

No. 17-7387

---

---

IN THE SUPREME COURT OF THE UNITED STATES

---

JOHN DOE, PETITIONER

v.

UNITED STATES OF AMERICA

---

ON PETITION FOR A WRIT OF CERTIORARI  
TO THE UNITED STATES COURT OF APPEALS  
FOR THE THIRD CIRCUIT

---

BRIEF FOR THE UNITED STATES IN OPPOSITION

---

NOEL J. FRANCISCO  
Solicitor General  
Counsel of Record

JOHN P. CRONAN  
Acting Assistant Attorney General

FRANCESCO VALENTINI  
Attorney

Department of Justice  
Washington, D.C. 20530-0001  
SupremeCtBriefs@usdoj.gov  
(202) 514-2217

---

---

## QUESTIONS PRESENTED

1. Whether petitioner's failure to object to a magistrate judge's order directing him to decrypt certain electronic devices precluded him from challenging the validity of the decryption order in subsequent civil contempt proceedings.

2. Whether the court of appeals correctly determined that the magistrate judge did not plainly err in concluding that the decryption order did not violate petitioner's Fifth Amendment privilege against self-incrimination.

IN THE SUPREME COURT OF THE UNITED STATES

---

No. 17-7387

JOHN DOE, PETITIONER

v.

UNITED STATES OF AMERICA

---

ON PETITION FOR A WRIT OF CERTIORARI  
TO THE UNITED STATES COURT OF APPEALS  
FOR THE THIRD CIRCUIT

---

BRIEF FOR THE UNITED STATES IN OPPOSITION

---

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. A1-A19) is reported at 851 F.3d 238. The orders of the district court finding petitioner in civil contempt (Pet. App. D1) and explaining the reasons for that finding (Pet. App. E1-E6) are unreported.

JURISDICTION

The judgment of the court of appeals was entered on March 20, 2017. A petition for rehearing was denied on July 28, 2017 (Pet. App. B1-B2). On October 16, 2017, Justice Alito extended the time within which to file a petition for a writ of certiorari to and including November 27, 2017, and the petition was filed on that

date. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

#### STATEMENT

Following a hearing in the United States District Court for the Eastern District of Pennsylvania, petitioner was found in civil contempt for failing to comply with a magistrate judge's order requiring him to decrypt certain electronic devices. The court of appeals affirmed. Pet. App. A1-A19.

1. During a child-pornography investigation, detectives from Delaware County, Pennsylvania executed a search warrant at petitioner's residence. They seized several electronic devices, including an Apple iPhone, a computer, and two external hard drives. Pet. App. A3. All of the devices had been protected with encryption software. Id. at A3-A4; Gov't C.A. Br. 4-5. Petitioner provided the password for the iPhone, but refused to decrypt the computer or the external hard drives. Pet. App. A4-A5; Gov't C.A. Br. 4.

Forensic analysts later discovered the password to decrypt the computer hidden on the iPhone. Pet. App. A4. A forensic examination of the computer revealed that it had been used to visit websites with titles indicative of child exploitation, such as "toddler\_cp," "tor-childporn," and "pthc." Id. at A4-A5.<sup>1</sup> The

---

<sup>1</sup> The acronym "cp" stands for child pornography; "pthc" stands for "preteen hardcore." Pet. App. A5 n.2.

examination further revealed that petitioner had accessed or attempted to access more than 20,000 files with names indicative of child pornography and that he had used the external hard drives to store the files. Ibid. Although the investigators could not view the images on the still-encrypted hard drives, they confirmed that the files petitioner had requested matched known images of child pornography. Id. at A5.<sup>2</sup> The analysts also confirmed that petitioner had successfully downloaded the images and transferred them to the external hard drives. Ibid.; see Gov't C.A. Br. 6-7.

Delaware County detectives interviewed petitioner's sister, who told them that he had unlocked the computer in her presence, Gov't C.A. Br. 7-8, and shown her hundreds of images of child pornography stored on the encrypted external hard drives, Pet. App. A5-A6. She also advised that petitioner had obtained a new cell phone shortly after the seizure of his electronic devices. Gov't C.A. Br. 8.

By the time petitioner's sister was interviewed, Philadelphia police officers had seized petitioner's new cell phone, another iPhone. Gov't C.A. Br. 8. At a family "intervention," petitioner had admitted taking sexually suggestive photos of his nieces and agreed to unlock his new phone and turn it over to his family.

---

<sup>2</sup> The analysts confirmed the match using "hash" values, which are the result of algorithms that calculate "a unique value" for an image or other set of data. Pet. App. A5 n.3 (citation omitted).

Id. at 8-9. On the phone, petitioner's family members found a video of petitioner's four-year-old niece in bed wearing only underwear. Id. at 9. The video focused on the child's genital area. Ibid. The family also found 15 to 25 pictures of petitioner's six-year-old niece, taken at an angle where the camera was aimed underneath her dress. Ibid. The family called the Philadelphia police, and officers confirmed the existence of the video and photographs when they seized the still-unlocked phone. Id. at 9-10.

A subsequent forensic examination of petitioner's new iPhone revealed that he had set up additional layers of encryption, which had by then locked. Gov't C.A. Br. 10. The video and photos of petitioner's nieces were not accessible on the unencrypted portion of the device, and petitioner refused to grant access to the encrypted areas. Ibid.; see Pet. App. A6.

2. Federal investigators invoked Federal Rule of Criminal Procedure 41 to obtain a warrant authorizing a search of petitioner's encrypted devices. Pet. App. A6. A magistrate judge then issued an order pursuant to the All Writs Act, 28 U.S.C. 1651, requiring petitioner to "produce the Apple Mac Pro computer, two attached external hard drives, and iPhone 6 cell phone to the Government in a fully unencrypted state." C.A. App. 3; see Pet. App. A6. Petitioner filed a motion to quash, arguing that

compelling him to decrypt the devices violated his Fifth Amendment privilege against self-incrimination. Pet. App. A6.

The magistrate judge denied the motion. Pet. App. C1. The judge concluded that, under this Court's "foregone conclusion" doctrine, "any testimonial aspect" of petitioner's act of decrypting the devices was not protected by the Fifth Amendment because the government already had the devices and knew that they contained child pornography. Id. at C1 n.1; see Fisher v. United States, 425 U.S. 391, 411 (1976) (finding that a taxpayer's production of his accountant's workpapers in response to a subpoena would not be protected by the Fifth Amendment because "[t]he existence and location of the papers [we]re a foregone conclusion").

The magistrate judge directed petitioner to comply with the decryption order within one week. Pet. App. C1. The judge's order also advised that "[a]ny party may file objections to this Order" with the district court and that "[f]ailure to file timely objections may constitute a waiver of any appellate rights." Id. at C2 n.1. Petitioner did not file an objection. Id. at A6.

3. A week later, petitioner appeared for the court-ordered forensic examination of his devices. Pet. App. A7. Because the decryption order compelled him only to decrypt the devices -- not to disclose his passwords -- he was given a private space to enter the passwords so they would not be revealed to law enforcement

officers. Gov't C.A. Br. 11; C.A. App. 136-137. Petitioner produced his new iPhone in unencrypted form, but asserted that he had forgotten the passwords for his hard drives. Pet. App. A7.

Believing that petitioner was lying, the government filed a motion for an order to show cause why he should not be held in contempt for willfully disobeying the decryption order. Pet. App. A7. At a hearing before the magistrate judge, petitioner did not testify or offer evidence. The judge found that petitioner's claimed failure of memory was a "deliberate ruse" and that he had intentionally disobeyed the decryption order. C.A. App. 9. The judge ordered petitioner to appear before the district court to show cause why he should not be held in contempt. Id. at 6.

4. The district court held a de novo hearing. Pet. App. D1. The government called four witnesses, who established petitioner's failure to comply with the decryption order and the circumstances suggesting that his claimed failure of memory was a pretext to avoid revealing the large quantity of child pornography stored on his hard drives. Id. at E3-E5. Petitioner "did not testify or call any witnesses," "did not offer any documentary or physical evidence," and "offered no on-the-record explanation for his present failure to comply" with the order. Id. at E5. Petitioner also did not argue at the hearing that order violated his Fifth Amendment privilege against self-incrimination. Id. at A13.



The district court held petitioner in civil contempt. Pet. App. E6. It found that the government had discharged its initial burden of showing petitioner's noncompliance with the decryption order. Id. at E4-E5. The court further found that, "[i]n the absence of any explanation from [petitioner], the Government's prima facie showing of contempt satisfie[d] [its] burden of proof." Id. at E5. The court advised petitioner that he would be taken into custody, but that he could purge himself of the contempt at any time by complying with the order. Ibid. The court then afforded petitioner time to consult with his attorney. Ibid. Petitioner again refused to comply and was transferred to the custody of the United States Marshal. Id. at E5-E6.

5. The court of appeals affirmed the finding of civil contempt. Pet. App. A1-A19. As relevant here, the court first observed that petitioner had failed to object to the magistrate judge's order rejecting his Fifth Amendment challenge to the decryption order despite the warning that such a failure could waive his appellate rights. Id. at A13.<sup>3</sup> The court also noted that "it is generally the case that 'a contempt proceeding does not open to reconsideration the legal or factual basis of the order

---

<sup>3</sup> The court of appeals separately rejected petitioner's contention that the magistrate judge had lacked subject matter jurisdiction to issue the decryption order. Pet. App. A9-A13. Petitioner does not renew that contention before this Court.

alleged to have been disobeyed.'" Id. at A13-A14 (citation omitted).

The court of appeals further stated that "[e]ven if [it] could assess the Fifth Amendment decision of the Magistrate Judge, [its] review would be limited to plain error" because petitioner "did not renew [his] self-incrimination claim during the contempt proceedings." Pet. App. A13-A14. The court then devoted the balance of its opinion to explaining why petitioner's Fifth Amendment challenge failed under the "deferential" plain-error standard. Id. at A14.

The court of appeals noted that although the Fifth Amendment does not allow a defendant to refuse to produce documents merely because they are incriminating, it may be implicated when "[t]he act of producing evidence \* \* \* has communicative aspects of its own, wholly aside from the contents of the papers produced." Pet. App. A14 (quoting Fisher, 425 U.S. at 410). The court recognized, for example, that responding to a subpoena may implicitly assert that the requested documents exist, are in the person's possession, and are authentic. Id. at A15. But the court observed that the implicit assertions associated with producing evidence are not protected by the Fifth Amendment when they have no (or only negligible) testimonial value. Ibid. In particular, it explained that under the "'forgone conclusion' rule" articulated by this Court in Fisher, the Fifth Amendment does not protect an act of

production where “any potentially testimonial component of [that act] -- such as the existence, custody, and authenticity of evidence -- is a ‘forgone conclusion’ that ‘adds little or nothing to the sum total of the Government’s information.’” Ibid. (quoting Fisher, 425 U.S. at 411).

The court of appeals observed that although it had not previously considered the application of the foregone-conclusion doctrine to the compelled decryption of electronic devices, the Eleventh Circuit had considered the issue in In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335 (2012). Pet. App. A15. Under the circumstances presented there, the Eleventh Circuit had concluded that the implicit factual communications associated with decrypting the devices at issue were not foregone conclusions -- and that the decryption order therefore violated the Fifth Amendment -- because the government had not shown with “reasonable particularity” the basis for its belief “that encrypted files exist[ed] on the drives, that [the suspect] ha[d] access to those files, or that he [wa]s capable of decrypting the files.” 670 F.3d at 1349; see Pet. App. A16.

In this case, in contrast, the court of appeals determined that the record established, among other things, that the government already knew that petitioner had “possessed, accessed and owned” the devices at issue and that “there are images on the electronic devices that constitute child pornography.” Pet. App.

A16. Under those circumstances, the court found that the magistrate judge "did not commit a clear or obvious error" in concluding that "any testimonial component of the production of decrypted devices added little or nothing to the information already obtained by the Government." Id. at A17.

In finding no plain error on the facts of this case, the court of appeals emphasized that it was not holding that "the Government's knowledge of the content of the devices is necessarily the correct focus of the 'foregone conclusion' inquiry in the context of a compelled decryption order." Pet. App. A17 n.7 (emphasis added). To the contrary, the court recognized that "a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production." Ibid. The court noted that in this case, the testimony that would be implicit in petitioner's act of decrypting his hard drives would simply be that "I, [petitioner], know the password for these devices," not anything about what the devices contain. Ibid. But the court explained that because its review was "limited to plain error" -- and because the government knew both that petitioner had the password to the hard drives and that the drives contained child pornography -- it was not required to decide the proper focus of the foregone-conclusion analysis. Id. at A18 n.7.

## ARGUMENT

Petitioner contends that the court of appeals erred in finding his claim to be procedurally foreclosed (Pet. 12-14) and in determining that the claim lacked merit (Pet. 15-29). The court of appeals' decision is correct and does not conflict with any decision of this Court or another court of appeals. No further review is warranted.

1. Petitioner first contends (Pet. 12-14) that the court of appeals erroneously determined that his failure to object to the magistrate judge's orders precluded appellate review of his Fifth Amendment claim. That contention does not warrant this Court's review.

a. Petitioner's contention that he was free to forgo district-court review of the magistrate judge's order rests on an unsound premise. Federal magistrate judges are non-Article III judges who function as "adjuncts" to Article III district courts. Northern Pipeline Constr. Co. v. Marathon Pipe Line Co., 458 U.S. 50, 78-79 (1982) (plurality opinion) (citing United States v. Raddatz, 447 U.S. 667 (1980)). The Federal Magistrates Act, 28 U.S.C. 636, expressly specifies the standards for district-court review of certain actions by magistrate judges. See 28 U.S.C. 636(b)(1). Petitioner appears to acknowledge (Pet. 13-14) that a party may be required to object to a magistrate judge's action on

a matter addressed in Section 636(b)(1) in order to preserve an issue for appeal. See Thomas v. Arn, 474 U.S. 140, 155 (1985).

Petitioner contends (Pet. 13-14), however, that "[a] party is only ever required to seek reconsideration" by a district court when a magistrate judge acts under Section 636(b)(1), and never when a magistrate judge acts as an adjunct to the district court under another provision of the Federal Magistrates Act. Petitioner therefore maintains (Pet. 13) that he "was not required to seek reconsideration" in this case because the magistrate judge issued the decryption order (and denied petitioner's motion to quash) under Section 636(b)(3), which provides that "[a] magistrate judge may be assigned such additional duties as are not inconsistent with the Constitution and laws of the United States."

Petitioner's argument that he was not required to object to the magistrate judge's order appears to rest on the assumption that, notwithstanding the order's statement that "[a]ny party may file objections," Pet. App. C2 n.1, he had no available procedure by which to object because the magistrate judge acted under Section 636(b)(3). That assumption is incorrect. Although Section 636 and the applicable local rules do not expressly address review of a magistrate judge's actions under Section 636(b)(3), the Third Circuit has determined that, "[t]o preserve the adjudicatory role of Article III judges, matters referred under [S]ection 636(b)(3) [are] subject to review" by district courts. NLRB v. Frazier, 966

F.2d 812, 816 (1992).<sup>4</sup> Indeed, the Eastern District of Pennsylvania decision on which petitioner relies (Pet. 13) was itself reviewing a magistrate judge's order issued "under 28 U.S.C. § 636(b)(3)" following an objection by one of the parties. In re Search Warrant No. 16-960-M-1 to Google, 275 F. Supp. 3d 605, 608 n.4 (2017). Petitioner, too, could have filed such an objection with the district court. And he does not explain why he should be permitted to challenge the decryption order in contempt proceedings despite his failure to pursue that avenue of review.

b. Petitioner does not contend that the court of appeals' discussion of his failure to object to the magistrate judge's orders implicates any disagreement among the circuits. Indeed, he does not cite any decision holding that a party may forgo district-court review of such an order while still preserving the ability to challenge its validity in contempt proceedings. That issue thus does not satisfy this Court's traditional certiorari standards. See Sup. Ct. R. 10.

c. In any event, this case would be a poor vehicle for reviewing the first question that petitioner seeks to raise even

---

<sup>4</sup> Other courts of appeals have likewise concluded that "a magistrate judge exercising 'additional duties' jurisdiction [under Section 636(b)(3)] remains constantly subject to the inherent supervisory power of the district judge and the judge retains the 'ultimate responsibility for decision making in every instance.'" Colorado Bldg. & Const. Trades Council v. B.B. Andersen Const. Co., 879 F.2d 809, 811 (10th Cir. 1989) (citation omitted); see, e.g., In re United States, 707 F.3d 283, 289 (4th Cir. 2013).

if that question otherwise warranted this Court's review. To the extent that the court reached a definitive conclusion on the issue at all, see Pet. App. A13-A14 & n.6, it was at most an alternative holding, because the court proceeded to review -- and reject -- petitioner's Fifth Amendment argument on the merits. Id. at A14-A19. The court's judgment thus did not rest solely on its observations about the potential implications of petitioner's failure to object to the magistrate judge's orders.

2. Petitioner also renews his contention (Pet. 15-29) that the decryption order violated his Fifth Amendment privilege against self-incrimination. That argument lacks merit. And because petitioner did not raise his Fifth Amendment claim during the contempt proceedings, the court of appeals determined only that he was not entitled to relief under the deferential plain-error standard. That narrow conclusion does not conflict with any decision of this Court or another court of appeals, and the plain-error posture -- along with the court of appeals' potential alternative waiver holding -- would make this case an unsuitable vehicle in which to consider the second question presented even if that question otherwise warranted this Court's review.<sup>5</sup>

---

<sup>5</sup> The court of appeals' application of plain-error review was independent of its discussion of the first question presented. The court applied the plain-error standard not because of petitioner's failure to object to the magistrate judge's underlying orders, but rather because petitioner "did not renew [his] self-incrimination claim during the contempt proceedings,"



a. The Fifth Amendment provides that “[n]o person \* \* \* shall be compelled in any criminal case to be a witness against himself.” U.S. Const. Amend. V. This Court has repeatedly instructed that the Fifth Amendment privilege against self-incrimination does not “proscribe the compelled production of every sort of incriminating evidence.” Fisher v. United States, 425 U.S. 391, 408 (1976). In Fisher, for example, the Court concluded that the Fifth Amendment would not permit a taxpayer to refuse to comply with a subpoena “requiring him to produce [his] accountant’s workpapers.” Id. at 409. The Court explained that although such a subpoena “without doubt involves substantial compulsion,” it does not “compel oral testimony” and does not “compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought.” Ibid. And “the Fifth Amendment would not be violated by the fact alone that the papers on their face might incriminate the taxpayer, for the privilege protects a person only against being incriminated by his own compelled testimonial communications.” Ibid.

The Court’s decision in Fisher noted, however, that “[t]he act of producing evidence in response to a subpoena has communicative aspects of its own, wholly aside from the contents of the papers produced.” 425 U.S. at 410. That is because

---

and instead “only reasserted his Fifth Amendment claim [on] appeal.” Pet. App. A13 (emphasis added).

production "tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer," as well as "the taxpayer's belief that the papers are those described in the subpoena." Ibid. The Court thus explained that the application of the Fifth Amendment to a subpoena of the sort described in Fisher turns on whether the "tacit averments" inherent in producing the requested materials are "both 'testimonial' and 'incriminating.'" Ibid. The Court stated that those issues "do not lend themselves to categorical answers" and "may instead depend on the facts and circumstances of particular cases or classes thereof." Ibid.

In Fisher, this Court was "confident that however incriminating the contents [of the requested documents] might be, the act of producing them -- the only thing which the taxpayer is compelled to do -- would not itself involve testimonial self-incrimination." 425 U.S. at 410-411. The Court explained that "[t]he existence and location of the papers [we]re a foregone conclusion" because the government already knew that they existed and were in the taxpayer's possession. Id. at 411. The tacit averments in the taxpayer's production of the documents would thus add "little or nothing to the sum total of the Government's information." Ibid.

The Court's decision in Fisher establishes that the Fifth Amendment does not protect a refusal to produce evidence when, in

light of the information already known to the government, the testimonial aspects of the production -- i.e., the existence, custody, and authenticity of the evidence sought -- are a "foregone conclusion." 425 U.S. at 411. In that circumstance, "no constitutional rights are touched" by a subpoena compelling the production of evidence because the compulsion "is not of testimony but of surrender." Ibid. (citation omitted); see United States v. Hubbell, 530 U.S. 27, 44-45 (2000) (distinguishing Fisher and declining to apply the foregone-conclusion doctrine because the government had "not shown that it had any prior knowledge of either the existence or the whereabouts" of the documents sought).

b. This Court's decision in Fisher makes clear that the decryption order did not violate the Fifth Amendment. As in Fisher, petitioner "cannot avoid compliance \* \* \* merely by asserting that the item of evidence which he is required to produce" -- here, decrypted hard drives -- "contains incriminating [evidence]." 425 U.S. at 410. And to the extent that producing electronic devices or files in an unencrypted state could have potentially testimonial aspects similar to those associated with producing documents sought in a subpoena, in this case any such potentially testimonial representations are foregone conclusions.

First, producing documents in response to a subpoena "tacitly concedes the existence of the papers demanded." Fisher, 425 U.S. at 410. Similarly, the production of devices or files in a

decrypted state could in some circumstances tacitly concede that those devices or files exist. In this case, however, the existence of petitioner's hard drives is unquestionably a foregone conclusion. The government already has the drives in its custody, and decryption would add nothing to the government's knowledge of their existence.

Second, the act of producing documents in response to a subpoena implicitly acknowledges that the papers sought are in the recipient's "possession or control" -- that is, that the recipient has the ability to produce them. Fisher, 425 U.S. at 410. Similarly, the production of petitioner's hard drives in an unencrypted state would entail an implied statement that "I, [petitioner], know the password for these devices." Pet. App. A17 n.7. As the court of appeals explained, however, that fact is likewise "a foregone conclusion." Id. at A18 n.7. No one disputes that petitioner at some point knew the passwords to his hard drives, and the courts below found that his claim to have forgotten them after the decryption order was a sham, id. at A18-A19 -- a finding that petitioner no longer challenges.

Third, the act of producing papers in response to a subpoena "indicate[s] the taxpayer's belief that the papers are those described in the subpoena." Fisher, 425 U.S. at 410. Similarly, the act of producing decrypted files matching a particular description might in some cases convey an implicit representation

that the produced files are the ones described in the subpoena or production order. But no such implicit representation is at issue here, where the order requires petitioner to decrypt specifically identified devices that are already in the government's possession. Unlike the act of producing documents that fit a description in a subpoena, the act of decrypting petitioner's hard drives would not tacitly convey anything about the contents of what is being decrypted. Pet. App. A17 n.7. In any event, even if that were not so, the courts below correctly found overwhelming evidence that the existence of child pornography on the hard drives is itself a foregone conclusion. Id. at A17.

c. The decryption order thus did not violate petitioner's Fifth Amendment privilege against self-incrimination because any implicit representations that petitioner might make in complying with the order would "add[] little or nothing to the \* \* \* Government's information." Fisher, 425 U.S. at 411. Petitioner's contrary arguments lack merit.

First, petitioner contends (Pet. 18-20) that the court of appeals should not have applied the foregone-conclusion doctrine because that doctrine is inapplicable to compelled "communication of personal knowledge like a memorized security code." Pet. 18. Petitioner's argument depends on his repeated assertion (e.g., Pet. 20) that the decryption order requires him to "communicate passwords" to the government -- something that petitioner

analogizes to "telling an inquisitor the combination to a wall safe," Hubbell, 530 U.S. at 43. But the order does not require petitioner to communicate his passwords to anyone. It simply requires him to "produce [specified electronic devices] to the Government in a fully unencrypted state." C.A. App. 3. To do that, of course, he must enter his passwords. But he is not required to disclose them. To the contrary, he was afforded a private space at the court-ordered forensic examination specifically to ensure that he could enter his passwords without revealing them. Gov't C.A. Br. 11.

Petitioner does not appear to dispute that he could comply with the decryption order without disclosing his passwords. But he maintains (Pet. 21) that "[t]he fact that the government seeks to have the passwords entered into a forensic interface rather than spoken aloud does not change the analysis." It is true enough (ibid.) that the Fifth Amendment analysis generally does not depend on the form of a compelled communication: If the government cannot require a suspect to make an incriminating statement orally, it also cannot require him to type the same statement into a computer for the government's review. But petitioner is not being required to communicate his passwords at all.

The critical point here is not that the decryption order requires petitioner to type his passwords instead of speaking them aloud; it is that the order does not require him to disclose the

passwords. As this Court has repeatedly emphasized, the Fifth Amendment reaches only “compelled explicit or implicit disclosures of incriminating information.” Doe v. United States, 487 U.S. 201, 212 (1988) (emphasis added); see id. at 210-211 (collecting cases).<sup>6</sup> The fact that the order does not require petitioner to reveal his passwords to the government (or to anyone else) thus forecloses his contention that this case involves a compelled testimonial communication of those passwords.

Second, petitioner asserts (Pet. 22) that Fisher is inapplicable to orders to produce unencrypted devices because such orders “reveal[] the entire content of a device,” rather than a “discrete set of documents described in a subpoena.” But the breadth of the information potentially contained in an electronic device is relevant to the privacy interests safeguarded by the Fourth Amendment, not to the Fifth Amendment privilege against self-incrimination -- as petitioner’s reliance on Riley v. California, 134 S. Ct. 2473 (2014), makes clear.

---

<sup>6</sup> The opinions on which petitioner relies (Pet. 21) all addressed compelled disclosures. See Pennsylvania v. Muniz, 496 U.S. 582, 594 (1990) (stating that the Fifth Amendment applies only if “some attempt is made to secure a communication -- written, oral, or otherwise”) (emphasis added; citation omitted); Doe, 487 U.S. at 219 (Stevens, J., dissenting) (stating that a suspect may not “be compelled to reveal the combination to his wall safe -- by word or deed”) (emphasis added); Braswell v. United States, 487 U.S. 99, 126 (1988) (Kennedy, J., dissenting) (the Fifth Amendment potentially applies where a person is required “to ‘disclose the contents of his own mind,’ through words or actions”) (emphasis added; citation omitted).

In this case, unlike in Riley, the government obtained a warrant to search petitioner's electronic devices. Pet. App. A6; see Riley, 134 S. Ct. at 2480. The warrant was issued by a neutral magistrate based on evidence establishing probable cause to believe that petitioner's hard drives contain large quantities of child pornography, and petitioner "does not dispute the validity of the underlying search warrant." Pet. App. A10 n.4. The use of the warrant procedure ensured that petitioner received the full measure of privacy protection required by the Fourth Amendment, and the concededly valid warrant gives the government full constitutional authority to search his hard drives. The only question is whether it violates the privilege against self-incrimination to require petitioner to decrypt those devices so that the government can carry out the validly authorized search.

On that question, the logic of Fisher applies with even greater force when an order requires a suspect to decrypt an entire device instead of producing specifically described documents. As the Court explained in Fisher, the act of producing documents described in a subpoena implicitly communicates "the [recipient's] belief that the papers are those described in the subpoena." 425 U.S. at 391. Here, in contrast, petitioner would not be making any implicit representations about the contents of his hard drives if he complied with the order to decrypt them. See pp. 18-19, supra. In these circumstances, petitioner's decryption is just



like the one-time use of a key to open the door to a location that the government has a valid warrant to search -- an act that raises no Fifth Amendment concerns. See Hubbell, 530 U.S. at 43.

Third, petitioner contends (Pet. 24-25) that the magistrate judge erred in concluding that, as a factual matter, any implicit testimonial aspects of petitioner's act of decrypting his hard drives would be a foregone conclusion. That challenge to the magistrate judge's factual findings does not warrant this Court's review. See Sup. Ct. R. 10 ("A petition for a writ of certiorari is rarely granted when the asserted error consists of erroneous factual findings."). That is particularly true because petitioner does not advance any developed argument on this point in his petition and instead seeks (Pet. 25) to incorporate by reference arguments that he "has elaborated elsewhere," in his briefs in the court of appeals. And in any event, petitioner's challenge lacks merit. As the court of appeals explained, the magistrate judge's factual findings were "amply supported by the record," which included undisputed evidence that the hard drives belonged to petitioner; forensic evidence showing that he used them to store child pornography; and his sister's statement that he had used the drives to show her "hundreds of pictures and videos of child pornography." Pet. App. A17; see id. at A4-A5 & n.3.

Fourth, petitioner contends (Pet. 26-28) that this Court should overrule Fisher and hold that "the Fifth Amendment privilege

protects against the compelled production not just of incriminating testimony, but of any incriminating evidence." Pet. 26 (quoting Hubbell, 530 U.S. at 49 (Thomas, J., concurring)). That contention lacks merit. As Fisher explained, a long line of decisions establish that the Fifth Amendment does not "proscribe the compelled production of every sort of incriminating evidence." 425 U.S. at 408. The Court has, for example, "declined to extend the protection of the privilege to the giving of blood samples; to the giving of handwriting exemplars; voice exemplars; or the donning of a blouse worn by the perpetrator." Ibid. (citations omitted). And while the Court at one time endorsed a Fifth Amendment rule that "a person may not be forced to produce his private papers," Fisher abandoned that rule because its "foundations \* \* \* ha[d] been washed away." 425 U.S. at 409. Petitioner disagrees with that conclusion, but he does not attempt to offer any sort of "special justification," Dickerson v. United States, 530 U.S. 428, 443 (2000) (citation omitted), for revisiting and overruling it.

Furthermore, even if this Court were prepared to reconsider Fisher "in a proper case," Hubbell, 530 U.S. at 56 (Thomas, J., concurring), this would not be such a case. Unlike the subpoena at issue in Fisher, the decryption order does not require petitioner "to furnish incriminating physical evidence" or private papers. Ibid. Instead, it requires him only to decrypt electronic

devices that are already in the government's possession and that are subject to a concededly valid warrant. Neither Fisher nor Justice Thomas's concurring opinion in Hubbell addressed the application of the Fifth Amendment to such an order. And this unusual case would not be an appropriate vehicle in which to reconsider the application of the Fifth Amendment to a more typical order requiring the production of evidence that is not already in the government's possession -- particularly because the issue here, if preserved at all, arises in a plain-error posture.

d. Petitioner asserts (Pet. 15-16) that this Court should grant review to harmonize what he calls a "hodgepodge of approaches" to orders requiring the decryption of electronic devices. But petitioner does not and could not contend that the court of appeals' decision conflicts with any decision by another court of appeals.

Only the Eleventh Circuit has addressed the question presented in a precedential decision. See In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335 (2012). The court there applied the foregone-conclusion reasoning of Fisher and determined that the decryption order at issue violated the Fifth Amendment because "[n]othing in the record \* \* \* reveal[ed] that the Government knows whether any files exist and are located on the hard drives" subject to the order, and because "nothing in the record illustrate[d] that the Government knows

with reasonable particularity that [the suspect] is even capable of accessing the encrypted portions of the drives.” Id. at 1346. The court of appeals in this case identified key distinctions between those circumstances and the very different situation presented here, emphasizing that “[u]nlike In re Grand Jury Subpoena, the Government has provided evidence to show both that files exist on the encrypted portions of the devices and that [petitioner] can access them.” Pet. App. A16. The decision below is thus entirely consistent with the Eleventh Circuit’s decision.

Petitioner also cites (Pet. 16) United States v. Mitchell, 76 M.J. 413 (C.A.A.F. 2017). That case is inapposite because the Court of Appeals for the Armed Forces expressly declined to “address whether [the defendant’s] delivery of his passcode was ‘testimonial’ or ‘compelled’” and thus did not reach the question “whether the Government directly violated [the defendant’s] Fifth Amendment privilege against compelled self-incrimination.” Id. at 419 (citation omitted). Instead, the court determined that agents had “violated [the defendant’s] Fifth Amendment right to counsel as protected by Miranda” because they continued to question him about his iPhone passcode after “he invoked his right to counsel.” Id. at 417.<sup>7</sup>

---

<sup>7</sup> Petitioner also cites (Pet. 16 n.8) decisions by district courts and state trial courts sustaining Fifth Amendment claims advanced in connection with the decryption of electronic devices. Those decisions could not establish the existence of any conflict warranting this Court’s review, see Sup. Ct. R. 10(a) and

e. Even if the application of the Fifth Amendment to decryption orders otherwise warranted this Court's consideration, the unusual procedural posture of this case would make it a poor vehicle in which to consider the issue. As the court of appeals observed, petitioner's failure to object to the magistrate judge's orders raises a question about his ability to assert his Fifth Amendment challenge in these contempt proceedings. Pet. App. A13-A14; see pp. 11-14, supra. And even apart from that obstacle, the court concluded that petitioner's Fifth Amendment argument is reviewable only for plain error because he "did not renew [that argument] during the contempt proceedings before the Magistrate Judge and the District Judge" and instead reasserted it only on appeal. Pet. App. A13. The plain-error posture would render this case a poor vehicle in which to consider the question presented

---

(b), and they are inapposite in any event. Most of them appeared to address orders that required individuals "to disclose \* \* \* passcodes" to the government rather than simply producing electronic devices in unencrypted form. SEC v. Huang, No. 15-cv-269, 2015 WL 5611644, at \*1 (E.D. Pa. Sept. 23, 2015); see United States v. Kirschner, 823 F. Supp. 2d 665, 668 (E.D. Mich. 2010); Commonwealth v. Jones, No. 2017CR49, 2017 WL 3340408, at \*3 (Mass. Super. Ct. July 26, 2017); Commonwealth v. Baust, No. CR14-1439, 2014 WL 10355635, at \*1, \*4 (Va. Cir. Oct. 28, 2014). And in the only decision that clearly addressed a request to compel a defendant to produce decrypted devices, the court held that the prosecution could not rely on the foregone-conclusion rationale of Fisher because in that case -- unlike this one -- the prosecution "d[id] not know that Defendant has or had control over the [devices]" and "d[id] not know what information [wa]s stored on the [devices]." State v. Trant, No. 15-2389, 2015 Me. Super. LEXIS 272, at \*9 (Me. Super Ct. Oct. 27, 2015).

because it would require petitioner to demonstrate, among other things, that the asserted Fifth Amendment error "is clear or obvious, rather than subject to reasonable dispute." United States v. Marcus, 560 U.S. 258, 262 (2010) (citation and internal quotation marks omitted); see Fed. R. Crim. P. 52(b).<sup>8</sup>

#### CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

NOEL J. FRANCISCO  
Solicitor General

JOHN P. CRONAN  
Acting Assistant Attorney General

FRANCESCO VALENTINI  
Attorney

APRIL 2018

---

<sup>8</sup> Petitioner asserts (Pet. 14-15) the court of appeals should not have applied plain-error review because he implicitly "press[ed]" his Fifth Amendment claim during his cross-examination of government witnesses and because he "maintained his privilege" by "electing not to testify" at the hearings. But petitioner did not argue during the contempt proceedings that the Decryption Order violated the Fifth Amendment, and the district court accordingly did not address the issue. Pet. App. A13 & n.6. Under the circumstances, the court of appeals correctly concluded that petitioner's claim is reviewable only for plain error.