint," and providing it "did not reveal the contents of Diamond's mind." *See id.* at 876–77. But to the extent that it did—perhaps in the choice of which finger he selected as the "key"—it would not matter:

> Even if providing a fingerprint *did* reveal the contents of the mind, because the act of providing evidence of physical characteristics has no testimonial significance, . . . Diamond's act would still be nontestimonial. The *Doe II* Court clarified 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." [*Doe v. United States*, 487 U.S. 201, 211 n.10 (1988)] (stating that "it is not enough that the compelled communication is sought for its content. The content itself must have testimonial significance" (citing [*Fisher v. United States*, 425 U.S. 391, 408 (1976)]; *Gilbert v. California*, 388 U.S. 263, 267 (1967); [*United States v. Wade*, 388 U.S. 218, 222 (1967)])).

See id. at 877 & n.8. *Diamond* cautioned that it was not deciding "whether providing a password is a testimonial communication." *See id.* at 876 n.5. But the same principle would apply, as unlocking the phone via biometrics and via passcode both lack "testimonial significance" for the same reasons. Both kinds of compelled decryption are "equally comparable to using a key to unlock a door," which is a non-testimonial act of production. *See Sneed*, 230 N.E.3d at 115.

Even after recognizing that, some courts find that "the act of entering a passcode to a cell phone is testimonial" insofar as it "implicitly asserts that . . . (1) the passcode exists, (2) the person producing the passcode possesses or controls it, and (3) the passcode produced is authentic." *See id.* at 114–15. But if that were enough, then a handwriting exemplar would be testimonial: it impliedly asserts that the suspect's handwriting exists, that the suspect is able to produce it, and that the exemplar is authentic. Even so, a handwriting exemplar is not sufficiently testimonial unless the suspect is ordered to write a phrase that becomes "testimonial or communicative matter" because of "the content of what is written." *See Gilbert*, 388 U.S. at 266–67. Or consider a

recording of the suspect's voice, made by compelling the suspect to read an exemplar statement: it impliedly asserts that the suspect can read and speak the words in the statement and that he has possession/control of the voice that is heard on the recording. And yet, it does not qualify as "compulsion to utter statements of a 'testimonial' nature." *See Wade*, 388 U.S. at 222–23 (citing *Schmerber v. California*, 384 U.S. 757, 761, 764 (1966)). The point is that testimonial significance cannot be manufactured by approaching reality with wide-eyed epistemic uncertainty as to whether ordinary things exist and whether a person is capable of ordinary volitional acts.

This is the view taken in *Fisher v. United States*, where the Court held that a group of taxpayers could not assert Fifth Amendment privilege to bar enforcement of subpoenas that ordered them to produce certain documents prepared by their accountants. *See Fisher*, 425 U.S. at 394–96. It explained that "the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence"—rather, it "applies only when the accused is compelled to make a Testimonial Communication that is incriminating." *See id.* at 408. So the fact that the contents of those papers "might incriminate the taxpayer" was irrelevant. *See id.* at 410. The question was whether the act of producing the documents was sufficiently testimonial to implicate the Fifth Amendment. *Fisher* analyzed the issue like this:

> A subpoena served on a taxpayer requiring him to produce an accountant's workpapers . . . does not compel oral testimony; nor would it ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought. . . .
>
> The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced. Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena.. . .
>
> It is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testimony within the protection of the Fifth Amendment. . . .The existence and location of the papers are **a foregone conclusion** and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons "no constitutional rights are touched. The question is not of testimony but of surrender." *In re Harris*, 221 U.S. 274, 279 (1911).
>
> When an accused is required to submit a handwriting exemplar he admits his ability to write and impliedly asserts that the exemplar is his writing. But in common experience, the first would be a near truism and the latter self-evident. In any event, although the exemplar may be incriminating to the accused and although he is compelled to furnish it, his Fifth Amendment privilege is not violated because nothing he has said or done is deemed to be sufficiently testimonial for purposes of the privilege. This Court has also time and again allowed subpoenas against the custodian of corporate documents or those belonging to other collective entities . . . over claims that the documents will incriminate the custodian despite the fact that producing the documents tacitly admits their existence and their location in the hands of their possessor. . . . The existence and possession or control of the subpoenaed documents being no more in issue here than in the above cases, the summons is equally enforceable.

See id. at 410–12 (emphasis added). So *Fisher* rejected the claim of privilege.

The bolded phrase is the origin of the foregone-conclusion doctrine, to be discussed later. But before getting there, it's important to recognize that there's a threshold question of whether any of the "communicative aspects" of the act of production "rises to the level of testimony within the protection of the Fifth Amendment." *See id.* at 411. *Fisher* held that "implicitly admitting the existence and possession of the papers" was not sufficiently testimonial, and thus compelling the act of production did not compel testimony "within the protection of the Fifth Amendment." *See id.* And *Fisher* explained that by analogy to other cases where Fifth Amendment privilege did not apply *at all* to compelled acts of production or exhibition: even though each of the acts arguably "impliedly asserts" or "tacitly admits" some ontological fact, each of those admissions or assertions is so "self-evident" or "near truism" that they fail to qualify as "sufficiently testimonial for purposes of the privilege." *See id.* at 411–12. *Fisher* implies that it's possible to make a foregone-conclusion showing to overcome a claim of privilege when a compelled act of production *is* testimonial. But in *Fisher* itself, no such showing was required—because these compelled acts of production were *not* testimonial, despite the fact that they "implicitly admit[ed] the existence and possession of the papers." *Id.*

So too, here. The district court noted that some courts have ruled that the act of inputting the passcode to unlock a phone is testimonial and cannot

be compelled over a claim of Fifth Amendment privilege because it "implicitly acknowledges ownership and control over the device and its content." *See* D0044, Ruling, at 4–5. But those rulings can't survive *Fisher*—not because of the foregone-conclusion doctrine, but because those are exactly the kinds of implied admissions that are "self-evident" and "near truism," and thus are not sufficiently testimonial to support a claim of Fifth Amendment privilege.

There are some acts of production that are sufficiently testimonial to sustain an invocation of privilege. In *Doe I*, the government tried to compel a business owner to produce records from businesses that he owned, as part of an investigation into corruption in awarding county/municipal contracts. The Court rejected the claim that the records themselves were testimonial—even if their contents were incriminating. *See United States v. Doe*, 465 U.S. 605, 611–12 (1984). But on the act of production, it distinguished *Fisher*:

> In *Fisher*, the Court explored the effect that the act of production would have on the taxpayer and determined that the act of production would have only minimal testimonial value and would not operate to incriminate the taxpayer. Unlike the Court in *Fisher*, we have the explicit finding of the District Court that the act of producing the documents would involve testimonial self-incrimination. . . . The District Court's finding essentially rests on its determination of factual issues. . . . We therefore decline to overturn the finding of the District Court in this regard, . . .

Id. at 613–14. This was perplexing, given that the district court had merely listed the same three implied assertions that were insignificant in *Fisher*: that

the act of producing those documents would "admit that the records exist, that they are in [respondent's] possession, and that they are authentic." *See id.* at 608 (quoting *In re Grand Jury*, 541 F. Supp. 1, 3 (D.N.J. 1981)). Only in two footnotes did *Doe I* offer analysis that helped explain the difference:

> "[W]e find nothing in the record that would indicate that the United States knows, as a certainty, that each of the myriad documents demanded by the five subpoenas in fact is in the [respondent]'s possession or subject to his control. The most plausible inference to be drawn from the broad-sweeping subpoenas is that the Government, unable to prove that the subpoenaed documents exist—or that [he] even is somehow connected to the business entities under investigation—is attempting to compensate for its lack of knowledge by requiring [him] to become, in effect, the primary informant against himself." [*In re Grand Jury*, 680 F.2d 327, 335 (3d Cir. 1982).]
>
> The Government concedes that the act of producing the subpoenaed documents might have had some testimonial aspects, but it argues that any incrimination would be so trivial that the Fifth Amendment is not implicated. . . . On the basis of the findings made in this case we think it clear that the risk of incrimination was "substantial and real" and not "trifling or imaginary." Respondent did not concede in the District Court that the records listed in the subpoena actually existed or were in his possession. Respondent argued that by producing the records, he would tacitly admit their existence and his possession. Respondent also pointed out that . . . [b]y producing the documents, respondent would relieve the Government of the need for authentication. These allegations were sufficient to establish a valid claim of the privilege against self-incrimination. This is not to say that the Government was foreclosed from rebutting respondent's claim by producing evidence that possession, existence, and authentication were a "foregone conclusion." *Fisher*, 425 U.S. at 411. In this case, however, the Government failed to make such a showing.

Id. at 613 n.12 & 614 n.13. Essentially, *Doe I* distinguished *Fisher* on three different grounds. First, the act of *identifying* documents as responsive to the "broad-sweeping subpoenas" would have testimonial significance (which mirrors what *Hubbell* would later say). *See id.* at 613 n.12; *accord Hubbell*, 530 U.S. at 41–43. Second, the act of producing any given record would also *authenticate* that record, which could be testimonial if these records would otherwise require authentication (and if the respondent's act of production would "relieve the Government" of a need to find a way to authenticate them). *See Doe*, 465 U.S. at 614 n.13; *accord Andresen v. Maryland*, 427 U.S. 463, 475 (1976) (noting that privilege may protect against compelled production that equates to "a compulsory authentication of incriminating information"). Neither of those was a problem in *Fisher*, because the subpoenas identified records that were known to exist and because authentication could only come from the accountants who authored them (not those taxpayer respondents). *See Fisher*, 425 U.S. at 412–13. And the third way *Doe I* distinguished *Fisher* was by noting that, in *Doe I*, the government had not offered other evidence to establish matters that the act of production would tacitly admit—namely, "possession, existence, and authentication" of those documents—to the point where each matter became a "foregone conclusion." *See Doe*, 465 U.S. at 614 n.13. And that, if shown, would have "rebutt[ed] respondent's claim." *See id.*

So an act of production that identifies certain evidence as responsive or authenticates the evidence produced may have testimonial significance—but only if that identification/authentication is inherent in the act of production *and* carries some fact-specific and non-pedantic "risk of incrimination." *See id.* at 614 n.13; *Fisher*, 425 U.S. at 411–13. An act of production that passes that test may still be compelled, if the government shows that the facts that the act of production would impliedly assert are "foregone conclusions." *Id.* Most courts skip to that second step. But that ignores the part of *Fisher* that directs courts not to reflexively accept a claim that an implied assertion has testimonial significance. That analysis matters for two reasons. First, if the entire batch of implied assertions/admissions lacks testimonial significance (like all those inherent in the act of providing a handwriting exemplar), then there is no need to apply the foregone-conclusion doctrine at all—the act of production may be compelled, without further inquiry and without requiring the government to meet any foregone-conclusion standard of proof. *See, e.g.*, *Fisher*, 425 U.S. at 411; *cf. Hubbell*, 530 U.S. at 34–35 (collecting examples). Second, if only *some* implied assertions have testimonial significance, then the foregone-conclusion inquiry should focus on those—to the exclusion of implied assertions that *lack* significance that "rises to the level of testimony within the protection of the Fifth Amendment." *See Fisher*, 425 U.S. at 411.

Now apply that to the canard that "entering a passcode to a cell phone is testimonial" because it "implicitly asserts that . . . (1) the passcode exists, (2) the person producing the passcode possesses or controls it, and (3) the passcode produced is authentic." *See, e.g.*, *Sneed*, 230 N.E.3d at 114–15. A faithful application of *Fisher* would discard both (1) and (3) immediately—both are "self-evident." *See Fisher*, 425 U.S. at 411–12. Whenever a device warns that a passcode is required to unlock it, such a passcode must exist. The authenticity of a passcode that unlocks the phone is both self-evident and wholly irrelevant, when a person is compelled to enter that passcode without revealing it (because the State can't offer a still-unknown passcode as evidence, so this can't "relieve the [State] of the need for authentication" of evidence that it would otherwise need to authenticate). *See Doe*, 465 U.S. at 614 n.13; *see also State v. Andrews*, 234 A.3d 1254, 1275 (N.J. 2020) ("[T]o the extent that authentication is an issue . . . , the passcodes self-authenticate by providing access to the cellphones' contents" making implied assertions as to their authenticity irrelevant); *cf. Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 615 n.14 (Mass. 2014) ("[D]efendant's decryption . . . does not present an authentication issue analogous to . . . a subpoena for specific documents because he is not selecting documents and producing them . . . ."). Neither of those have any testimonial significance; both fall right out of the analysis.

The only implied assertion that *could* have testimonial significance is the second one: by inputting the passcode that unlocks the phone, a person admits (through conduct) that they know the passcode. This assertion *may* have testimonial significance, in certain cases. *See Fisher*, 425 U.S. at 410 (noting testimonial significance may "depend on the facts and circumstances of particular cases or classes thereof"). But in any case "where ownership and control of an electronic device is not in dispute, its passcode is generally not substantive information" and confirming the device-owner's knowledge of its passcode "does not reveal an inference that a crime has been committed." *See Andrews*, 234 A.3d at 1276. It is a "near truism" that a person who owns or uses a cellphone will know the passcode that unlocks it and renders it usable. *See Fisher*, 425 U.S. at 411. This applies to the pink iPhone, here: that device was found in Larsen's purse; it rang when officers dialed the phone number that Larsen gave them and said was hers; and it displayed a photo of Larsen and her daughter, on the lock screen. *See* D0037, Attachment 4, at 10; D0151, Transcript, 12:17–13:11. Compelling Larsen to input a passcode to unlock that pink iPhone is not "the functional equivalent" of "being compelled to answer questions" about "sources of potentially incriminating evidence." *See Hubbell*, 530 U.S. at 43–44. It is functionally equivalent to being ordered to produce a key to a strongbox found in her home—a non-testimonial act of production.

The district court apparently agreed with most of that, and then erred in misapprehending the nature of the State's request for an order compelling Larsen to *enter* the passcode—not recite it out loud or otherwise reveal it. *See* D0044, Ruling, at 6–8; D0095, Motion, at 2–5. Though it fumbled the ball on the five-yard line, it correctly identified that the act of unlocking a phone is generally non-testimonial, unless it "requires the defendant to use his or her thought process to make an oral expression." *See* D0044, Ruling, at 8. To be more precise, the compelled oral expression is what would make that testimonial. The fact that a defendant must "use his or her thought process" to perform the compelled act of production is a red herring:

> [T]argets must use their minds at least to some extent every time they produce evidence. In terms of 'using the contents of the mind,' there is no meaningful distinction between producing a key and recalling the combination to a safe. To produce a key, a target would need to use their memory (i.e., mind) to recall the key's location (perhaps calling up a mental picture of the key, identifying its keychain or color-coded rubber cap, and retracing steps to its last sighting). Even if the key in question is hanging from a chain on their person, the recognition of that fact and identification of the key on the ring also use mental powers. Similarly, to recall the combination to a safe, the target would have to recall the series of numbers and the associated dial twists. Indeed, a physical key (such as the key to a safe-deposit box) could itself be kept in a combination safe. And yet, once the government establishes the target's possession of an existing key . . . , its storage in a locked combination safe would not preclude production just because the target would first need to use their mind to open the safe. It certainly would not have mattered if the attorneys [or defendants] in *Fisher* were storing the workpapers in a combination safe.

Gabriel Pell, *The 'Realness' Key to Compelled Passcode Production*, 115 J. CRIM. L. & CRIMINOLOGY 1, 19–20 (2025). Nor does any act of "obedience to a regulatory requirement, such as filing an income tax return, maintaining required records, or reporting an accident" acquire testimonial significance from the fact that all those acts require some amount of conscious thought—that "does not clothe such required conduct with the testimonial privilege." *See Hubbell*, 530 U.S. at 35–36. Only "the communicative aspect" of the act might be testimonial—the Fifth Amendment privilege only bars a court from compelling an act that *reveals* the actor's thoughts. *See id.* at 43–44; *accord Curcio v. United States*, 354 U.S. 118, 128 (1957) (explaining that courts may compel "production of corporate or association records by their custodian," but cannot compel that custodian to testify about location of missing records because that "requires him to disclose the contents of his own mind"). Here, unlocking the phone (by biometrics or by passcode) neither reveals thoughts nor requires any oral expression, so it is a non-testimonial act of production and may be compelled, over Larsen's claim of Fifth Amendment privilege. To whatever extent that the district court ruled otherwise, it erred.

* * *

Neither of the first two grounds on which *Doe I* distinguished *Fisher* apply to imbue this act of production with any testimonial significance—it

does not identify particular documents or objects as responsive, nor does it provide authentication for any evidence that may need to be authenticated. *See Doe*, 465 U.S. at 613 n.12 & 614 n.13. Entering that passcode to unlock the phone would only admit "present knowledge of the cipher," which has no testimonial significance that triggers Fifth Amendment privilege—not under *Fisher*, nor under any founding-era understanding of the Fifth Amendment. *See Burr*, 25 F. Cas. at 40. All of the facts that the act of unlocking the phone could impliedly admit—that the passcode exists, that she knows it, and that it is authentic—are "self-evident" and "a near truism." *Fisher*, 425 U.S. at 411. The act of unlocking a phone using biometrics is non-testimonial—and so is the functionally-equivalent act of unlocking a phone by entering a passcode, for the same reasons. *See Diamond*, 905 N.W.2d at 875–77. Both those acts are "equally comparable to using a key to unlock a door"—a non-testimonial act of production. *See Sneed*, 230 N.E.3d at 115. On issuance of a warrant or a subpoena for any evidence behind the door or on the phone, a person who knows how to unlock it may be compelled to do so. The content of evidence to be found there—incriminating or not—is not relevant; nor is the fact that the act of production requires some amount of thought (since no such thoughts are revealed by the act itself). *See Hubbell*, 530 U.S. at 35–36. This remains a non-testimonial act of production, so Larsen's claim of privilege must fail.

II. Even if unlocking a phone by entering a passcode has some testimonial significance, it only impliedly asserts facts that "add little or nothing." So the foregone-conclusion doctrine defeats Larsen's assertion of Fifth Amendment privilege.

Preservation of Error

Error was preserved. The court considered and rejected the argument that the foregone-conclusion doctrine applied. *See* D0044, Ruling, at 8–10; D0095, Motion, at 4–5; D0096, Re-Ruling. That ruling preserved error.

Standard of Review

This is another ruling on a constitutional claim. Review is de novo. *See, e.g.*, *Liggins*, 978 N.W.2d at 434.

Merits

Fisher's remark that the assertions implied by that act of production were each "a foregone conclusion" introduced a new thread to the tapestry: it suggested that an act of production that carried implied assertions with some amount of testimonial significance could still be compelled—if those assertions only established facts that the government would be able to prove without difficulty, either before or without the compelled act of production. *See Fisher*, 425 U.S. at 410–12. In *Hubbell*, the Court remarked that *Fisher* had recognized the applicability of a foregone-conclusion exception because the record showed that "the Government already knew that the documents were in the attorneys' possession and could independently confirm their

existence and authenticity," without reliance on the acts of production. *See Hubbell*, 530 U.S. at 44–45 (citing *Fisher*, 425 U.S. at 410–12). Conversely, in *Hubbell*, the government had not shown that it "had any prior knowledge of either the existence or the whereabouts of the . . . documents" produced, so the foregone-conclusion doctrine could not apply on those facts. *See id.*

The district court expressed skepticism of the doctrine's validity and declared that it "cannot sidestep the protection against self-incrimination." *See* D0044, Ruling, at 10. But "virtually every federal circuit court ha[s] used *Fisher* to compel production of evidence from resistant targets," usually by applying the foregone-conclusion doctrine. *See* Pell, *The 'Realness' Key*, 115 J. CRIM. L. & CRIMINOLOGY at 15 & n.73 (collecting cases). *Fisher* is binding; state courts cannot overrule it. The only question is how to apply it.

Courts are split on whether the foregone-conclusion doctrine applies to compelled entry of passcodes to unlock or decrypt devices. Most courts hold that it does. *See, e.g.*, *Sneed*, 230 N.E.3d at 115–20; *Andrews*, 234 A.3d at 1273–75; *State v. Stahl*, 206 So.3d 124, 132–37 (Fla. Dist. Ct. App. 2016); *Commonwealth v. Jones*, 117 N.E.3d 702, 709–18 (Mass. 2019) & *Gelfgatt*, 11 N.E.3d at 612–16; *State v. Johnson*, 576 S.W.3d 205, 225–28 (Mo. Ct. App. 2019); *Reynolds v. State*, 516 P.3d 249, 253–55 (Okla. Ct. Crim. App. 2022); *United States v. Apple MacPro Computer*, 851 F.3d 238, 246–48 & n.7 (3d

Cir. 2017); *United States v. Smith*, 706 F. Supp. 3d 404, 407–09 (S.D.N.Y. 2023); *United States v. Spencer*, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *1–3 (N.D. Cal. Apr. 26, 2018). A minority of courts hold that it does not. *Seo v. State*, 148 N.E.3d 952, 954–62 (Ind. 2020); *Commonwealth v. Davis*, 220 A.3d 534, 550–52 (Pa. 2019); *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1341–49 (11th Cir. 2012). Some courts have rejected motions to compel subjects to *reveal* a passcode—while noting that the foregone-conclusion doctrine would permit a court to compel them to *enter* a passcode and turn over the unlocked device. *See, e.g.*, *State v. Valdez*, 552 P.3d 159, 167–73 (Utah 2023); *Shvartsman*, 722 F. Supp. 3d at 314–20.

The district court identified *Sneed* and *Shvartsman*, then adopted *Shvartsman*'s reasoning that the foregone-conclusion doctrine "has flaws and was inapplicable to compelling the defendant to provide the passcode to a phone." *See* D0044, Ruling, at 8–10. The most glaring problem is that *Shvartsman* goes out of its way to say that courts *can* "compel the suspect to turn over an unlocked phone—whether through biometric means . . . or through entering the passcode themselves without providing the passcode to police," without running afoul of the Fifth Amendment. *See Shvartsman*, 722 F. Supp. 3d at 320 (quoting *Valdez*, 552 P.3d at 163). And that part of *Shvartsman* is correct; the district court erred in ruling otherwise.

A. The act of entering the passcode to unlock the phone (at most) only asserts one fact: the person knows the passcode. So the court may compel that act if Larsen's knowledge of that passcode is a foregone conclusion.

As discussed earlier, some courts begin this analysis by mentioning three implied assertions that correspond to those in *Fisher* and *Doe I*: that "(1) the passcode exists, (2) the person . . . possesses or controls it, and (3) the passcode produced is authentic." *See Sneed*, 230 N.E.3d at 114–15. But (1) and (3) never have testimonial significance (or relevance), and they are generally shown to be foregone conclusions without need for much analysis. *Id.* at 118–19; *Johnson*, 576 S.W.3d at 226. The only real action is on (2):

> "I know the password" is the only assertion implicit in unlocking the device. Because the password is entered without revealing it to the government, any communicative content that its characters might contain (such as a hypothetical password, "ISELLDRUGS") is not asserted to the government. In addition, the act of unlocking the device does not communicate knowledge about the device's contents. Knowing the password and knowing the contents of a decrypted device are two different things. . . .
>
> [. . .]
>
> A bright-line rule results: when investigators . . . obtain an order compelling the suspect to enter in the correct password, the suspect cannot have a valid Fifth Amendment privilege if the government independently can show that the suspect knows the password. The government's independent evidence that the suspect knows the password means that the suspect's knowledge is not in issue. It adds nothing to the sum total of the government's information for the government to learn what it already knows. As a result, the government's independent knowledge that the person knows the password makes the implied testimony of entering it a foregone conclusion.

See Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 779, 782–83 (2019). And that correctly applies the test, as *Hubbell* understood *Fisher*: a fact that would be implied or admitted by the act of production is a "foregone conclusion" if that fact is already provable without "relying on" the act of production itself, so that any arguably testimonial dimension of the compelled act "adds little or nothing to the sum total of the Government's information." *See Hubbell*, 530 U.S. at 44–45 (quoting *Fisher*, 425 U.S. at 411). Here, the testimonial dimension of the act of production "is limited to communicating [the subject's] knowledge of the passcodes." *See Andrews*, 234 A.3d at 1274. Once that fact is proven by other evidence, the issue becomes "one of surrender, not testimony." *Id.* at 1275; *accord Fisher*, 425 U.S. at 411 (quoting *In re Harris*, 221 U.S. at 279).

"The Government has the burden of proof" to prove the facts that will "establish a foregone conclusion, but it is unsettled whether the standard is a preponderance of the evidence or clear and convincing evidence." *United States v. Combs*, No. 24-CR-542, 2025 WL 2211300, at *1 (S.D.N.Y. June 30, 2025) (citing *Smith*, 706 F. Supp. 3d at 409 n.1).[1] That's probably because the

[1] Some state courts have held that their state constitutions require that those facts must be proven beyond a reasonable doubt. *See Jones*, 117 N.E.3d at 713–16; *State v. Pittman*, 479 P.3d 1028, 1050–51 (Or. 2021). Here, the district court's ruling was about Fifth Amendment privilege. There was no separate claim or ruling about Article I, Section 9 of the Iowa Constitution.

real question is whether the evidence already establishes that foregone fact in a way that deprives further proof of that fact of any real usefulness. And that means the evidence must be strong—either conclusive on that point, or so close to it that a fact-finding court can rely on common-sense inferences to get the rest of the way there. *Cf. Sneed*, 230 N.E. at 118 (holding that the State must establish that "it knew with reasonable particularity that . . . the passcode was within defendant's possession and control"); *accord Stahl*, 206 So.3d at 136 (same); *Reynolds*, 516 P.3d at 254 (same).

When the evidence shows that the device is inaccessible and unusable to those who don't know the passcode (as here), any evidence that a person has been accessing and using that device is generally sufficient to show that they know the passcode. *See, e.g.*, *Andrews*, 234 A.3d at 1275 (holding that Andrews's knowledge of passcodes was a foregone conclusion, based on the facts showing "that the cellphones were in Andrews's possession when seized and that he owned and operated the cellphones"); *Stahl*, 206 So.3d at 136 (same, because "Stahl's identification of the phone and the corresponding phone number" made it a foregone conclusion "that the phone was Stahl's and therefore the passcode would be in Stahl's possession"); *Sneed*, 230 N.E.3d at 118–19 (same, because a witness testified "that the phone was seized from defendant's person upon his arrest and that, on the bail bond

sheet, defendant identified the phone number associated with the phone as his own phone number"); *cf. Jones*, 117 N.E.3d at 556–57 (finding that facts had proven Jones's knowledge of the passcode beyond a reasonable doubt by "creat[ing] the reasonable inference that [he] regularly used [that] phone and that he therefore knew its password," and also noting that "exclusive control of the phone is not required" because the possibility "[t]hat multiple people may have used [that] phone and therefore may know its password does not disprove the defendant's knowledge of the password"). So too, here. Larsen told police her phone number. When they dialed it, her pink iPhone rang. So it was already apparent that Larsen used that phone and knew its passcode, even before police saw that the background for the lock screen was a photo of Larsen and her daughter. *See* D0037, Attachment 4, at 10; D0151, Transcript, 12:17–13:11. And Larsen admitted that she had more than one cell phone—so when additional phones were found inside the safe in her living area that contained a check with her signature on it (along with jewelry and more of the same drug that was found in smaller quantities in her living space), the common-sense inference was that those phones belonged to Larsen, as well. *See* D0151, Transcript, at 26:6–39:13 & 50:12–52:14. A passcode-protected device has little value to someone who doesn't know the code. That wasn't the case here—Larsen kept these phones in the safe with her other valuables.

Even if the three phones from the safe are a close question, the pink iPhone is not. The fact that Larsen knew the passcode to unlock that phone was a foregone conclusion—so even if the act of entering the passcode had some testimonial significance, it could still be compelled. It was already so obvious that Larsen would know the passcode to that pink iPhone that the compelled act of production would be an act of "surrender, not testimony." *Andrews*, 234 A.3d at 1274; *Fisher*, 425 U.S. at 411. The district court erred in denying the motion to compel that non-privileged act of production.

B. Contents of the device—incriminating or otherwise—are irrelevant to this analysis.

Some courts hold that the State must prove its knowledge of the fact that "particular files on the device exist [and] that she possessed those files" as part of its foregone-conclusion showing. *See Seo*, 148 N.E.3d at 958; *In re Grand Jury Subpoena*, 670 F.3d at 1347. That's wrong, for two reasons.

1. The act of unlocking the phone makes no implied assertions about its contents.

In resisting the motion to compel, Larsen identified that familiar set of three implied assertions that entering the passcode would offer up—and she added a fourth. She argued that compelling her to enter the passcode would also compel her to admit "that any files found on the device(s) exist." D0040, Resistance, at 5. That would be a truism, lacking testimonial significance. But

just as importantly, it's not something that is communicated or implied *at all* by the act of entering the passcode to unlock the device. Here, "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." *See Jones*, 117 N.E.3d at 711; *accord Stahl*, 206 So.3d at 134 ("By providing the passcode, Stahl would not be acknowledging that the phone contains evidence of video voyeurism."); *Sneed*, 230 N.E.3d at 114.

The extent of the State's knowledge about the contents of the device is irrelevant, because "[t]he focus . . . is the extent of the State's knowledge of the existence of the facts conveyed through the compelled act of production." *See Johnson*, 576 S.W.3d at 227. In a *Hubbell*-type scenario where a target is ordered to find, select, and produce responsive files, the act of production makes implied assertions about the contents of files produced—so the State would have to prove those implied assertions about the contents of the files were foregone conclusions. But in Larsen's case, where the compelled act is "only to unlock the device," the act doesn't make an implied assertion about the contents of the device at all. The State doesn't need to establish that the contents of the device are a foregone conclusion "if the government, not the target, is going to [search] it" and retrieve files after it has been unlocked. *See* Kerr, *Compelled Decryption*, 97 TEX. L. REV. at 786–88.

2. Acts of production that are either non-testimonial or non-privileged via the foregone-conclusion doctrine may be compelled, even if the evidence to be produced is powerfully incriminating.

Some courts have contorted the analysis out of dissatisfaction with the notion that a suspect may be compelled to "lead the Government to evidence that would incriminate him." *In re Grand Jury Subpoena*, 670 F.3d at 1349. So they consider the potentially incriminating content of the evidence to be produced—then impute that to the act of production itself. *See Seo*, 148 N.E.3d at 957–58. But *Fisher* itself rejected that, out of hand. The Fifth Amendment is not violated, "however incriminating the contents of the [documents] might be," if "the act of producing them—the only thing which the [suspect] is compelled to do—would not itself involve testimonial self-incrimination." *See Fisher*, 425 U.S. at 410–11.

When a compelled act of production "is not testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence." *See Stahl*, 206 So.3d at 134 (quoting *Doe*, 487 U.S. at 208 n.6); *accord Hubbell*, 530 U.S. at 36 (explaining that act of producing subpoenaed files cannot become testimonial or privileged "merely because the demanded documents contained incriminating evidence"). And "the testimony implicit in the act of entering the passcode to a cell phone is the same" regardless of its contents—incriminating or otherwise. *See Sneed*,

230 N.E.3d at 114–17. The only implied assertion with (potential/arguable) testimonial significance is that the person knows the passcode that unlocks that phone—so once that fact is shown to be a foregone conclusion, there is no valid claim of Fifth Amendment privilege. *See Fisher*, 425 U.S. at 410–11; *cf. Pittman*, 479 P.3d at 524–26 ("It is only the testimonial aspects of the act of unlocking the phone, and not the practical result of unlocking the phone, that have constitutional significance" in a foregone-conclusion analysis).

C. Applying the foregone-conclusion doctrine to these facts will not expand it or cause it to swallow the privilege. This is a faithful application, not an expansion.

The district court quoted *Shvartsman*'s dissatisfaction with applying the foregone-conclusion doctrine in new ways that threaten to "swallow the constitutional privilege." *See* D0044, Ruling, at 10 (quoting *Shvartsman*, 722 F. Supp. 3d at 318–19). *Shvartsman*, in turn, was quoting *Davis*, which suggested the foregone-conclusion doctrine applies "only in the compulsion of specific existing business or financial records." *See Davis*, 220 A.3d at 237. *Davis*, like *Shvartsman*, is about a motion to compel the suspect to *reveal* their passcode through an oral/written statement (not input it). *See Davis*, 220 A.3d at 223. Applying the foregone-conclusion doctrine to compelled oral/written statements would (arguably) be an expansion—though courts may already compel oral/written statements that are either non-testimonial

or non-incriminating. *See Doe*, 487 U.S. at 209–14. But the doctrine, from its inception, has *always* applied to nonverbal acts of production. Indeed, the whole point of using that phrase in *Fisher* was that there needed to be some sensible limit to claims that acts of production were privileged—and beyond the power of the court to compel—based on implied assertions that might be (marginally) testimonial if stated aloud, but were not genuinely at issue or in dispute. *See Fisher*, 425 U.S. at 410–12. The foregone-conclusion doctrine is best understood as an equilibrium adjustment, to restore balance after the Court held nonverbal acts of production can count as testimonial—the Court understood those earlier pronouncements were far too broad. *See id.* at 405–09 (citing *Boyd v. United States*, 116 U.S. 616 (1886) and others). The reach of the foregone-conclusion doctrine can be understood accordingly: it applies to compelled acts of production (and not oral/written statements) that interpose a weak claim of testimonial privilege, so that the recognition that *some* acts of production are testimonial/privileged does not "proscribe the compelled production of every sort of incriminating evidence." *See id.*

The way to limit the foregone-conclusion doctrine to acts of production is to hold that it may enable a court to compel the target to *enter* a passcode, but not to make oral/written statements that recite or reveal it. *See Valdez*, 552 P.3d at 171–73; *Shvartsman*, 722 F. Supp. 3d at 319–20. To the extent that

the potential expansion of the foregone-conclusion doctrine is a concern, it is not implicated here—the State sought to compel a nonverbal act of production (entering the passcode). The district court erred when it refused to apply the foregone-conclusion doctrine, in reliance on that misplaced concern.

D. Any appeal to privacy interests is a smokescreen. The Fourth Amendment protects privacy interests. When the State obtains a search warrant, privacy gives way.

The district court quoted *Shvartsman* to say that the Fifth Amendment demanded this result out of "our respect [of] the inviolability of the human personality and of the right of each individual to a private enclave where he may lead a private life." *Shvartsman*, 722 F. Supp. 3d at 320 (quoting *Doe*, 487 U.S. at 212); D0044, Ruling, at 10. Larsen did have a right to privacy in the contents of her phone: a *Fourth* Amendment right. That right was already overcome by issuance of a search warrant, on a finding of probable cause by a neutral magistrate. "[T]he Fourth Amendment's privacy protections should not factor into analysis of the Fifth Amendment's applicability." *See Andrews*, 234 A.3d at 1274. The Fifth Amendment, as now understood (without *Boyd*), does not protect any privacy interest. It can only be invoked to avoid giving *incriminating* testimony—and non-incriminating testimony about "intensely private, highly embarrassing matters" cannot trigger the privilege. *See* Akhil Reed Amar & Renee B. Lettow, *Fifth Amendment First Principles: The Self-*

Incrimination Clause, 93 MICH. L. REV. 857, 891 (1995). Another indicator that Fifth Amendment privilege has nothing to do with privacy is that "[a] witness given immunity can be forced to testify about anything." Once the possibility of self-incrimination disappears, the Fifth Amendment privilege loses *all* applicability—no matter how "private" the subject matter. *See id.*

In other words, as the United States Supreme Court explained:

> If the Fifth Amendment protected generally against the obtaining of private information from a man's mouth or pen or house, its protections would presumably not be lifted by probable cause and a warrant or by immunity. . . . The Framers addressed the subject of personal privacy directly in the Fourth Amendment. They struck a balance so that when the State's reason to believe incriminating evidence will be found becomes sufficiently great, the invasion of privacy becomes justified and a warrant to search and seize will issue. They did not seek in still another Amendment —the Fifth—to achieve a general protection of privacy but to deal with the more specific issue of compelled self-incrimination.
>
> We cannot cut the Fifth Amendment completely loose from the moorings of its language, and make it serve as a general protector of privacy—a word not mentioned in its text and a concept directly addressed in the Fourth Amendment. We adhere to the view that the Fifth Amendment protects against "compelled self-incrimination, not (the disclosure of) private information."

Fisher, 425 U.S. at 400–01 (quoting *United States v. Nobles*, 422 U.S. 225, 233 n.7 (1975)). So concerns about privacy are irrelevant to the applicability of Fifth Amendment privilege. The district court erred in ruling otherwise.

On a related note: an animating concern of both *Davis* and *Seo* was the "unique ubiquity and capacity of smartphones" or computers. *See Seo*,

148 N.E.3d at 959–60; *Davis*, 220 A.3d at 240 n.9 (complaining that granting access to the computer that contained the child-pornography video that the law enforcement agents had already viewed "could [also] lead to a trove of a presently unknown number of files" acquired by "peer-to-peer file sharing"). But defendants like Larsen are "free to challenge a search warrant under the [F]ourth [A]mendment" if it purports to authorize a search that exceeds the showing of probable cause. *See Sneed*, 230 N.E.3d at 117–18. Likewise, "the only relevant particularity requirement comes from the Fourth Amendment's warrant clause." *See* Kerr, *Compelled Decryption*, 97 TEX. L. REV. at 787–88. So this Court "should not alleviate concerns over the potential overbreadth of a digital search"—implicating "Fourth Amendment privacy concerns"— by "invoking the Fifth Amendment privilege against self-incrimination, which offers no privacy protection." *See Andrews*, 234 A.3d at 1271 (quoting *Davis*, 220 A.3d at 557 (Baer, J., dissenting)); *accord Pittman*, 479 P.3d at 1046–47 ("[O]nce the state has obtained a valid warrant to search a phone, a defendant does not have a legal right to keep the contents of the phone from the state.").

E. The Fifth Amendment does not enable a defendant to make real evidence "warrant-proof" by placing it in a locked safe or device, then asserting that the physical act of unlocking it is testimonial and privileged.

A ruling that Larsen cannot be compelled to enter a passcode to unlock these phones (regardless of the strength of the showing that her knowledge

of that passcode is a foregone conclusion) would make the contents of all her phones "warrant-proof." *See Garcia*, 350 So.3d at 324 n.3 (quoting *Lawful Access*, U.S. DEP'T OF JUST. (Oct. 30, 2020), https://perma.cc/6VJV-2UMH); *accord* D0095, Motion, at 5–6; D0095, Attachment (12/5/25), at 2 (noting that a passcode is "required" and biometrics are not sufficient to grant access when "[t]he device has just been turned on or restarted" or when "[t]he user hasn't unlocked their device for more than 48 hours"). But the whole point of *Fisher* was to reject these kinds of attempts to shield real evidence in existence from lawful process by cloaking it with Fifth Amendment privilege, when the act of production lacks its own testimonial/evidentiary significance.

> When the government compels a person to open the door and let the government see the treasure inside, it obtains both the door-opening evidence and whatever treasure is revealed.
>
> . . . As a practical matter, the door-opening evidence operates causally as a [potentially] testimonial gateway to the nontestimonial treasure. The government may be unable to obtain the treasure without the door-opening. But the two are analytically distinct, and only the latter is compelled [and potentially] testimony.
>
> The best explanation for the foregone conclusion doctrine is that it prevents the causal relationship between door-opening evidence and treasure from being used to shroud the treasure in the Fifth Amendment protection properly limited to the door-opening. Without the foregone conclusion doctrine, suspects could take simple steps to introduce testimonial doors that block government access to their nontestimonial treasure. For example, a person in Fisher's situation could just gather all of his records and keep them in his possession. Any act of production would have to be compelled from him . . . , introducing an act that implies . . . testimony under the act of production doctrine.

> The foregone conclusion doctrine blunts the advantage from such manipulation. It evaluates if the door-opening testimony is significant or is merely a matter of easily manipulated form. If opening the door implies incriminating testimony that the government does not already know, then the risk of compelled self-incrimination is real and the person has a privilege against opening the door that then necessarily blocks access to the treasure. On the other hand, if [not], then the risk of compelled self-incrimination is only a matter of form. At that point, as *Fisher* recognized, quoting Justice Holmes, "The question is not of testimony but of surrender." When the testimony implicit in the door-opening is not in play, and is only an incidental matter of form rather than substance, access to the treasure should not be blocked by the Fifth Amendment privilege.

Kerr, *Compelled Decryption*, 97 TEX. L. REV. at 777–78; *accord Fisher*, 425 U.S. at 411–12. The district court's refusal to apply *Fisher* offered Larsen the benefit of the *Boyd*-type rule that *Fisher* had rejected: a "prohibition against forcing the production of private papers," that applies *without* any showing that entering the passcode to unlock the phone had testimonial significance "on the facts and circumstances" surrounding this case (or a specific phone). *See Fisher*, 425 U.S. at 408–11. So the data on each phone still exists, but it is now shrouded in Fifth Amendment privilege—made "warrant-proof" by the form of the nonverbal act that Larsen would need to perform, to enable the search that the warrant already gave the State a right to execute.

"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." *See Reynolds*, 516 P.3d at 254. A

ruling that affirms the district court "would create an entire class of evidence, encrypted computer files, that is impervious to governmental search"—and it would "render law enforcement incapable of accessing relevant evidence" in any passcode-protected device. *Davis*, 220 A.3d at 250 (Baer, J., dissenting). The Fifth Amendment does not require that outcome—to the contrary, it is a "settled proposition" that no class of evidence already in physical existence is cloaked in Fifth Amendment privilege, by virtue of content or location. *See Hubbell*, 530 U.S. at 34–36; *accord Sneed*, 230 N.E.3d at 117–18.

The harms of that outcome would be manifold. It would defang every warrant for data on a modern smartphone or computer. Attempts to unravel criminal conspiracies (like large-scale narcotics trafficking) would no longer proceed smoothly along the lines of communication/coordination that were used by each apprehended participant—claims of Fifth Amendment privilege would bring those data-based investigative efforts to a screeching halt, just as if the data had been deleted altogether. *See* D0037, Attachment 4, at 10; D0151, Transcript, 41:24–44:8 (discussing evidence of Larsen's scheme to delete that data). Efforts to stop child pornographers would be hardest hit:

> Recent estimates have indicated that the majority of child sexual abuse material is now exchanged via non-commercial channels, specifically public peer-to-peer platforms, such as Gnutella, eDonkey and eMule. Private peer-to-peer networks are often used by mid-level offenders who establish closed groups to exchange encrypted files.

> [. . .]
>
> Whereas encryption measures were previously not widespread among producers, distributors and consumers of child sexual abuse material—due to fears of being inadvertently locked out of their collections—many offenders now use both local and remote storage services that include built-in encryption technology to evade detection and complicate the work of law enforcement agencies.

Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, U.N. OFFICE ON DRUGS & CRIME, at 32–33 (2015), https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf; *cf. Davis*, 220 A.3d at 537–38 (detailing a child-pornography investigation that led to discovery of encrypted hard drive in defendant's sole possession and no way to access the data without entry of 64-bit encryption key, which defendant admitted that he knew); *State v. Marchant*, No. 24–1500, 2026 WL 380053, at *2 (Iowa Ct. App. Feb. 11, 2026) (noting that police recovered "over 1,000 nude images of the victim across [Marchant's] two phones"). And smartphones increasingly contain relevant evidence to establish commission of other offenses, including serious violent crimes. *See, e.g.*, *State v. Anywar*, No. 23–0149, 2024 WL 3887198, at *2 (Iowa Ct. App. Aug. 21, 2024) (noting "video recorded on Anywar's phone depicted several seconds of the robbery"). At minimum, justice demands an approach that permits the State to obtain that evidence by making a fact-specific showing that the act of production is non-testimonial, or that the foregone-conclusion exception applies.

* * *

The act of entering a passcode to unlock a phone only asserts one fact that *can* have testimonial significance: that the person knows the passcode. In many cases, that assertion will lack testimonial significance. In others, it will have some amount of testimonial significance—but if the State can show that fact is a foregone conclusion, then the act of production should still be compelled over a claim of Fifth Amendment privilege. The State made that showing, here. The pink iPhone was definitely Larsen's, and the other phones were found in a locked safe in her living area, co-mingled with her property and valuables. The act of entering a passcode to unlock her phone makes no assertions about the *contents* of the phone, so its contents are irrelevant to the foregone-conclusion analysis—"however incriminating [they] might be." *See Fisher*, 425 U.S. at 410–11. Applying the foregone-conclusion doctrine to compelled acts of production is nothing new; the "basic Fifth Amendment principles" at work have been "articulated in general terms" and apply to all nonverbal acts of production (but stop there). *See Doe*, 487 U.S. at 209 & n.8; *accord Shvartsman*, 722 F. Supp. 3d at 319–20. Claims of privacy interests receive no weight, given the valid search warrant. And the Fifth Amendment offers no constitutional right to lock up critical evidence and swallow the key. So this act of production may be compelled, over Larsen's claim of privilege.

CONCLUSION

The State respectfully requests that this Court reverse the ruling that denied its motion to compel and remand for further proceedings.

REQUEST FOR NONORAL SUBMISSION

This case should be set for nonoral submission. In the event argument is scheduled, the State asks to be heard.

Respectfully submitted,

BRENNA BIRD
Attorney General of Iowa



LOUIS S. SLOVEN
Assistant Attorney General
Hoover State Office Bldg., 2nd Fl.
Des Moines, Iowa 50319
(515) 281-5976
louie.sloven@ag.iowa.gov

CERTIFICATE OF COMPLIANCE

This brief complies with the typeface requirements and type-volume limitation of Iowa Rs. App. P. 6.903(1)(d) and 6.903(1)(g)(1) or (2) because:

- This brief has been prepared in a proportionally spaced typeface using Georgia in size 14 and contains **12,763** words, excluding the parts of the brief exempted by Iowa R. App. P. 6.903(1)(g)(1).

Dated: April 28, 2026



LOUIS S. SLOVEN
Assistant Attorney General
Hoover State Office Bldg., 2nd Fl.
Des Moines, Iowa 50319
(515) 281-5976
louie.sloven@ag.iowa.gov