

No. _____

IN THE SUPREME COURT OF THE UNITED STATES

JOHN DOE,
PETITIONER,

- VS. -

UNITED STATES OF AMERICA,
RESPONDENT.

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

KEITH M. DONOGHUE
Assistant Federal Defender
Counsel of Record

BRETT G. SWEITZER
Assistant Federal Defender
Chief of Appeals

LEIGH M. SKIPPER
Chief Federal Defender

FEDERAL COMMUNITY DEFENDER OFFICE
FOR THE EASTERN DISTRICT OF PENNSYLVANIA
Suite 540 West - Curtis Center
601 Walnut Street
Philadelphia, PA 19106
(215) 928-1100

Counsel for Petitioner

QUESTIONS PRESENTED

Applying what is known as the “act of production” doctrine, a magistrate judge ordered petitioner John Doe to enter computer passwords over his assertion of the Fifth Amendment right against self-incrimination. When Mr. Doe thereafter failed to recall and communicate the passwords, he was held in contempt and remanded to custody. On appeal, the Third Circuit deemed his claim of privilege unpreserved and denied relief on plain error review. Petitioner has now been jailed without charges for more than two years.

The act-of-production doctrine holds, contrary to the apparent understanding of the Constitution’s framers, that a target may sometimes be compelled to supply documents responsive to a subpoena despite their incriminating content. *Fisher v. United States*, 425 U.S. 391 (1976); see *United States v. Hubbell*, 530 U.S. 27, 49 (2000) (Thomas, J., concurring). Prior to a series of computer password cases over the last decade, the doctrine had never been thought to bear on the compelled disclosure of the contents of a person’s own mind. In fact, this Court has already offered the example of a memorized security code to illustrate the doctrine’s limits. The lower courts are now split in the password cases on whether the doctrine applies and, if so, how.

The questions presented are:

1. May appellate review of a claim of Fifth Amendment privilege be obtained by raising the claim before a presiding magistrate judge and thereafter suffering a contempt in lieu of compliance with an adverse ruling?
2. May a person be compelled to recall and communicate a computer password over a claim of the right against self-incrimination?

TABLE OF CONTENTS

	PAGE
Questions Presented	i
Table of Contents	ii
Table of Authorities	iv
Opinions Below	1
Jurisdictional Grounds	2
Parties to the Proceedings	2
Constitutional and Statutory Provisions Involved	3
Statement of the Case	4
Reasons for Granting the Petition	11
I. Certiorari should be granted to affirm the proper means of preserving claims of privilege for immediate review on appeal.	12
II. Certiorari should be granted to resolve discord rooted in a growing number of courts' erroneous application of the "act of production" doctrine.	15
A. The lower court decisions diverge in rationale and result.	15
B. The right against self-incrimination protects against compulsion to communicate a password to aid investigators' search for evidence.	17
1. Compelling divulgence of a password transgresses the right not to be forced to communicate personal knowledge for use against oneself.	18
2. Revelation of all of the content of an encrypted device is not analogous to the production of a discrete set of responsive documents.	22
3. Here, not only the password itself but the admissions tacit in its disclosure trigger the protection of the Fifth Amendment.	24
C. Review is warranted of whether the act-of-production doctrine is sound in any context.	26

TABLE OF CONTENTS – continued

	PAGE
III. The issues should be resolved in the present case.	28
Conclusion	30
Appendices:	
Third Circuit Opinion	Appendix A
Third Circuit Order Denying Rehearing	Appendix B
District Court Decryption Order	Appendix C
District Court Contempt Order	Appendix D
District Court Supplemental Contempt Order	Appendix E

TABLE OF AUTHORITIES

FEDERAL CASES	PAGE(s)
<i>Baltimore City Dep't of Soc. Servs. v. Bouknight</i> , 493 U.S. 549 (1990)	27
<i>Barrett v. Acevedo</i> , 169 F.3d 1155 (8th Cir. 1999)	27
<i>Bellis v. United States</i> , 417 U.S. 85 (1974)	26
<i>In re Boucher</i> (“ <i>Boucher I</i> ”), No. 06-mj-91, 2007 WL 4246473 (D. Vt. 2007)	16, 21, 22
<i>In re Boucher</i> (“ <i>Boucher II</i> ”), 2009 WL 424718 (D. Vt. 2009)	16, 17, 22
<i>Boyd v. United States</i> , 116 U.S. 616 (1886)	26, 28
<i>Braswell v. United States</i> , 487 U.S. 99 (1988)	19, 20, 21, 24
<i>Brightwell v. Lehman</i> , 637 F.3d 187 (3d Cir. 2011)	10, 13
<i>Butcher v. Bailey</i> , 753 F.2d 465 (6th Cir. 1985)	27
<i>Church of Scientology of California v. United States</i> , 506 U.S. 9 (1992)	12
<i>Cobbledick v. United States</i> , 309 U.S. 323 (1940)	12
<i>Curcio v. United States</i> , 354 U.S. 118 (1957)	17, 18, 19
<i>Doe v. United States</i> (“ <i>Doe II</i> ”), 487 U.S. 201 (1988)	11, 18, 19, 20, 21
<i>FDIC v. Ogden Corp.</i> , 202 F.3d 454 (1st Cir. 2000)	12
<i>Fisher v. United States</i> , 425 U.S. 391 (1976)	passim
<i>In re Grand Jury</i> , 705 F.3d 133 (3d Cir. 2012)	12

TABLE OF AUTHORITIES - continued

	PAGE(s)
<i>In re Grand Jury Subpoena Duces Tecum Dated March 25,</i> 670 F.3d 1335 (11th Cir. 2012)	16, 17, 29
<i>Maness v. Meyers,</i> 419 U.S. 449 (1975)	12
<i>Nara v. Frank,</i> 488 F.3d 187 (3d Cir. 2007)	10, 13
<i>Pennsylvania v. Muniz,</i> 496 U.S. 582 (1990)	20, 21
<i>Riley v. California,</i> 134 S. Ct. 2473 (2014)	22, 24
<i>In re Search Warrants to Google,</i> –F. Supp. 3d–, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017)	13
<i>SEC v. Huang,</i> Civ. No. 15-269, 2015 WL 5611644 (E.D. Pa. 2015)	16, 17, 21
<i>In re Steinberg,</i> 837 F.2d 527 (1st Cir. 1988)	27
<i>Thomas v. Arn,</i> 474 U.S. 140 (1985)	14
<i>United States v. Doe (“Doe I”),</i> 465 U.S. 605 (1984)	26, 27
<i>United States v. Dionisio,</i> 410 U.S. 1 (1973)	19
<i>United States v. Fricosu,</i> 841 F. Supp. 2d 1232 (D. Colo. 2012)	16, 17
<i>United States v. Gavegnano,</i> 305 F. App’x 954 (4th Cir. 2009)	16, 17
<i>United States v. Hubbell,</i> 530 U.S. 27 (2000)	passim
<i>United States v. Kirschner,</i> 823 F. Supp. 2d 665 (E.D. Mich. 2010)	16, 21

TABLE OF AUTHORITIES - continued

	PAGE(s)
<i>United States v. Mitchell</i> , 76 M.J. 413 (C.A.A.F. 2017)	16
<i>United States v. Pearson</i> , Crim. No. 04-340, 2006 U.S. Dist. LEXIS 32982 (N.D.N.Y. 2006)	16
<i>United States v. Polishan</i> , 336 F.3d 234 (3d Cir. 2003)	14
<i>United States v. Workman</i> , 863 F.3d 1313 (10th Cir. 2017)	4
 STATE CASES	 PAGE(s)
<i>Commonwealth v. Baust</i> , 89 Va. Cir. 267, 2014 WL 10355635 (2014)	16, 21
<i>Commonwealth v. Gelfgatt</i> , 11 N.E.3d 605 (Mass. 2014)	5, 16, 17
<i>Commonwealth v. Jones</i> , Crim. No. 2017-49, 2017 WL 3340408 (Mass. Super. 2017)	16
<i>State v. Stahl</i> , 206 So.3d 124 (Fla. App. 2016)	16, 17
<i>State v. Trant</i> , No. 15-2389, 2015 Me. Super. LEXIS 272 (2015)	16, 17
 FEDERAL STATUTES	 PAGE(s)
28 U.S.C. § 636(b)	<i>passim</i>
28 U.S.C. § 1254(1)	2
28 U.S.C. § 1291	2
28 U.S.C. § 1651	6
 RULES	 PAGE(s)
E.D. Pa. Local Civil Rule 72.1	13
Fed. R. Civ. P. 72(a)	14

TABLE OF AUTHORITIES - continued

	PAGE(s)
Fed. R. Crim. P. 59	14

OTHER AUTHORITIES

	PAGE(s)
<i>Entick v. Carrington</i> , 19 How. St. Tr. 1029	28
James Wareham, <i>Cracking the Code: The Enigma of the Self-Incrimination Clause and Compulsory Decryption of Encrypted Media</i> , 1 Geo. L. Tech. Rev. 247 (2017)	15

No. 17-_____

IN THE SUPREME COURT OF THE UNITED STATES

JOHN DOE,
PETITIONER

v.

UNITED STATES OF AMERICA,
RESPONDENT.

PETITION FOR WRIT OF CERTIORARI

Petitioner John Doe respectfully prays that a writ of certiorari issue to review the judgment of the United States Court of Appeals for the Third Circuit rendered in this case on March 20, 2017.

OPINIONS BELOW

The opinion of the court of appeals affirming the order of contempt is reported at 851 F.3d 238 and attached at Appendix A. That court's order denying rehearing is at Appendix B. The district court order requiring Mr. Doe to enter passwords for several previously seized encrypted devices is at Appendix C. The order and supplemental order of contempt are at Appendices D and E.

JURISDICTIONAL GROUNDS

The district court's jurisdiction was previously disputed but has been resolved by the Third Circuit. Pet. App. A10 (upholding subject matter jurisdiction under Criminal Procedure Rule 41). The court of appeals had jurisdiction pursuant to 28 U.S.C. § 1291. That court issued its opinion and judgment on March 20, 2017. A petition for rehearing was denied by order of July 28, 2017. This petition is timely filed pursuant to Rule 13.3 and the granting of petitioner's application for a 30-day extension of time, docketed at No. 17A416. The jurisdiction of this Court is invoked pursuant to 28 U.S.C. § 1254(1).

PARTIES TO THE PROCEEDING

Petitioner John Doe was granted leave to proceed pseudonymously in the court of appeals. He originally appeared in the district court by means of a motion to quash respondent United States' application for an order compelling him to recall and communicate the passwords to several encrypted devices. The government's application was styled in the manner of a proceeding in rem, with the devices listed under the heading "In the Matter of the Search Of Seized Items," to wit: Apple Mac Pro Computer; Apple iPhone 6 Plus Cellular Telephone; Western Digital My Book for Mac External Hard Drive; and Western Digital My Book VelociRaptor Duo External Hard Drive. At this time, the only devices remaining in controversy are the two external hard drives.¹

¹ Apple Inc. has trademarked the name "Mac Pro," rather than "MacPro," as appears in the case caption below. The text here uses the trademarked name. The caption in the court of appeals reflects a typographical error not reproduced here.

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fifth Amendment to the United States Constitution provides:

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury***; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law***.

The Federal Magistrates Act, Pub. L. 90-578, 82 Stat. 1108, as amended, provides in pertinent part:

(b)(1) Notwithstanding any provision of law to the contrary –

(A) a judge may designate a magistrate judge to hear and determine any pretrial matter pending before the court, except [eight enumerated categories of motions]. A judge of the court may reconsider any pretrial matter under this subparagraph (A) where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law.

(B) a judge may also designate a magistrate judge to conduct hearings, including evidentiary hearings, and to submit to a judge of the court proposed findings of fact and recommendations for the disposition, by a judge of the court, of any motion excepted in subparagraph (A), of applications for posttrial relief made by individuals convicted of criminal offenses and of prisoner petitions challenging conditions of confinement.

(C) the magistrate judge shall file his proposed findings and recommendations under subparagraph (B) with the court and a copy shall forthwith be mailed to all parties.

Within fourteen days after being served with a copy, any party may serve and file written objections to such proposed findings and recommendations as provided by rules of court. A judge of the court shall make a de novo determination of those portions of the report or specified proposed findings or recommendations to which objection is made[.]***

(3) A magistrate judge may be assigned such additional duties as are not inconsistent with the Constitution and laws of the United States.***

28 U.S.C. § 636(b).

STATEMENT OF THE CASE

Petitioner John Doe was held in civil contempt and jailed indefinitely for asserting his right against self-incrimination in response to a demand that he enter passwords for two encrypted hard drives. On his appeal from the contempt order, the Third Circuit denied relief under a doctrine applicable to subpoenas or summonses requiring the production of documentary evidence. The court apprehended no distinction between the production of a discrete set of responsive records and the communication of personal knowledge to aid a search of the entirety of a hard drive. Mr. Doe has now been confined for more than two years without charges, spending the better part of this time under restrictive conditions in a “special housing unit” due to his career in law enforcement.

1. On March 30, 2015, a team of investigators working out of the district attorney’s office in Delaware County, Pennsylvania, executed a state warrant at Mr. Doe’s home and seized numerous digital devices, including the hard drives now at issue. Mr. Doe had apparently become a person of interest by using a publicly available online network called Freenet, over which users can communicate and share files in a secure environment. C.A. App. 37. Like the more widely known ‘TOR’ network, *see, e.g. United States v. Workman*, 863 F.3d 1313, 1315-16 (10th Cir. 2017), Freenet anonymizes communications by routing each communication through other “nodes,” *i.e.*, other devices on the network, so that the original source of a transmission becomes difficult to identify. C.A. App. 37.

Several months after the warrant’s execution, authorities sought by means of a state grand jury to compel Mr. Doe to disclose the passwords needed to decipher the drives’ encrypted content. Following Mr. Doe’s invocation of the Fifth Amendment privilege against self-

incrimination, a judge of the Pennsylvania Court of Common Pleas ruled that Mr. Doe would not be compelled to enter the passwords himself or provide them to the grand jury. C.A. App. 18.

Rather than accept the state court's determination, investigators turned to federal court. A Homeland Security agent applied in the Eastern District of Pennsylvania for a new warrant, attaching an affidavit recounting what he had learned about the Delaware County investigation. C.A. App. 37-43. In some instances, the federal agent related what he had been told by local investigators; in others, his representations were of what local investigators said they had been told by civilian witnesses.

According to this second- and third-hand account, the seized hard drives had initially been secured with Apple Inc.'s FileVault encryption and connected to an encrypted Apple Mac Pro. C.A. App. 39-40. Mr. Doe, the affidavit said, had "refused to provide Detectives with the password. The hard drives remained encrypted, but investigators had independently decrypted the Mac Pro, which was thought to have been requesting and/or "routing" suspected child pornography files via the network's anonymization architecture. C.A. App. 37-38.²

Forensic analysis, however, had turned up just one image of interest, which depicted a teenage girl wearing a bathing suit in what someone (the affidavit did not say who) described as a "sexually suggestive position." C.A. App. 39. The forensic analysis was otherwise said to

² Investigators' decryption of the Mac Pro was by way of a recovery key pictured in a photograph they found on a different device for which Mr. Doe had provided the password at the time it was seized. C.A. App. 38-39. A discussion of how encryption works is set forth in the amicus brief supporting Mr. Doe filed by the Electronic Frontier Foundation in the Third Circuit on April 6, 2016, at pages 4-8. *See also Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 610 n.9 (Mass. 2014) (discussing distinction between recovery key and password); *see also* Apple Inc., *Use FileVault to encrypt the startup disk on your Mac*, at <https://support.apple.com/en-us/HT204837>. Broadly speaking, encryption is designed to protect the security of digital records and communications by "transform[ing] plain, understandable information into unreadable letters, numbers, or symbols using a fixed formula or process." Pet. App. A4 n.1.

have indicated the computer “had access to” or had visited Freenet message boards with names consistent with child pornography, C.A. App. 39, but the affidavit did not make clear whether this was true of any computer operating as a Freenet “node.” The agent represented that Mr. Doe’s sister had told local investigators Mr. Doe showed her images of child pornography on the “computers seized” and had spoken with family members of a problem with child pornography. C.A. App. 40-41. Other officers were reportedly summoned to a Doe family function where they seized an iPhone belonging to Mr. Doe with images that focused on two young nieces’ underwear between their legs. C.A. App. 40-41.

Based on the Homeland Security agent’s affidavit, a warrant authorizing a search of the previously seized devices was issued by the district court on July 29, 2015.³

2. A few days later, an Assistant United States Attorney applied pursuant to the All Writs Act, 28 U.S.C. § 1651, for an order compelling Mr. Doe to decrypt the devices. The application nowhere acknowledged that decryption would entail having Mr. Doe recall and communicate passwords. Instead, the government submitted that it sought ‘assistance’ in the warrant’s execution by compelling Mr. Doe “to produce” the (previously seized) devices “in an unencrypted state.” C.A. App. 60, 61, 62. The odd locution (“producing” items in the government’s possession) reflected the application’s reliance on a doctrine originally conceived in *Fisher v. United States*, 425 U.S. 391 (1976). There, the Court held that “the act of producing” documents, no matter how incriminating their content, is not necessarily protected by the Fifth Amendment. *See* 425 U.S. at 409-10. The government submitted that *Fisher* should

³ Though not relevant at this juncture, Mr. Doe notes for the record that he does not concede the “validity” of the warrant (nor of the earlier state warrant) as a matter of the Fourth Amendment and other authority of law. Pet. App. A10.

apply, and that under it, decryption could be compelled because it was a “foregone conclusion” evidence would be found on the hard drives, as well as that Mr. Doe was their possessor and knew how to decrypt them. C.A. App. 60-65 (quoting *Fisher*, 425 U.S. at 411).

In *Fisher*, the Court had stated this “foregone conclusion” rationale to explain that several taxpayers could be compelled to turn over specified work papers known to have been prepared by their accountants and transferred to their attorneys. 425 U.S. at 394-96, 410-11. The Court explained that, in some circumstances, the act of producing a document in response to a subpoena may be privileged in that it “tacitly” communicates “incriminating testimony,” *id.* at 409-10 – say, by implicitly affirming a document’s authenticity, *see id.* at 412-13. But the Court reasoned that under the circumstances, these taxpayers’ production was not a “testimonial communication” protected by the right against self-incrimination. *Id.* at 409. In speaking of a “foregone conclusion,” the Court amplified the fact that the records’ existence and whereabouts were already known to a certainty: “Surely the Government is in no way relying on the ‘truth-telling’ of the taxpayer to prove the existence of or his access to the documents. 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.” *Id.* at 411.

Mr. Doe opposed the government’s application for an order compelling decryption, renewing the claim of Fifth Amendment privilege previously upheld in state court. In a motion to quash, he argued that the government had not shown it was a “foregone conclusion” any evidence was stored on the hard drives, and that compelling him to divulge the passwords would unconstitutionally require him to “use the contents of his mind against himself.” C.A. App. 77.

Under local practice in the Eastern District of Pennsylvania, Magistrate Judge Thomas J. Rueter presided over the proceedings on the government's application pursuant to 28 U.S.C. § 636(b)(3), authorizing magistrate judges to "be assigned such additional duties as are not inconsistent with the Constitution and laws of the United States." Judge Rueter rejected Mr. Doe's arguments and granted the government's application, stating in a footnoted order as follows:

Here, the Affidavit of [the Homeland Security agent] supporting the application for a Search Warrant, establishes that (1) the Government has custody of the electronic devices; (2) prior to the Government's seizure, Mr. [Doe] possessed, accessed and owned all the electronic devices; and (3) there are images on the electronic devices that constitute child pornography. (Affidavit ¶¶ 13-31.) Therefore, under the "foregone conclusion" doctrine, requiring Mr. [Doe] to assist in the decrypting of those devices does not violate his privilege against self-incrimination.

Pet. App. C2. Pursuant to the order, Mr. Doe appeared at a local district attorney's office where the hard drives had been secured. There, he entered passwords into a forensic interface set up by investigators. C.A. App. 140, 164. The passwords did not work.

3. On the government's application, Judge Rueter thereafter ordered Doe to show cause. At two ensuing hearings, first before the magistrate and then before then-District Judge L. Felipe Restrepo, a detective testified that Mr. Doe had stated he could not remember the passwords. C.A. App. 136-38, 141-42, 324. The government presented testimony from Mr. Doe's sister, who claimed she had previously seen him entering passwords to access files. Pet. App. A18. Mr. Doe chose not to testify about whether or not he could enter the passwords. Because he "did not testify or call any witnesses," "did not offer any documentary or physical evidence into the record," and "offered no on-the-record explanation for his present failure to comply," Pet. App. E5, Judge Restrepo held him in civil contempt. Pet. App. D, E. Mr. Doe's

motion to stay the contempt was denied, and he was remanded to the custody of the Marshals Service on September 30, 2015.⁴

4. Mr. Doe noticed a timely appeal and again applied for a stay, which the Third Circuit denied. Following briefing and oral argument, the court of appeals rejected Mr. Doe's claim that the Fifth Amendment bars the government from compelling a suspect to recall and communicate a password to investigators so they may decipher the content of an encrypted device.

The panel (Vanaskie, J., joined by Jordan and Nygaard, JJ.) held first that Mr. Doe's sufferance of the contempt was not sufficient to preserve the issue for review. The panel did not pause to elaborate on this view. Instead, it cited without discussion two circuit decisions addressing matters referred to a magistrate judge for an advisory report and recommendation, *see* 28 U.S.C. § 636(b)(1)(B), rather than proceedings over which a magistrate judge presides in the exercise of "additional duties" authority, § 636(b)(3).

⁴ At the hearings in the district court, a detective testified it was his "best guess" that child pornography would be found on the hard drives. C.A. App. 346. The court of appeals recognized this testimony to lie beyond the scope of its review of the magistrate judge's earlier ruling for plain error. *See* Pet. App. A17. By way of background, the detective's opinion was based in part on "references" he had observed on the Mac Pro to "content hash keys" on the hard drives. *See* C.A. Reply Br., Addendum (excerpted testimony). Content hash keys are character strings used by the Freenet network to re-create images abiding on various of its nodes. The testimony identified a connection between the keys on the hard drives and child pornography elsewhere on the network. The detective did not testify, however, that the Mac Pro had downloaded and stored on the hard drives "thousands of files known by their 'hash' values to be child pornography," as the Third Circuit's opinion states. Pet. App. A5; *see* Reply Br., Addendum. It also bears clarifying that the "2,015 videos and photographs" found "in an encrypted application on Doe's phone," Pet. App. A6, were not child pornography. If need be, issues like these could be revisited in the circuit or district court. *See infra* Reasons II.B.3. But just as factual controversies of this kind are not usually relevant to a suspect's right to remain silent, they are not properly relevant here either. *Infra* Reasons II.B.1-2.

Proceeding to exercise plain error review,⁵ the Court upheld the decryption order. The Court declined to address several arguments put forward by Mr. Doe: that the “act of decryption” is in truth a statement of the contents of one’s own mind and thus always protected by the right against self-incrimination; and that the revelation of all of the contents of a hard drive or smart phone is not subject to the analysis set forth in *Fisher* because decryption is unlike the production of a discrete set of documents responsive to a subpoena. See C.A. Appellant’s Br. 33-40, 45; Reply Br. 10-13. Instead, the Court adopted the act-of-production rubric without discussion. Under that approach, the court explained, an act of production tacitly concedes “the existence, custody, and authenticity of that evidence.” Pet. App. A15. But the Court concluded it was not plain error to find that this “testimonial component” of decryption “would be a foregone conclusion” here. Pet. App. A17. Because Mr. Doe had remained silent rather than present evidence to “explain his failure to comply,” the court affirmed the order of contempt. Pet. App. A18-19. Mr. Doe’s petition for rehearing was denied. Pet. App. B.

⁵ The opinion states at one point that “[e]ven if we could assess” the Fifth Amendment issue, the challenge would fail on plain error review. 851 F.3d at 246. Despite the arguable ambiguity, the precedents cited by the court of appeals hold that a failure to object to a magistrate’s § 636(b)(1)(B) report and recommendation does not effect a waiver barring review altogether, but only a forfeiture limiting the scope of review to plain error. See Pet. App. A8 (citing *Brightwell v. Lehman*, 637 F.3d 187, 193 & n.7 (3d Cir. 2011), and *Nara v. Frank*, 488 F.3d 187, 194 (3d Cir. 2007)). In tandem with the opinion’s sustained discussion of the issue, it is evident the court of appeals charged Mr. Doe with a forfeiture rather than a waiver, so that its conclusion there was no plain error represents one holding of the decision.

REASONS FOR GRANTING THE PETITION

This case presents the important, recurring question of the Fifth Amendment's application to computer passwords and compelled decryption. The ruling below dishonors the right against self-incrimination, encouraging resort to cruel methods of compulsion that Mr. Doe's own experience well illustrates. Whatever may be the constitutional right's application to the production of documentary evidence under *Fisher* and its progeny, the privilege has never been thought to tolerate compulsion to communicate one's own personal knowledge for the government's use in finding evidence. Rather, it is the Fifth Amendment's core purpose to protect against such assaults upon "the dignity of the human mind." *Doe v. United States*, 487 U.S. 201, 219 n.1 (1988) (Stevens, J., dissenting) (hereinafter *Doe II*). Review is warranted to correct the Third Circuit's dangerous neglect of this first principle.

A decade of controversy has not yielded any regularity in lower court decisions addressing the question. Some courts have correctly held that a suspect may never be compelled to disclose a password over a claim of privilege. A greater number have held that disclosure may sometimes be compelled, but among these latter courts, there appears a further divergence in rationale and result. The inconsistency is the creature of a fundamental error in likening the mental process of recalling and communicating a password to the production of specific documents responsive to a subpoena. Review is warranted to correct the lower courts' misapprehension on this point and untangle a mass of doctrinal confusion.

Furthermore, review is warranted to revisit whether the Self-Incrimination Clause, as originally understood by the Constitution's framers, protects against compulsion to furnish incriminating documentary evidence, be the act of producing it "testimonial" or not. *See United States v. Hubbell*, 530 U.S. 27, 49 (2000) (Thomas, J., concurring). In taking a contrary premise,

Fisher not only failed to examine the historical backdrop to the Fifth Amendment, it also required ... a difficult parsing of the act of responding to a subpoena duces tecum.” *Id.* at 56. This case presents opportunity to correct *Fisher*’s substitution of a confounding doctrine for the Self-Incrimination Clause’s original meaning, and thus to bring to an end that decision’s imperilment of a fundamental human right.

I. Certiorari should be granted to affirm the proper means of preserving claims of privilege for immediate review on appeal.

As a preliminary matter, this matter affords opportunity to cut off an inroad suggested by the Third Circuit on the function of contempt proceedings as the preferred means of obtaining prompt appellate review of claims of privilege.

In holding Mr. Doe’s claim unpreserved, the Third Circuit departed from longstanding doctrine. *See Cobbledick v. United States*, 309 U.S. 323, 328 (1940) (identifying sufferance of contempt as proper means of obtaining interlocutory review of privilege claim); *FDIC v. Ogden Corp.*, 202 F.3d 454, 459 (1st Cir. 2000) (reviewing “the *Cobbledick* rule”). Mr. Doe proceeded in the fashion this Court has directed by asserting his Fifth Amendment right and then submitting to the court’s contempt power rather than communicating the passwords or testifying to his inability to do so. *See Church of Scientology of California v. United States*, 506 U.S. 9, 18 n.11 (1992) (“A party that seeks to present an objection to a discovery order immediately to a court of appeals must refuse compliance, be held in contempt, and then appeal the contempt order.”). “This method of achieving precompliance review,” the Court has said, “is particularly appropriate where the Fifth Amendment privilege against self-incrimination is involved.” *Maness v. Meyers*, 419 U.S. 449, 461 (1975).

The Third Circuit usually recognizes this well-established doctrine, *see In re Grand Jury*, 705 F.3d 133, 142-43 (3d Cir. 2012), and even in this case the panel acknowledged the ordinary

rule, Pet. App. A10 n.5. As best as can be told from the unclear opinion, the court nonetheless regarded the issue to have been forfeited because Mr. Doe did not seek reconsideration by a district judge of the magistrate judge's order denying his motion to quash. *See* Pet. App. A8 (stating that issue would be reviewed for plain error and citing without elaboration two circuit precedents⁶ requiring objections to advisory report and recommendation prepared by magistrate judge pursuant to 28 U.S.C. § 636(b)(1)(B)); *see also* Pet. App. A6, A13 n.6 (repeatedly noting that Mr. Doe did not seek reconsideration of magistrate judge's ruling). Under *Cobbledick* and its progeny, that conclusion is wrong because this is not an appeal from a final judgment raising an issue decided by a magistrate judge at an earlier juncture. Rather, Mr. Doe availed himself of a route to immediate appellate review in a special proceeding instituted by the government's application for the issuance of legal process. *See* Pet. App. A10.

Furthermore, even putting aside the distinction between obtaining immediate review by sufferance of a contempt and preserving an issue for later review, Mr. Doe was not required to seek reconsideration because the magistrate presided here pursuant to 28 U.S.C. § 636(b)(3), authorizing the discharge of "such additional duties as are not inconsistent with the Constitution and laws of the United States." *See In re Search Warrants to Google*, –F. Supp. 3d–, 2017 WL 3535037, at *2 n.4 (E.D. Pa. Aug. 17, 2017) (explaining that in Eastern District of Pennsylvania, magistrate judge's ruling on motions to compel enforcement of a warrant is "best understood" as exercise of "additional duties" authority pursuant to § 636(b)(3)); *see also* E.D. Pa. Local Civil Rule 72.1(e)(5). A party is only ever required to seek reconsideration when, unlike here, a presiding district judge designates a magistrate judge to hear a pretrial matter pursuant to 28

⁶ *Brightwell v. Lehman*, 637 F.3d 187, 193 & n.7 (3d Cir. 2011), and *Nara v. Frank*, 488 F.3d 187, 194 (3d Cir. 2007).

U.S.C. § 636(b)(1)(A) or to prepare an advisory report and recommendation pursuant to § 636(b)(1)(B). *See* Fed. R. Civ. P. 72(a) & advisory committee note (1983 adoption) (limiting requirement to subparagraphs (b)(1)(A) and (B)); *see also* *Thomas v. Arn*, 474 U.S. 140 (1985). Here, no district judge was even presiding. Moreover, the Local Rules of the Eastern District of Pennsylvania codify no procedure for seeking reconsideration of a magistrate’s rulings in the exercise of subsection (b)(3) “additional duties” authority. *Cf.* Local Civil Rule 72.1(IV) (specifying means for seeking reconsideration of rulings pursuant to designation under § 636(b)(1)(A) or (B) only).⁷

Apart from stressing that Mr. Doe did not seek reconsideration, the Third Circuit stated that he did not raise his Fifth Amendment claim as a defense to the citation for contempt, Pet. App. A13, while also suggesting he would not have been permitted to do so, Pet. App. A10. It is not clear whether these observations were meant to state a holding as to preservation. In any event, Mr. Doe’s counsel did press the Fifth Amendment claim at the contempt hearings by disputing it was a “foregone conclusion” that evidence would be found on the hard drives. *See, e.g.*, C.A. App. 263-265, 339-340, 350, 374-376. As set forth in the Statement, that issue went strictly to whether, on the government’s theory of the case, Mr. Doe could be ordered over his assertion of the right against self-incrimination to disclose the passwords. Indeed, the government’s own briefing in the Third Circuit relied on the testimony adduced at the hearings in support of its “foregone conclusion” argument. C.A. Appellee’s Br. 39-43.

⁷ Because Mr. Doe has not been charged with any crime – be it by indictment, information, or complaint – the present matter is not a criminal case, as the court of appeals recognized at several junctures below. *See* Order (filed June 10, 2016); Order (filed Apr. 22, 2016); Text Order (Apr. 6, 2017). Accordingly, the matter is not subject to the rule stated by the Third Circuit in *United States v. Polishan*, 336 F.3d 234 (3d Cir. 2003), *cited at* Pet. App. A13 n.6, or to Rule 59 of the Federal Rules of Criminal Procedure.

Finally, Mr. Doe maintained his privilege claim at the contempt hearings by electing not to testify regarding his inability to comply with the decryption order. It was due precisely to his failure to present such evidence that he has been held in contempt. *See* Pet. App. E5; Pet. App. A18-19. He has continued to maintain the claim by suffering confinement under the contempt order rather than waiving his right against self-incrimination by testifying to his inability to comply with the decryption order.

For all of these reasons, there was no forfeiture or waiver. Certiorari should be granted on the first question presented to confirm that contempt proceedings are the preferred means of obtaining immediate appellate review of a claim of privilege.

II. Certiorari should be granted to resolve discord rooted in a growing number of courts' erroneous application of the "act of production" doctrine.

This Court's review is essential to bring regularity to what is at present a hodgepodge of approaches to the vital question of whether the Fifth Amendment protects against the compelled divulgence of a password to decrypt devices such as hard drives and smart phones. That amendment commands that no person "shall be compelled in any criminal case to be a witness against himself." Certiorari should be granted to ensure this constitutional guarantee is not overwhelmed by technological advances that, for all their novelty, need not endanger the right against self-incrimination.

A. The lower court decisions diverge in rationale and result.

Decisions in the lower courts have yielded no rule as to what protection a suspect is guaranteed from compulsion to recall and communicate a password. A recent survey of the cases found "little analysis that assists the everyday criminal litigator in understanding and applying constitutional principles in digital encryption cases." James Wareham, *Cracking the Code: The Enigma of the Self-Incrimination Clause and Compulsory Decryption of Encrypted*

Media, 1 Geo. L. Tech. Rev. 247, 248 (2017). Of the reported state and federal decisions known to counsel, six have upheld the privilege while six (counting the Third Circuit’s decision below) have not.⁸

Across this spectrum of discord, at least three different rules have been adopted. One set of cases gets the rule right: disclosure may not be compelled because forcing a defendant “to reveal the password requires [him] to communicate ‘knowledge,’ unlike the production of a handwriting sample or a voice exemplar.” *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010); see *Commonwealth v. Baust*, 89 Va. Cir. 267, 2014 WL 10355635, at *4 (2014) (computer password is privileged “because it is not known outside of Defendant’s mind” and cannot be divulged except “through his mental processes”); see also *United States v. Mitchell*, 76 M.J. 413, 419 (C.A.A.F. 2017) (suspect in custody may not be asked for password once he invokes right to counsel, even if his knowledge of password is foregone conclusion); cf. *SEC v. Huang*, Civ. No. 15-269, 2015 WL 5611644, at *1 (E.D. Pa. 2015) (stressing that to compel password would “require intrusion into the knowledge of Defendants and no one else”).

⁸ Compare *In re Grand Jury Subpoena Duces Tecum Dated March 25*, 670 F.3d 1335 (11th Cir. 2012) (upholding privilege claim), *Commonwealth v. Jones*, Crim. No. 2017-49, 2017 WL 3340408 (Mass. Super. 2017) (same), *SEC v. Huang*, Civ. No. 15-269, 2015 WL 5611644 (E.D. Pa. 2015) (same), *State v. Trant*, No. 15-2389, 2015 Me. Super. LEXIS 272 (2015) (same), *Commonwealth v. Baust*, 89 Va. Cir. 267, 2014 WL 10355635 (2014) (same), and *United States v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich. 2010) (same) with *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014) (5-2 decision) (rejecting privilege claim), *State v. Stahl*, 206 So.3d 124 (Fla. App. 2016) (same), *United States v. Gavegnano*, 305 F. App’x 954 (4th Cir. 2009) (not precedential) (same), *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012) (same), and *In re Boucher (Boucher II)*, No. 06-mj-91, 2009 WL 424718 (D. Vt. 2009) (same); see also *In re Boucher (Boucher I)*, 2007 WL 4246473 (D. Vt. 2007) (magistrate judge’s earlier ruling in same case upholding privilege claim). An additional decision includes a sustained analysis before concluding a further hearing was necessary. *United States v. Pearson*, Crim. No. 04-340, 2006 U.S. Dist. LEXIS 32982 (N.D.N.Y. 2006).

A majority of courts, however, have applied the “act of production” doctrine conceived in *Fisher v. United States*, 425 U.S. 391 (1976), to hold that disclosure may be compelled if a “foregone conclusion” is shown. *See, e.g., In re Grand Jury Subpoena Duces Tecum Dated March 25*, 670 F.3d 1335, 1345-46 (11th Cir. 2012). Just what conclusion must be foregone is the subject of considerable confusion. One view requires, among other things, that the specific files or data constituting known evidence be identified with “reasonable particularity.” *E.g., id.* at 1346; *Huang*, 2015 WL 5611644 at *3; *In re Boucher (Boucher II)*, No. 06-mj-91, 2009 WL 424718, *3 (D. Vt. 2009); *State v. Trant*, No. 15-2389, 2015 Me. Super. LEXIS 272, *10 (2015). A second view, by contrast, holds that only the suspect’s knowledge of the password must be a foregone conclusion. *Pet. App. A17-18 n.7*; *State v. Stahl*, 206 So.3d 124, 136 (Fla. App. 2016); *see Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 615 (Mass. 2014). There is even some suggestion in the cases that it may be enough to show that a device belonged exclusively to the defendant. *See United States v. Gavegnano*, 305 F. App’x 954, 956 (4th Cir. 2009) (*per curiam*) (not precedential); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012).

B. The right against self-incrimination protects against compulsion to communicate a password to aid investigators’ search for evidence.

While no rule of law has emerged, a fundamental category mistake stands out conspicuously. The error lies in a failure to recognize that while entering a computer password may culminate in the “production” of digital evidence, the password’s divulgence consists in the first instance of a suspect’s communication of personal knowledge in the form of a memorized security code. The right against self-incrimination categorically protects against compulsion to confess such “contents of [one’s] own mind.” *Curcio v. United States*, 354 U.S. 118, 128 (1957). What is more, the act-of-production doctrine concerns the enforcement of subpoenas that specify a discrete set of documents known to be in a subject’s possession. By contrast,

compelled decryption involves the revelation of the whole of an extraordinary cache of private information unknown to the government. Both because divulgence of a password is testimonial in itself, and because decryption is not limited to a discrete set of records, the act-of-production doctrine has no place.

1. Compelling divulgence of a password transgresses the right not to be forced to communicate personal knowledge for use against oneself.

The decision that innovated the act-of-production doctrine, *Fisher v. United States*, was not about the communication of personal knowledge like a memorized security code. Rather, it concerned strictly the issue of what protection may be afforded against the compelled production of incriminating documents already known by the government to exist. This novel approach to documents, however, has no application to compulsion to recall and communicate information known only to oneself.

In fact, this Court has repeatedly offered the example of a memorized security code to illustrate the limits of the act-of-production doctrine. As Justice Stevens first put it, a target “may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe – by word or deed.” *Doe II*, 487 U.S. at 219 (Stevens, J., dissenting); *see also id.* at 210 n.9 (majority’s statement of agreement with the distinction). The point of the hypothetical, Justice Stevens subsequently elaborated for the Court, is that divulging the combination would require a person to communicate “the contents of his own mind” for investigators’ use in finding evidence. *United States v. Hubbell*, 530 U.S. 27, 43 (2000) (quoting *Curcio*, 354 U.S. at 128). “[T]here is a significant difference,” the Court explained, “between the use of compulsion to extort communications from a defendant and compelling a person to engage in conduct that may be incriminating.” 530 U.S. at 35.

The *Curcio* case on which *Hubbell* relied illustrates the principle. There, the suspect was a local union official who, in response to a subpoena, had failed to produce the local's books and records. Because he was the designated custodian, he had no right to withhold documents that might incriminate him. 354 U.S. at 119. Despite his failure to produce the records, the unanimous Court held he could not be compelled to answer questions as to the whereabouts of the missing records. *Id.* That, the Court explained, would force him "to disclose the contents of his own mind" for use against himself, "contrary to the spirit and letter of the Fifth Amendment." *Id.* at 128. *Hubbell* repeated the point, instructing that the privilege protects a target "from being compelled to answer questions designed to elicit information about the existence of sources of potentially incriminating evidence." 530 U.S. at 43.

Put another way, a person may not be compelled "to disclose his own knowledge" in aid of prosecution. *Braswell v. United States*, 487 U.S. 99, 126 (1988) (Kennedy, J., dissenting) (discussing *Curcio*); see *Doe II*, 487 U.S. at 210 (recognizing that "the expression of the contents of an individual's mind is testimonial communication for purposes of the Fifth Amendment") (internal quotation marks and brackets omitted). Thus, while the privilege does not extend to purely physical acts that reveal nothing about a suspect's mental processes, it does extend to demands that "probe the state of mind, memory, perception, or cognition of the witness." *Braswell*, 487 U.S. at 126 (Kennedy, J., dissenting). See *United States v. Dionisio*, 410 U.S. 1, 6 (1973) ("The distinction which has emerged, often expressed in different ways, is that the privilege is a bar against compelling 'communications' or 'testimony,' but that compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it.") (additional quotation marks and citation omitted).

That rule was essential to the holding of *Pennsylvania v. Muniz*, 496 U.S. 582 (1990). There, the Court determined that while the right against self-incrimination did not prohibit the introduction into evidence of the fact of a drunk-driving suspect's slurred speech, it did bar admission of his mistaken answer to the question, "Do you know what the date was of your sixth birthday?" 496 U.S. at 593-94; *see id.* at 608. The distinction followed from the rule that the privilege spares an accused from "having to share his thoughts and beliefs with the Government." *Id.* at 592 (quoting *Doe II*, 487 U.S. at 213). Moreover, the Court made clear, this protection encompasses both "verbal and nonverbal conduct." *Id.* at 592 n.9. What matters is "the actor's communication of his thoughts to another." *Ibid.*; *see also Braswell*, 487 U.S. at 126 (Kennedy, J., dissenting) (privilege's protection of personal knowledge does not depend on whether compelled disclosure is "spoken" or communicated by means of physical act).

The same rule necessarily applies to divulgence of an encryption passcode – what, in one aspect, might be considered a virtual combination lock. The government does not propose to have Mr. Doe undertake a strictly physical act like turning a bolt or touching a digital thumbprint detector. It proposes to force him to recall, if he is able, and communicate the contents of his own mind. While an encrypted device may not much resemble a wall safe, the resemblance between a memorized password and memorized sequence of numbers could hardly be more patent.

Though the government has insisted it has no interest in the passwords themselves, it is wordplay to speak instead of having Mr. Doe "produce" the hard drives in an "unencrypted state." C.A. App. 60, 61, 62. The hard drives have already been seized, and there are no unencrypted versions of them in Mr. Doe's physical custody. What the government really seeks is not to have Mr. Doe produce the drives, but to recall and communicate passwords that will aid

a search of the drives' contents for evidence. The fact that the government seeks to have the passwords entered into a forensic interface rather than spoken aloud does not change the analysis. See *Muniz*, 496 U.S. at 594 (privilege applies equally to any demand for "a communication – written, oral or otherwise"); *Doe II*, 487 U.S. at 219 (Stevens, J., dissenting) (suspect may not be forced to reveal combination "by word or deed"); *Braswell*, 487 U.S. at 126 (Kennedy, J. dissenting) (immaterial whether communication is "spoken" or conveyed by other means). Mr. Doe has been jailed indefinitely not for failing to demonstrate his typing skills, but for declining to divulge the contents of his own mind.

Several of the decisions that have correctly upheld the privilege have reasoned accordingly. "In this case, the government is not seeking documents or objects – it is seeking testimony from the Defendant, requiring him to divulge through his mental processes his password – that will be used to incriminate him." *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (subpoena ad testificandum). Forcing a suspect "to provide access through his passcode is both compelled and testimonial and therefore protected." *Commonwealth v. Baust*, 89 Va. Cir. 267, 2014 WL 10355635, at *4 (2014). "Contrary to the Commonwealth's assertion, the password is not a foregone conclusion because it is not known outside of Defendant's mind." *Ibid.* See also *Huang, supra*, 2015 WL 5611644, at *1 (stating that "we find the personal thought process defining a smartphone passcode ... is testimonial," while also holding that no "foregone conclusion" had been shown on facts of case).

Perhaps the fullest statement of the correct rule appears in the first widely reported decision on the issue. See *In re Grand Jury Subpoena (Boucher I)*, No. 06-mj-91, 2007 WL 4246473 (D. Vt. 2007). There, a magistrate judge correctly concluded that disclosure of a

password could not be compelled because such disclosure requires the communication of personal knowledge:

Since the government is trying to compel the production of the password itself, the foregone conclusion doctrine cannot apply. The password is not a physical thing. If Boucher knows the password, it only exists in his mind. This information is unlike a document, to which the foregone conclusion doctrine usually applies, and unlike any physical evidence the government could already know of. It is pure testimonial production rather than physical evidence having testimonial aspects. Compelling Boucher to produce the password compels him to display the contents of his mind to incriminate himself.... The foregone conclusion doctrine does not apply to the production of non-physical evidence, existing only in a suspect's mind where the act of production can be used against him.

2007 WL 4246473, at *6.

Following the magistrate's ruling, a district judge erred in denying the privilege claim by way of a 'foregone conclusion' analysis. *See Boucher II*, 2009 WL 424718 (2009).

Unfortunately, it is the district judge's analysis that has proven the more influential. The Third Circuit's failure in the present case to so much as acknowledge the contrary authority threatens to accelerate this trend in the wrong direction.

2. Revelation of all of the content of an encrypted device is not analogous to the production of a discrete set of responsive documents.

Even were one to set aside the communication of personal knowledge inherent in any divulgence of a computer password, the doctrine conceived in *Fisher* could not apply on its own terms. Decrypting a device like a smart phone or hard drive is not an act of producing a discrete set of documents described in a subpoena. Rather, it is the revelation of the entire content of a device, be that content foreknown to the government or not. In its totality, this content often amounts to "a digital record of nearly every aspect of [users'] lives – from the mundane to the intimate." *Riley v. California*, 134 S. Ct. 2473, 2490 (2014).

Fisher did not involve the revelation of so much as a filing cabinet. All that was commanded was the production of a few types of tax documents detailed in a summons, which the government already knew had been prepared by the taxpayers' accountants and then transferred by the taxpayers to their attorneys. *See* 425 U.S. at 394-95. The only question was whether the admissions "tacit" in the act of producing these records had "testimonial" significance of a kind permitting the taxpayers to call upon the right against self-incrimination. *Id.* at 410. The *Fisher* majority's view was that, under the circumstances, the implicit concession of the documents' existence, possession or control, and authenticity was not privileged because the substance of these implicit admissions was already a "foregone conclusion." *Id.* at 411 (internal quotation marks omitted).

"Whatever the scope of this 'foregone conclusion' rationale," *Hubbell*, 530 U.S. at 44, it has come to predominate as the controlling rule in the computer password cases. *See supra* Part A. This rise from relative obscurity is odd, because the doctrine expounded in *Fisher* concerns the production of "specific documents" responsive to a reasonably particularized subpoena. *Hubbell*, 530 U.S. at 35; *see id.* at 30. Compelled decryption is a different proposition altogether. It consists not in the disclosure of a discrete set of documents already identified by the government, but in the revelation of an astounding cache of unknown information about a person's private activities, associations, interests, and diversions. This digital record comes in not one but many forms: a log of websites visited or books read or reality television shows viewed; personal notes and reminders; contact lists and emails with acquaintances, colleagues, friends, and loved ones; and all the other kinds of information stored in voluminous and variegated form on digital devices today, from photographs to shopping receipts to doctor's appointments to travel reservations, and much more. No part of this information is already a

“foregone conclusion.” Because *Fisher* and its progeny address the production of a discrete set of responsive documents, not the revelation of the “montage of the user’s life” composed by a device’s contents, *Riley*, 134 S. Ct. at 2490, the act-of-production doctrine has no place.

Another difference owes to how encryption works. The basic rationale of *Fisher* was that a subpoena or summons does not “compel the creation of a document; it compels its production.” *Braswell*, 404 U.S. at 121 (Kennedy, J., dissenting). But the same is not true of an order to communicate the password for an encrypted device. In this novel context, records *are* created – or at least *re-created* – upon entering a password so as to transform a mass of unintelligible text into potentially incriminating files, activity logs, and other legible data. See C.A. Br. Amicus Curiae Electronic Frontier Foundation, et al., at 4 (filed Apr. 6, 2016) (“[C]ompelled decryption is inherently testimonial because it compels a suspect to use the contents of their mind to translate unintelligible evidence into a form that can be used against them.”).

3. Here, not only the password itself but the admissions tacit in its disclosure trigger the protection of the Fifth Amendment.

For the reasons already stated, the right against self-incrimination protects against the compelled disclosure of a computer password to aid investigators’ search for evidence. Properly speaking, such divulgence is not solely an “act” but a communication that is in itself fully within the scope of the privilege.

Yet even were it to be determined that the act-of-production doctrine applies, a remand would be necessary. When a suspect communicates a password, he admits that he is among the persons potentially responsible for any evidence stored on the device. He also makes admissions as to the existence of the device’s contents, his prior possession (exclusive or joint) of those contents, and the authenticity of the device, *e.g.*, that a proper chain of custody has been maintained. Here, these admissions, in tandem with the absence of any showing to a “foregone

conclusion” that there is evidence encrypted on the hard drives, would carry enough testimonial significance to be privileged under the act-of-production doctrine.

On this point, the Third Circuit, consistent with its review only for plain error, limited its consideration to the warrant application relied upon by the magistrate judge in ordering disclosure. That application, consisting exclusively in a second- and third-hand account, did not establish a “foregone conclusion” there was evidence on the hard drives. Even were it not for the application’s hearsay character, its discussion was ambiguous as to the forensic examination’s significance, or lack of it, particularly in view of the affidavit’s discussion of how Freenet works. This ambiguity and the bare statements attributed to family members do not establish a foregone conclusion, as evident in the Third Circuit’s conclusion that the magistrate judge did not commit “clear or obvious” error in ordering decryption. Pet. App. A17.

Once the issue’s preservation by Mr. Doe’s sufferance of a contempt is recognized, resort may be had to the in-court testimony given by the government’s witnesses in the contempt proceedings. As Mr. Doe has elaborated elsewhere, these witnesses established no more than a “best guess” as to whether evidence might be found on the hard drives. C.A. App. 346; *see* C.A. Appellant’s Br. 45-47; Reply Br. 14-17; *supra* note 5.

This Court need not concern itself with the intensive factual analysis that could be occasioned were the act-of-production doctrine to be applied. Rather, in that event, Mr. Doe should be recognized to have preserved his Fifth Amendment claim and the matter remanded for further proceedings. Alternatively, relief should be granted to confirm the plain insufficiency of the hearsay set forth in the warrant application.

C. Review is warranted of whether the act-of-production doctrine is sound in any context.

Looking beyond computer passwords, the act-of-production doctrine also stands revisiting because it “may be inconsistent with the original meaning of the Fifth Amendment’s Self-Incrimination Clause.” *Hubbell*, 530 U.S. at 49 (Thomas, J., joined by Scalia, J., concurring). A “substantial body of evidence” in fact “suggests the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence.” *Ibid.* (inviting opportunity to reconsider doctrine “in light of the historical evidence that the Self-Incrimination Clause may have a broader reach than *Fisher* holds”); *see also id.* at 56 (“*Fisher* ... failed to examine the historical backdrop to the Fifth Amendment”).

As Justice Brennan reviewed in *Fisher* itself, 425 U.S. at 418-19 (opinion concurring in judgment), the right against self-incrimination had, until that case, always been understood to protect against the compelled production of incriminating papers. *E.g.*, *Bellis v. United States*, 417 U.S. 85, 87 (1974) (“It has long been established, of course, that the Fifth Amendment privilege against compulsory self-incrimination protects an individual from compelled production of his personal papers and effects as well as compelled oral testimony.”); *Boyd v. United States*, 116 U.S. 616, 634-35 (1886) (holding unanimously that right against self-incrimination protects a defendant from being compelled to produce documents).

The majority in *Fisher* contended that this understanding had “not stood the test of time.” 425 U.S. at 407. But the original rule turns out to have proven sturdier than thought: to date it has survived well enough to vex the question of whether diaries and other private papers, as distinct from business records, are covered by the novel doctrine expounded in *Fisher*. *See United States v. Doe*, 465 U.S. 605, 618 (1984) (“*Doe P*”) (O’Connor, J., concurring) *and id.* at

619 (Marshall, J., concurring in part) (disagreeing as to whether Court's instant opinion had extended *Fisher* to individual's private papers); *id.* at 612 & n.9 (opinion of Court); *Barrett v. Acevedo*, 169 F.3d 1155, 1168 & n.14 (8th Cir. 1999) (contemplating privilege's application to most private of personal papers); *In re Steinberg*, 837 F.2d 527, 530 (1st Cir. 1988) (same); *Butcher v. Bailey*, 753 F.2d 465, 469 (6th Cir. 1985) (same). Compare *Baltimore City Dep't of Soc. Servs. v. Bouknight*, 493 U.S. 549, 554-55 (1990) (applying rule of *Fisher* to "unadorned act of producing" identified child for placement in foster care on ground of known abuse and neglect).

The long line of precedents holding the privilege to reach incriminating documents traces to the framers' own apparent "view that the term 'witness' meant a person who gives or furnishes evidence." *Hubbell*, 530 U.S. at 49 (Thomas, J., concurring). That is, it may not be only "testimonial" communications (in the sense of *Fisher*) that are within the scope of the privilege, but also "the compelled production of books, records, and archives in response to a government request." *Id.* at 49-50 & n.1. Among other notable signs of this understanding, the broad 'give or furnish evidence' formulation appears with striking consistency in dictionaries of the period, in state constitutions adopted before the founding, and in bills of rights proposed by ratifying states. See *id.* at 50-53. Moreover, the "18th-century common-law privilege against self-incrimination protected against the compelled production of physical evidence such as papers and documents." *Id.* at 51. Two centuries later, Thurgood Marshall championed the "deeply held belief on the part of the Members of this Court throughout its history that there are certain documents no person ought to be compelled to produce at the Government's request." *Fisher*, 425 U.S. at 431-32 (Marshall, J., concurring).

The “technical and somewhat esoteric” *Fisher* analysis, aspiring to a pristine logic in its abstractions from the “act of production,” has been the darling of some in the legal academy since before its adoption. 425 U.S. at 430-31 (Marshall, J., concurring in judgment). But the “privilege against self-incrimination is a specific provision of which it is peculiarly true that a page of history is worth a volume of logic.” *Id.* at 417 n.2 (Brennan, J., concurring in judgment) (internal quotation marks omitted). If logic there be to consult, it is that when the right goes unrecognized, there ineluctably follows the question of what means may be used to “compel” a person to incriminate himself. In the celebrated decision that every statesman among the framers considered “the true and ultimate expression of constitutional law,” Lord Camden stated the answer: “[T]he law obligeth no man to accuse himself; because the necessary means of compelling self-accusation, falling upon the innocent as well as the guilty, would be both cruel and unjust.” *Boyd*, 116 U.S. at 629 (quoting *Entick v. Carrington*, 19 How. St. Tr. 1029). The lessons of history ought not have been replaced in *Fisher* by a doctrine better suited to law school exams than the protection of a fundamental human right.

III. The issues should be resolved in the present case.

This case is the right vehicle for resolution of the questions presented. Numerous other cases over the past decade have yielded only enduring divergence in rationale and result. Mr. Doe’s ordeal has sharpened the issue more acutely than ever before, proving Lord Camden’s dictum all too true.

Without ever having been charged with a crime, Mr. Doe has sat in jail for more than two years as the cost of calling upon the privilege. For the better part of this period, he was held virtually incommunicado, permitted just one 15-minute telephone call per month, because his history as a law enforcement officer prompted segregation in a “special housing unit.” Despite

the proliferation of cases, other persons have not been willing to pay so heavy a price. So far as the reported decisions show, the longest anyone has previously spent in custody for contempt of an order compelling divulgence of a password is eight months. *See Grand Jury Subpoena Dated March 25*, 670 F.3d at 1340 & n.12. In those cases where disclosure has been compelled, the target has in each instance pled guilty or nolo contendere, apparently unconditionally. In consequence, the issue has not reached this Court despite the confusion and discord in the lower courts.

The time is now to rescue the imperiled rule that must prevail: the right against self-incrimination prohibits forcing a person to cough up information in aid of investigators' search for evidence to be used against him in a criminal case. That is as true of a computer password as any other contents of one's own mind.

CONCLUSION

The petition should be granted to resolve discord in the lower courts and vindicate the Fifth Amendment right against self-incrimination.

Respectfully submitted,

/s/ Keith M. Donoghue

KEITH M. DONOGHUE
Assistant Federal Defender
Counsel of Record

BRETT G. SWEITZER
Assistant Federal Defender
Chief of Appeals

LEIGH M. SKIPPER
Chief Federal Defender

Federal Community Defender Office
for the Eastern District of Pennsylvania
Suite 540 West, Curtis Center
601 Walnut Street
Philadelphia, PA 19106
(215) 928-1100

Counsel for Petitioner