ELECTRONICALLY FILED SEP 16, 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

REPLY 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 3

STATEMENT OF THE ISSUES IN THE REPLY BRIEF 5

RESPONSE TO APPELLEE'S ARGUMENT 6

I. The contents of the device are irrelevant in this analysis. 8

A. A locked device's contents do not imbue an otherwise non-testimonial act of production (unlocking it) with testimonial significance. This is because unlocking it does not assert anything about what it contains. 8

B. The foregone-conclusion doctrine does not require the State to prove that the existence and/or contents of any particular file on the device is a foregone conclusion. 14

II. The Fifth Amendment analysis is unaffected by Larsen's arguments about the breadth of the search to be performed or the claimed lack of particularity in the search warrant... 18

III. The data on Larsen's phones is real and physical evidence, already in existence. Larsen can be compelled to produce it. Compelling her to use (not divulge) her knowledge of the passcode that decrypts it adds no constitutional wrinkle..... 20

CONCLUSION 30

REQUEST FOR NONORAL SUBMISSION 30

CERTIFICATE OF COMPLIANCE 31

TABLE OF AUTHORITIES

Federal Cases

Curcio v. United States, 354 U.S. 118 (1957) 21

Doe v. United States (Doe II), 487 U.S. 201 (1988) 9, 10, 11, 18, 20, 21, 23, 27, 29

Estelle v. Smith, 451 U.S. 454 (1981) 18

Fisher v. United States, 425 U.S. 391 (1976) 8, 10, 11, 15, 16, 19, 21, 25, 27, 28, 29

Gilbert v. California, 388 U.S. 263 (1967) 21

In re Search Warrant Appl. for the Cellular Telephone in United States v. Barrera, 415 F. Supp. 3d 832 (N.D. Ill. 2019) 13

Pennsylvania v. Muniz, 496 U.S. 582 (1990) 22

Schmerber v. California, 384 U.S. 757 (1966) 11

United States v. Burr, 25 F. Cas. 38 (CC Va. 1807) 12

United States v. Doe (Doe I), 465 U.S. 605 (1984) 9

United States v. Hubbell, 530 U.S. 27 (2000) 9, 10, 11, 23

United States v. Payne, 99 F.4th 495 (9th Cir. 2024) 12, 13, 28

United States v. Shvartsman, 722 F. Supp. 3d 276 (S.D.N.Y. 2024) 19, 22

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

State Cases

Commonwealth v. Davis, 220 A.3d 534 (Pa. 2019) 26

Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014) 15, 17, 28

Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019) 28

People v. Sneed, 230 N.E.3d 97 (Ill. 2023) 14, 16, 20, 28, 29

Reynolds v. State, 516 P.3d 249 (Okla. Ct. Crim. App. 2022).....20, 25, 28

State v. Andrews, 234 A.3d 1254 (N.J. 2020) 13, 20, 28

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

State v. Pittman, 479 P.3d 1028 (Or. 2021).....15, 18

State v. Stahl, 206 So.3d 124 (Fla. Dist. Ct. App. 2016).....23

State v. Valdez, 552 P.3d 159 (Utah 2023).....22, 24

Other Authorities

Wayne R. LaFave et al., 3 *Criminal Procedure* § 8.13(a) (4th ed. 2017, updated Nov. 2025).....23

Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767 (2019).....14, 16

Orin S. Kerr, *Decryption Originalism: The Lessons of Burr*, 134 HARV. L. REV. 905 (2021) 12

U.S. DEPT. OF JUSTICE, *Subject Matter Expert Working Group Reports* (June 2023), https://www.justice.gov/d9/2023-06/sme_wg_reports_combined_2.pdf 26

Gabriel Pell, *The 'Realness' Key to Compelled Passcode Production*, 115 J. CRIM. L. & CRIMINOLOGY 1 (2025)..... 21

Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203 (2018) 16, 17, 18

STATEMENT OF THE ISSUES IN THE REPLY BRIEF

I. The contents of the device are irrelevant in this analysis.

A locked device's contents do not imbue these otherwise non-testimonial acts of production (unlocking it) with testimonial significance. This is because unlocking a device does not assert anything about what it contains.

The foregone-conclusion doctrine does not require the State to prove that the existence and/or contents of any particular file on the device is a foregone conclusion.

II. The Fifth Amendment analysis is unaffected by Larsen's arguments about the breadth of the search to be performed or the claimed lack of particularity in the search warrant.

III. The data on Larsen's phones is real and physical evidence, already in existence. Larsen can be compelled to produce it. Compelling her to use (not divulge) her knowledge of the passcode that decrypts it adds no constitutional wrinkle.

RESPONSE TO APPELLEE'S ARGUMENT

Larsen's brief does not argue that the State failed to prove that her knowledge of any particular phone's passcode was a foregone conclusion. She instead says that she "has not attempted to attribute ownership of the phone to anyone else." *See* Def's Br. at 39. She also says that, if the State prevails, she will have to either comply with orders to enter the passcodes to unlock the phones or "refuse and face contempt sanctions"—or "*falsely* claim that she does not know or remember the passcode." *See id.* at 41–42 (emphasis added). Also, as far as the State can tell, she does not argue that this Court should find that the implied assertion that she knows the passcode to a particular phone has any meaningful testimonial significance, on its own (beyond arguing that the act is inherently testimonial because the passcode she would enter is "information residing in [her] mind"). *See id.* at 16–46.

Larsen insinuates foul play in how the State's brief summarized the second search warrant. *See* Def's Br. at 12. The State never denied that the second warrant, at its outer bounds, always purported to authorize officers to compel actions "revealing said security code to law enforcement, for the purposes of unlocking and keeping the . . . device in an unlocked state." *See* State's Br. at 13 (quoting D0037, Att. 3 (10/2/25, at 3). The actions it specified were always limited to applying biometrics or entering the passcode. It did

purport to authorize officers to compel a code entry in a manner "revealing said security code" to law enforcement. *See* D0037, Attachment 3, at 3. But as soon as Larsen asserted a Fifth Amendment claim in her resistance to the motion to compel, the State narrowed its ask: it urged the court to reject the Fifth Amendment claim and "order the Defendant to unlock her phones"—not to order her to reveal the passcode. *See* D0041, Reply (11/7/25). At the hearing on the motion, the State argued for an order compelling her "to enter physically the passcode into the phones" and "to open the phones," and not to "speak or write or do any of those things." *See* D0151, Transcript (11/10/25), 64:17–75:16. And its motion to reconsider emphasized: "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 2–3. It was not seeking an order compelling Larsen to enter passcodes in a way that revealed them to law enforcement—and it definitely was not seeking an order compelling her to "make an oral expression" via "orally providing the password." *See* D0044, Ruling (11/25/25), at 8–11.

Larsen might prefer to argue the unconstitutionality of an order compelling her to *reveal* the passcode. But the State's only claim on appeal is that the district court erred in not granting "what the State [was] actually requesting here—[an order compelling her to] turn over the unlocked phones

through the application of biometrics and the *physical entry* of the passcode into the device, even if the code is never disclosed to law enforcement."[1] *See* D0095, Motion, at 4–5. And nothing in Larsen's brief on appeal defeats the State's arguments that this would be a non-testimonial act of production, or (at worst) a marginally-testimonial act of production that may be compelled under the foregone-conclusion doctrine.

I. The contents of the device are irrelevant in this analysis.

Larsen argues that the contents of files on each device are "relevant to determining whether the compelled act is testimonial" and that the contents of those files must be established as a foregone conclusion. Both are incorrect.

A. A locked device's contents do not imbue an otherwise non-testimonial act of production (unlocking it) with testimonial significance. This is because unlocking it does not assert anything about what it contains.

Larsen argues "[t[he contents of the phone are relevant" in analyzing "whether the compelled act is testimonial." *See* Def's Br. at 38–40. But she acknowledges that "in *Fisher*, *Doe I*, and *Doe II*," the Court analyzed the act of production for testimonial significance "separately from the *contents* of what the compelled act produced." *Id.* at 23 (citing *Fisher v. United States*,

[1] Law enforcement can either perform the extraction immediately after Larsen unlocks the phone, or use that access to change the phone's passcode to enable decryption for extractions to be performed at some later time.

425 U.S. 391 (1976); *United States v. Doe (Doe I)*, 465 U.S. 605 (1984); and *Doe v. United States (Doe II)*, 487 U.S. 201 (1988)). Still, Larsen argues that "the cases do not stand for the proposition that the compelled act can always be divorced from the evidence it makes accessible." *See* Def's Br. at 23. She is incorrect. That is precisely what those cases say (and *Hubbell*, too).

Doe I and *Hubbell* held that the act of producing specific documents as responsive to *content-dependent* demands would carry implied (or express) assertions about the contents of those documents, as the act of identifying each document as responsive and producing it necessarily communicates a belief that its contents match the demand. *See Doe I*, 465 U.S. at 613 n.12 (testimonial significance found in act of production that would effectively require Doe to state whether "each of the myriad documents demanded by the five subpoenas in fact [was] in [his] possession or subject to his control"); *United States v. Hubbell*, 530 U.S. 27, 43 (2000) (testimonial significance found in act of "identifying the hundreds of documents responsive to the requests in the subpoena").[2] The contents of those documents didn't matter;

---

[2] Larsen argues that the State's brief misrepresents *Hubbell* by quoting from an excerpt that was "simply stating what the point of disagreement was, between the parties, in that specific case." *See* Def's Br. at 40 (citing State's Br. at 22 (quoting *Hubbell*, 530 U.S. at 40). But the disagreement was about whether "[any] testimony inherent in the act of producing those documents" had testimonial significance. That became the point of disagreement because binding precedent already made it clear to the parties—and the Court—that

the problem was that the government was attempting to compel an act that impliedly asserted *a belief about the contents* of each document produced. And in both *Fisher* and *Doe II*, the Court found the act of production lacked testimonial significance without assessing the breadth or probative value of evidence that the government would obtain, as a result. Again, that analysis stood "wholly aside from the contents of the papers produced." *See Fisher*, 425 U.S. at 409–13; *Doe II*, 487 U.S. at 215–18 (no testimonial significance in directive that "expresses no opinion" as to whether the listed evidence exists; that "executed form" did not acquire testimonial significance from the fact that it "allow[ed] the Government access to a potential source of evidence").

The takeaway is that it is only *assertions about the contents* of items to be produced that can imbue acts of production with testimonial significance, which only happens when such assertions inhere in the act of production. If the act of production makes no assertion about the produced item's contents, contents of the items produced cannot manufacture *testimonial* significance

---

"compelled testimony" could not "be found in the contents of the documents produced." *See Hubbell*, 530 U.S. at 40. Any suggestion that the State's brief misrepresented *Hubbell* wilts upon contact with the rest of the opinion. *See, e.g.*, *id.* at 37 ("Whether the constitutional privilege . . . protects the act of production itself, is a question that is distinct from the question whether the unprotected contents of the documents themselves are incriminating."); *id.* at 36 ("It is clear . . . [Hubbell] could not avoid compliance with the subpoena [at issue] merely because the demanded documents contained incriminating evidence, whether written by others or voluntarily prepared by himself.").

on their own (no matter what *evidentiary* significance they might have). That is why it is a "settled proposition that a person may be required to produce specific documents even though [those documents] contain incriminating assertions of fact or belief." *See Hubbell*, 530 U.S. at 35–36; *accord Doe II*, 487 U.S. at 215; *Fisher*, 425 U.S. at 410–11 (no testimonial significance in act of producing document that subpoena had already identified/described with specificity, "however incriminating the contents . . . might be").

Unlocking a phone makes no assertions about the data contained on it. Larsen will not be required to identify specific responsive files, nor will she be compelled to "provide the prosecutor with an accurate inventory" of the contents of any files/data as part of this act of production. *See Hubbell*, 530 U.S. at 42–43. The Ninth Circuit recently explained why unlocking a phone makes no assertions with testimonial significance about its contents:

> Payne was never compelled to acknowledge the existence of any incriminating information. He merely had to provide access to a source of potential information, just as was the case in *Doe [II]* and *Schmerber*. *See* [*Doe II*, 487 U.S. at 215]; [*Schmerber v. California*, 384 U.S. 757, 765 (1966)]. The officers were left to identify any incriminating evidence through their own investigation. This is decidedly unlike *Hubbell*, where the subpoena respondent was implicitly conceding the "existence, authenticity, and custody" of specific documents that prosecutors could use in building its case against the respondent. *Hubbell*, 530 U.S. at 41–42.
>
> One can imagine how Payne's case might alternatively fit more neatly in the *Hubbell* framework. For example, had officers somehow compelled Payne to cull through the information in his

> phone and produce any photos or videos that demonstrated his participation in fentanyl trafficking, there may have been a testimonial act of production. Turning over those photos or videos would implicitly concede that Payne had such videos, that they depicted what the officers were looking for, and that they related to his specific activities. Obviously, that is not the case here.

United States v. Payne, 99 F.4th 495, 511–12 (9th Cir. 2024). That analysis is correct and applicable here. Unlocking a phone and handing it over would make no assertion about its contents, so testimonial significance can't arise from any arguments about the contents of the files/data on that phone. [3]

At times, Larsen argues that "unlocking the phone" is testimonial because it "authenticates the content." *See* Def's Br. at 39. But she never explains how or why. Evidence that Larsen unlocked the phone does not

---

[3] Larsen challenges the State's (and Orin Kerr's) analysis of *Burr*. *See* Def's Br. at 17–18. But she admits that Chief Justice Marshall found that Willie could be compelled to testify as to whether he had present knowledge of the cipher, because "Willie's *present* knowledge of the cipher would not establish his *prior* knowledge of the letter's contents." *See id.* Correct—and so Kerr's point remains: "[i]t seems obvious that Willie's testimony could be a causal link to evidence against him," both by authenticating the letter and by incrementally contributing to an inference that he knew/understood the contents of a letter that described a treasonous plot (and kept it secret). *See* Orin S. Kerr, *Decryption Originalism: The Lessons of Burr*, 134 HARV. L. REV. 905, 952–56 (2021). But even so, the Chief Justice's holding was that even "[i]f the letter in question contain evidence of treason" and past knowledge of its contents would expose Willie to criminal liability, the court could *still* compel an answer to a question that "refers only to the present knowledge of the cipher." *See United States v. Burr*, 25 F. Cas. 38, 40 (CC Va. 1807). So the founding-era understanding of the Fifth Amendment does not support Larsen's claim that the court cannot compel her to unlock her phone because it would impliedly admit her present knowledge of the passcode.

prove that the files found on the phone are authentic. Rather, it will prove that *the passcode that she entered* is valid and authentic. *Accord Payne*, 99 F.4th at 512 (quoting *In re Search Warrant Appl. for the Cellular Telephone in United States v. Barrera*, 415 F. Supp. 3d 832, 841 (N.D. Ill. 2019)) (explaining that unlocking a locked device "does not automatically make each individual set of data" found on the device "immediately authentic"). Larsen's act of unlocking the phone, at most, impliedly asserts/admits that she presently knows the passcode. It does not assert anything about the existence, contents, or authenticity of any file it contains (even impliedly). *Accord State v. Andrews*, 234 A.3d 1254, 1274 (N.J. 2020) (explaining that the significance of entering the passcode is "limited to communicating the knowledge of the passcodes"). And it certainly does not impliedly assert the entirety of the decrypted content. *See* Def's Br. at 16–17. Per Orin Kerr:

> Some have argued that compelled decryption has broader testimonial significance because it effectively creates the evidence decrypted. The apparent thinking is that decryption causes information to exist that did not exist before, itself resembling an act of speech that adds to the testimony inherent in the act. This argument is wrong because it misses the distinction explained earlier between door-opening evidence and treasure. [*See* State's Br. at 52–53.] To be sure, the treasure revealed by door-opening can be extremely incriminating speech. It might include a signed confession. It might contain video of the defendant committing the crime. The door-opening may make that evidence exist in a way it did not exist in encrypted form. But all of this is irrelevant to the privilege against self-incrimination. The act of production doctrine

> considers the actor's communication implicit in the act . . . . How incriminating the treasure may be, or what the computer does when a person opens the door, does not change the testimony implicit in the door-opening act.

Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 779–81 (2019); *accord People v. Sneed*, 230 N.E.3d 97, 115–18 (Ill. 2023) (explaining "any information that may be found on the phone after it is unlocked is irrelevant" to the act-of-production analysis and the foregone-conclusion analysis, because entering a passcode only "implicitly asserts that defendant is able to unlock the phone" and that "the passcode [entered] is authentic"—not that data it contains is authentic).

None of Larsen's arguments can establish that the act of entering the passcode to unlock the device has testimonial significance beyond (at best) impliedly asserting that she knows the passcode that unlocks that device.

B. The foregone-conclusion doctrine does not require the State to prove that the existence and/or contents of any particular file on the device is a foregone conclusion.

Larsen argues that this "is a far cry from *Fisher*" because in *Fisher*, "the Government knew that the specific documents they sought existed"—as opposed to this case, where the State "seeks to force Larsen to declare what specific files are on her phone." *See* Def's Br. at 37–38. But that is not what the State sought to compel. Entering the passcode and unlocking the device makes no such declaration. The State will search the phone for itself,

and it will discover and prove the contents of the phone without reference to any statement (express or implied) from Larsen.[4] The act of entering the passcode to unlock each device only (at most) impliedly asserts that Larsen knows the correct passcode to unlock that device. So *that* is the only fact that the State must prove is already a foregone conclusion, under *Fisher*.

It is hard to find the rationale for Larsen's claim that "this Court needs to consider the contents of Larsen's phone in order to engage in the proper foregone conclusion analysis." *See* Def's Br. at 38. In *Fisher*, the government did not need to prove it knew what the documents would reveal. Indeed, the claim of attorney-client privilege was premised on the notion that there was still-private information in those documents—information which the Court thought would have "unquestionable relevance to the tax investigation." *See Fisher*, 425 U.S. at 401–05 & n.7. The foregone-conclusion doctrine would be all but useless if it could only be used to compel production of cumulative evidence. Fortunately, *Fisher* draws a distinction between assertions implied by the compelled act of production (what Kerr calls "door-opening evidence") and the evidence to be produced (what Kerr calls "treasure"). *See, e.g.*, *id.* at

---

[4] It will also prove the facts that connect Larsen to that data, without using her entry of a valid passcode as evidence. *See, e.g.*, *Pittman*, 479 P.3d at 1046 (prohibiting use of compelled act of production as evidence to prove ownership, in part because "judicial estoppel" applied to the State's position on foregone conclusion); *Gelfgatt*, 11 N.E.3d at 617 n.16 (similar limitation).

409 (explaining that "however incriminating the contents . . . might be," their production can be ordered via a subpoena does not "compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought"); *id*. at 410–11 (finding that "[c]ompliance with the subpoena tacitly concedes the existence of the papers and their possession or control by the taxpayer," then explaining a court may order that compliance because "[t]he existence and location of the papers"—not their contents—"are a foregone conclusion"); Kerr, *Compelled Decryption*, 97 TEX. L. REV. at 777–78.

At one point, Larsen's brief cites Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 209 (2018) for the proposition that *Sneed* "misapplied the doctrine" by "applying [it] to the passcode itself, rather than the contents of the phone." *See* Def's Br. at 34–35; *Sneed*, 230 N.E.3d at 118. Sacharoff's argument is:

> The act of entering the password is analogous to the act of physically handing over documents in the physical world. In neither instance does the foregone conclusion doctrine apply solely to that act; rather, it applies to the papers produced. In the physical world, the court asks whether it is a foregone conclusion that the papers produced exist and are in the defendant's possession, not whether the defendant is physically capable of producing the documents.
>
> In the password context, . . . the act of entering the password, like the act of physically handing over documents, produces the underlying documents on the device. . . .
>
> Some courts insist that if we know the person possesses the device, it is a foregone conclusion that the person possesses the

> items on the device, whatever they turn out to be. [FN: *United States v. Spencer*, No. 17-CR-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018).] But the government must show *before* the production that the person possesses the particular documents because, otherwise, it is the very production that shows possession.

Sacharoff, *Unlocking*, 87 FORDHAM L. REV. at 236–37. The problem with that analysis is that inputting the passcode is not analogous to finding and handing over documents in the physical world (which, as in *Fisher*/*Hubbell*, makes an implied assertion about existence/possession of each document). Larsen will never physically hand over any particular file and thereby admit its existence, nor will Larsen ever complete any physical act of "production that shows possession." *See id.*; *accord Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 615 & n.14 (Mass. 2014). The State already possesses these phones and the data on each phone's hard drive (currently encrypted). The act of entering the passcode that decrypts a specific device makes no assertions about what that data will say, when decrypted—just as providing a key that opens a door makes no assertions about what investigators will find after they open it.

Indeed, as Sacharoff notes, entering the passcode to decrypt a device leaves open the possibility "that the device contains no documents at all"—passcode-encrypted, but otherwise factory-fresh. *See id.* at 236 n.214. In the moments after Larsen completes the compelled act of production, the State will not know anything about the phone's contents—because Larsen's act of

entering the correct passcode won't have asserted or communicated any fact or belief about the contents of that now-decrypted and now-accessible data. Just like in *Doe II*, the compelled act "allows the [State] access to a potential source of evidence," but that act "itself does not point the [State] toward" any particular bit of data it might use "or otherwise provide information that will assist the prosecution"—it is still the State who "must locate that evidence 'by the independent labor of its officers'" who examine that data. *See Doe II*, 487 U.S. at 215–16 (last excerpt quoting *Estelle v. Smith*, 451 U.S. 454, 462 (1981)). Or, as Larsen has put it: "once unlocked, the phone will be searched for the incriminating evidence [the State] seeks"—and Larsen's act of unlocking it won't have told officers anything about where to find it or what it might be. *See* Def's Br. at 39. It is only "[t]he testimonial aspects of the act [that] have constitutional significance"—and "the access that the act provides does not." *See State v. Pittman*, 479 P.3d 1028, 1046–47 (Or. 2021). None of Larsen's arguments about the contents of the phone can overcome that analysis.

II. The Fifth Amendment analysis is unaffected by Larsen's arguments about the breadth of the search to be performed or the claimed lack of particularity in the search warrant.

Larsen block-quotes the search warrant application and argues that it "failed to describe, with any amount of particularity whatsoever, what exactly it was seeking to obtain from [her] phone." *See* Def's Br. at 42–44. But that

is a Fourth Amendment challenge to the validity of the search warrant (one that was not raised or argued below). It is Larsen who "conflates two distinct constitutional provisions." *See id.* at 42. And nothing in Larsen's brief puts any dent in the State's analysis that established error in the district court's ruling that Larsen could not be compelled to unlock her phone because of a Fifth Amendment interest in "the right of each individual to a private enclave where he may lead a private life." *See* D0044, Ruling, at 10 (quoting *United States v. Shvartsman*, 722 F. Supp. 3d 276, 320 (S.D.N.Y. 2024)); *cf.* State's Br. at 49–51. *Fisher* expressly and thoroughly disavowed the notion that the Fifth Amendment was "a general protector of privacy" that overlapped with the Fourth Amendment. *See Fisher*, 425 U.S. at 400–01. There is no way to defend the district court's ruling as consistent or reconcilable with *Fisher*.

The act of unlocking a lockbox to enable a search of its contents does not vary in testimonial significance based on the size of the box or the scope of the search to be performed. The act of unlocking a door to enable a search of a house or room does not vary in its testimonial significance based on the square footage of the space beyond the door or the wording of the warrant that authorizes the ensuing search of the premises. "Likewise, the testimony implicit in the act of entering the passcode to a cell phone [or other device] is the same, regardless of the phone's capacity." *See Sneed*, 230 N.E.3d at 117.

Arguments that the breadth of a search is relevant "confuse one's protections under the Fourth Amendment with those of the Fifth Amendment." *Reynolds v. State*, 516 P.3d 249, 254 (Okla. Ct. Crim. App. 2022). And they disregard "the stark distinction the Court has drawn between the evidentiary object and [the act of] production—a division reinforced even in those cases where the foregone conclusion exception was held not to apply." *See Andrews*, 234 A.3d at 1266–69 & 1274. The act of production is entering the passcode to unlock each phone; the testimonial significance of that act is assessed by reference to whether it "communicates any factual assertions, implicit or explicit, or conveys any information." *See Doe II*, 487 U.S. at 214–15. The scope or breadth of any "access to a potential source of evidence" that results is irrelevant. *Id.*

III. The data on Larsen's phones is real and physical evidence, already in existence. Larsen can be compelled to produce it. Compelling her to use (not divulge) her knowledge of the passcode that decrypts it adds no constitutional wrinkle.

There is a critical distinction between an act of production that requires a defendant to *communicate* knowledge or *divulge* the contents of her mind (which tends to be testimonial) and an act of production which only requires her to "use knowledge residing in her mind" to complete the act, without ever divulging that knowledge to the State (which could only be testimonial in the sense that it impliedly reveals that she *has* that knowledge). *See* Def's Br. at 23–24; *Doe II*, 487 U.S. at 211 (quoting *Curcio v. United States*, 354 U.S. 118,

128 (1957)) (explaining that the privilege prohibits an effort to force a person "to disclose the contents of his own mind"). The fact that a compelled act of production requires some *use* of thought processes or mental faculties is not enough to make it testimonial (and is analytically irrelevant). A person must always use their mind "to some extent every time they produce evidence." *See* Gabriel Pell, *The 'Realness' Key to Compelled Passcode Production*, 115 J. CRIM. L. & CRIMINOLOGY 1, 19 (2025). For example, a handwriting exemplar requires the suspect to use (and demonstrate) his knowledge of how to draw P's and Q's—but that use of mental faculties lacks inherent significance, and it does not change the reality that "nothing he has *said or done* is deemed to be sufficiently testimonial for purposes of the privilege." *Fisher*, 425 U.S. at 411 (emphasis added); *Gilbert v. California*, 388 U.S. 263, 266–67 (1967).

Thus, Larsen is correct when she states "[t]he relevant inquiry is what the act communicates, not how much mental effort it takes to perform it." *See* Def's Br. at 38–39. But this means that Larsen can be compelled to unlock her phones, because that act of production only communicates (at most) that she knows the passcodes; it does not reveal or divulge any other thought.

> The Government need not compel the suspect to reveal the contents of his mind by divulging a passcode or cross the line drawn in *Doe* and *Hubbell*. Consistent with those cases, the Government can instead "ask or seek to compel the suspect to turn over an unlocked phone . . . through entering the passcode themselves without providing the passcode to police."

See Shvartsman, 722 F. Supp. 3d at 319–20 (quoting *State v. Valdez*, 552 P.3d 159, 168 (Utah 2023)); *accord Andrews*, 234 A.3d at 1274.

Larsen agrees that the Fifth Amendment "does not protect [her] from being compelled by the State to produce 'real or physical evidence.'" *See* Def's Br. at 45 (quoting *Pennsylvania v. Muniz*, 496 U.S. 582, 589 (1990)). But she contends that this principle does not apply here, because "[t]he passcode is information residing in [her] mind," and that code "is not 'real' or physical evidence in the same sense as a key." *See id.* But *the data on her phones* is the real/physical evidence that the State is trying to compel her to produce. It already exists in the form of stored data, locked behind an encryption gate. Larsen is claiming a constitutional right to refuse to provide access to that real/physical evidence, despite a judicial warrant authorizing that access—solely because the "key" is an action that she would need to perform using her knowledge of a particular string of digits, rather than a physical object that she could simply insert or hand over. *See, e.g.*, *id.* at 37.

Larsen attacks the State for advancing "a formal distinction between a defendant disclosing a passcode and physically entering it." *See id.* at 40. But she is advancing her own formalistic distinction: "that the Fifth Amendment should provide greater protection to individuals who passcode protect their iPhones with letter and number combinations than to individuals who use

their fingerprint [or another biometric/physical item] as the passcode." *See State v. Stahl*, 206 So.3d 124, 135 (Fla. Dist. Ct. App. 2016); *accord* Def's Br. at 30–32 (arguing that "[a] passcode is fundamentally different" from a key or a biometric identifier).[5] One advantage of the State's approach is that it is faithful to the distinctions drawn in *Hubbell* and *Doe II*, between "telling an inquisitor the combination to a wall safe [and] being forced to surrender the key to a strongbox." *See Hubbell*, 530 U.S. at 43 (citing *Doe II*, 487 U.S. at 210 n.9); *see also* Wayne R. LaFave et al., 3 *Criminal Procedure* § 8.13(a) (4th ed. 2017, updated Nov. 2025) (surveying pertinent cases and concluding that "to require the subpoenaed party to reveal a passcode" would "require a testimonial communication standing apart from the act of production," and thus falls on the wrong side of the classic distinction "between producing a key to a lockbox and revealing a password"); *accord Valdez*, 552 P.3d at 168 (observing that "functionally, there may not be much real-world difference between . . . speaking or writing out a passcode for the police and physically providing an unlocked device to the police"—but "the two scenarios present

---

[5] Larsen's brief discusses *State v. Diamond*, but misses Footnote 8—*Diamond's* explanation of the alternative basis for its holding, which the State block-quoted as the basis for its argument about how *that* rationale would apply with equal force to compelled entry of passcodes. *See* Def's Br. at 30–32; State's Br. at 23–24 (quoting *State v. Diamond*, 905 N.W.2d 870, 877 & n.8 (Minn. 2018)). The State's claim is analytically sound.

distinct issues under the Fifth Amendment" because the first is "testimony" and the latter is only an act of production, which may be non-testimonial).

Another advantage of the State's approach is that prevents a trove of real/physical evidence from becoming "warrant-proof" if a device's owner (or manufacturer) encrypts it with a special kind of lock. *See* State's Br. at 51–55. Larsen's response is to argue that this "is a problem the State must solve through its own investigative efforts"—and it should have "established that the existence, possession or control, [and] authenticity" of particular files on her phone "were already known." *See* Def's Br. at 46. But this just proves the State's point. Under Larsen's approach, the State can't enforce a warrant to extract/search any file from a password-protected device unless it already knows the actual contents of that particular file (at whatever level of proof is required for a foregone conclusion, beyond the probable-cause showing that the Fourth Amendment requires for issuance of a search warrant). So law enforcement loses access to search warrants that could enable a *search* to uncover new evidence in furtherance of active investigations. Anything that is non-cumulative (even when police know it *must* exist, but currently lack information that would enable them to fully describe its content) now sits within "impenetrable enclaves" for that real/physical evidence—beyond the reach of the law and the courts. *See Reynolds*, 516 P.3d at 254. And so

Boyd rises and eclipses *Fisher*—despite *Fisher*'s express disavowal of *Boyd*. *See Fisher*, 425 U.S. at 405–09 (dissecting and overruling *Boyd*'s holding that "a compulsory production of the private books and papers of the owner . . . is compelling him to be a witness against himself, within the meaning of the Fifth Amendment," and describing it as "a rule searching for a rationale consistent with the proscriptions of the Fifth Amendment against compelling a person to give 'testimony' that incriminates him"). And communities suffer real-world consequences as investigations into criminal networks wither on the vine (notwithstanding the showing of probable cause that should enable the seizure of real/physical evidence as the next investigative step).

> [T]he investigation and prosecution of crime are thwarted when we cannot access the contents of a hard drive or a smart phone, even with a lawful court order or search warrant issued only after a neutral judge has determined there is probable cause that the hard drive or phone contains evidence of a crime. . . . Most significantly, victim identification and rescue are rendered impossible even if it is known that [CSAM] images or videos that could lead to that rescue reside on the device.

U.S. DEPT. OF JUSTICE, *Subject Matter Expert Working Group Reports* (June 2023), https://www.justice.gov/d9/2023-06/sme_wg_reports_combined_2.pdf. This is neither hypothetical nor speculative. This was the actual outcome in *Davis*, which Larsen has urged this Court to follow: officers knew that Davis's IP address "utilize[ed] a peer-to-peer file sharing network to share videos depicting child pornography," and they had viewed one such

CSAM video that was known to be on Davis's computer—but they were still barred from compelling Davis to decrypt the drive and produce its contents because that "could lead to a trove of a presently unknown number of files," the exact names/location/contents of which were impossible to discern and impossible to prove while the drive remained encrypted. *See Commonwealth v. Davis*, 220 A.3d 534, 551 n.9 (Pa. 2019). And so it would go, even when a suspect voluntarily admits to police that "he knew the password"—even then, all non-cumulative incriminating evidence becomes warrant-proof (despite his admission to the singular fact that the act of entering that passcode would impliedly assert, making that fact a foregone conclusion). *See id.* at 539.

Luckily, the Fifth Amendment does not require that noxious outcome, where "one weird trick" can put any real/physical evidence beyond the reach of the law and the court. Under *Fisher*, a suspect "cannot avoid compliance with [a lawful order] merely by asserting that the item of evidence which he is required to produce contains incriminating writing, whether his own or that of someone else." *See Fisher*, 425 U.S. at 409–10. An act of production is only testimonial to the extent that it "has communicative aspects of its own, wholly aside from the contents of the papers produced." *See id.* If it doesn't require the subject to "restate, repeat, or affirm" anything about "contents of the documents sought," then those contents are irrelevant to the analysis

on the Fifth Amendment issue—and they cannot make the act of production testimonial or privileged, "however incriminating [they] might be." *See id.* at 410–11; *Doe II*, 487 U.S. at 209–10 & n.8 (rejecting attempt to limit *Fisher* to its facts, and noting its "principles were articulated in general terms" about "when the privilege applies" to any acts of production, regardless of form). Moreover, the foregone-conclusion doctrine only requires a showing that "the tacit averments" that inhere in the act of production *itself* are already "a foregone conclusion"—so when the act of production makes no assertions about the contents of the evidence produced, the State need not prove that it already knows every detail about the contents of evidence that its search will uncover and examine. *See Fisher*, 425 U.S. at 409–11. And so the proper constitutional balance is struck: the Fifth Amendment privilege prohibits an order to perform an act with (live) testimonial significance, but it cannot be invoked "loose from the moorings of its language" to make all encrypted data effectively warrant-proof, even when the acts that would produce that data lack any meaningful testimonial significance. *See id.* at 401; *accord Sneed*, 230 N.E.3d at 115–20; *Andrews*, 234 A.3d at 1273–75; *Pittman*, 479 P.3d at 1046–47; *Reynolds*, 516 P.3d at 253; *Commonwealth v. Jones*, 117 N.E.3d 702, 710–11 & n.9–n.10 (Mass. 2019) (citing *Gelfgatt*, 11 N.E.3d at 613–16); *Payne*, 99 F.4th at 511–12.

* * *

The State's brief established error in the district court's ruling that denied its motion to compel. Even if the district court was correct to hold that Larsen could not be compelled to *reveal* the passcodes, it erred in not granting the more limited request that it order her to *enter* the passcodes to put the phones into their unlocked state. *See* D0095, Motion, at 4–5. That act of production (at most) will only imply that she knows the passcodes to unlock the phones. It will not assert anything about any phone's contents. That means two things: (1) the evidentiary significance of that data is not relevant in assessing the testimonial significance of the act of production; and (2) the foregone-conclusion doctrine only requires the State to prove that it can already establish *Larsen's knowledge of that phone's passcode*—it need not prove that it can already establish any fact about the data/files that the phone contains. This is not about privacy—the breadth and scope of any search implicate the Fourth Amendment, not the Fifth Amendment (and they don't change the degree to which the act of unlocking the phone, in itself, has testimonial significance). *See Fisher*, 425 U.S. at 400–01; *Sneed*, 230 N.E.3d at 117. Larsen has no constitutional right to make real/physical evidence "warrant-proof" and place it beyond the reach of judicial process by locking it up and claiming that unlocking it would be a testimonial act—

not because it would admit that she has the key, but because of the content of the evidence that the State would find within, upon searching it for itself. *See Doe II*, 487 U.S. at 215–18. The district court erred in ruling otherwise, and this Court should reverse that ruling and remand with instructions to issue an order compelling Larsen to enter passcodes to unlock the devices that contain data that the warrant authorized officers to search and seize.

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 **6,333** words, excluding the parts of the brief exempted by Iowa R. App. P. 6.903(1)(g)(1).

Dated: September 16, 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