APPEAL NUMBER 15-3537

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

UNITED STATES OF AMERICA,
Appellee

v.

APPLE MACPRO COMPUTER, et al.

*JOHN DOE,
Movant Appellant

# BRIEF FOR APPELLANT

Appeal from Judgment of Contempt Entered in the United States District Court for the Eastern District of Pennsylvania, at Case Number 15-mj-00850 by the Honorable L. Felipe Restrepo

KEITH M. DONOGHUE
Assistant Federal Defender

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
601 Walnut Street, Suite 540 West
Philadelphia, PA 19106
(215) 928-1100

# TABLE OF CONTENTS

**PAGE**

**TABLE OF CONTENTS**
**(continued)**

**PAGE**

**TABLE OF CONTENTS**
**(continued)**

**PAGE**

**TABLE OF CONTENTS**
**(continued)**

**PAGE**

# TABLE OF AUTHORITIES

**FEDERAL CASES** **PAGE**

## TABLE OF AUTHORITIES
**(continued)**

**FEDERAL CASES** **PAGE**

# TABLE OF AUTHORITIES
**(continued)**

**FEDERAL CASES** **PAGE**

# TABLE OF AUTHORITIES
**(continued)**

**FEDERAL CASES** **PAGE**

## TABLE OF AUTHORITIES
**(continued)**

**FEDERAL CASES** **PAGE**

# TABLE OF AUTHORITIES
**(continued)**

**FEDERAL CASES** **PAGE**



**FEDERAL STATUTES** **PAGE**

## TABLE OF AUTHORITIES
**(continued)**

**STATE CASES** **PAGE**



**FEDERAL RULES** **PAGE**



**OTHER AUTHORITY** **PAGE**

## STATEMENT OF SUBJECT MATTER AND APPELLATE JURISDICTION

The district court exercised jurisdiction pursuant to the All Writs Act, 28 U.S.C. § 1651, and ordered appellant to give evidence in advance of potential criminal charges. (App. 3; *see* App. 53-54, 58).[1] This was error because the Act does not supply jurisdiction over pre-indictment criminal investigations, as detailed below.

Appellant has been confined under a judgment of civil contempt predicated on non-compliance with the district court's order. (App. 11-12). The present appeal was instituted by timely notice from the judgment of contempt. (App. 1-2). This Court has jurisdiction under 28 U.S.C. § 1291, providing for appeal from a final judgment of a district court. *In re Grand Jury*, 705 F.3d 133, 142-43 (3d Cir. 2012) ("A district court's contempt order is itself immediately appealable because it is a final judgment imposing penalties on the willfully disobedient witness in what is effectively a separate proceeding.")

[1] "App." followed by a number denotes the relevant page of the joint appendix.

## STATEMENT OF RELATED CASES AND PROCEEDINGS

The subject matter of this case was previously before the Pennsylvania Court of Common Pleas in and for Delaware County at *In re Investigating Grand Jury IX (Encrypted Electronic Devices*), MD No. 781 of 2015. By order dated June 24, 2015, that court upheld a claim of Fifth Amendment privilege raised by appellant herein and declined to order him to divulge the passcodes to several devices running Apple encryption software. (App. 18; *see* App. 187-190).

The United States thereafter obtained an order from the district court compelling appellant to divulge the passcodes. Appellant was subsequently held in contempt of the decryption order, giving rise to this appeal.

Counsel is aware of no other case or proceeding — completed, pending or about to be presented to this Court or any other court or agency, state or federal — that is in any way related to this appeal.

## STATEMENT OF THE ISSUES

### I.

**Whether subject matter jurisdiction was lacking in the district court because proceedings to compel the giving of evidence in advance of potential criminal charges are entrusted by federal law to the grand jury.**

Preservation of Issue

The issue was not preserved. "[D]efects in subject matter jurisdiction require correction regardless of whether the error was raised in district court." *United States v. Cotton*, 535 U.S. 625, 630 (2002).

### II.

**Whether compelling the target of a criminal investigation to recall and divulge an encryption passcode transgresses the Fifth Amendment privilege against self-incrimination.**

Preservation of Issue

The issue was preserved by written motion asserting that the Fifth Amendment barred issuance of an order compelling appellant to supply the passcode needed to decrypt several digital devices previously seized by law enforcement agents. (App. 73-78). A magistrate judge denied the motion. (App. 4-5).

## STATEMENT OF THE CASE

1. *Overview*

The government seeks to force appellant, identified herein as John Doe, to recall and type in the passcode or passcodes needed to "decrypt" two hard drives seized from his residence.[2] A magistrate judge so ordered, exercising jurisdiction pursuant to the All Writs Act. *See* 28 U.S.C. § 1651. After Mr. Doe appeared at a local district attorney's office and entered numerous passcodes that failed to unlock the devices, he was held in contempt and placed in custody. He has not been charged with any crime.

This course of events offends the constitutional guarantee that no person shall be compelled to be a witness against himself. Because the All Writs Act did not supply jurisdiction for the proceedings below, and because even if it did the Fifth Amendment protects against compelled disclosures of the kind sought by the government, Mr. Doe must be released from custody immediately.

---

[2] As there are two hard drives, this brief hereinafter refers to "passcodes." The government represents that due to the drives' encryption with Apple's FileVault software, forensic examiners have been unable to view their contents. (App. 55). While law enforcement agencies are commonly able to bypass a simple log-on password, encryption involves a more sophisticated process that scrambles data, rendering it unreadable, unless the passcode is entered. (App. 296-299, 314-315).

2. *The encrypted devices*

In early 2015, a team of investigators working out of the Office of the District Attorney for Delaware County, Pennsylvania, were surveilling a public online network called Freenet, which allows users to communicate and share files in a secure environment. (App. 37). In the course of the investigation, a team of local and federal law enforcement agents executed a state warrant at appellant's home to search for evidence of child pornography. (App. 37, 116, 146, 290).

Contemporaneously with the warrant's execution, several officers met with appellant at his place of employment. (App. 6, 352-354). According to subsequent testimony, Mr. Doe advised that he had "encryption on his computer," stated that he did not wish to supply any passcode, and asked to speak with an attorney. (App. 354). Officers meanwhile seized a number of digital devices, among them an Apple Mac Pro computer, an iPhone 5S, and two external hard drives. (App. 116-117).

Several months after the seizure, around the time of Memorial Day, members of Mr. Doe's family summoned police to a gathering at which Mr. Doe was present. (App. 102-103, 252-253). According to subsequent testimony from Mr. Doe's sister, he had permitted family members to view a video and photographs on an iPhone 6. (App. 254-256). The images allegedly focus on the

clothed genital area of two nieces, aged four and six. (App. 128). A responding officer took custody of the phone. (App. 257).

3. *The decryption order*

In June 2015, investigators sought to compel Mr. Doe to divulge passcodes for certain of the seized devices by means of a proceeding in the Court of Common Pleas in Delaware County. (App. 18; *see* App. 187-190). Following a hearing, the Honorable Chad F. Kenney determined such compulsion would be unconstitutional. Citing numerous cases, President Judge Kenney wrote that Mr. Doe "has properly invoked the Fifth Amendment privilege against self-incrimination when indicating that he would neither perform the act of decrypting the electronic devices, seized by the Commonwealth, nor provide the passwords to the Grand Jury for the electronic devices." (App. 18).

Investigators turned to federal court, where an Assistant United States Attorney applied pursuant to the All Writs Act, 28 U.S.C. § 1651, for an order commanding Mr. Doe to decrypt and produce the contents of the iPhone seized at the family gathering, the Mac Pro, and the external hard drives. (App. 53-54). As framed by the government, the application sought Mr. Doe's assistance in the execution of a newly obtained federal warrant authorizing a search of the devices. (App. 59; *see* App. 24, 49, 51).

The application acknowledged that Fifth Amendment concerns are raised when the government seeks to compel an investigative target to recall and divulge the passcode to an encrypted device. (App. 60-64). The government contended, however, that such compulsion would not violate the privilege against self-incrimination under the "foregone conclusion" rule. (App. 61-64). That doctrine holds that the government may compel the production of papers whose existence is already so well established that the act of production is a matter merely of the surrender of evidence, rather than the disclosure of new information. *Fisher v. United States*, 425 U.S. 391, 411 (1976).

Just three days after the government's filing, without hearing from Mr. Doe or his counsel, a magistrate judge signed a form of order supplied by the government. (App. 3). The order commanded Mr. Doe to appear at the district attorney's office in Delaware County and there "produce" the (previously seized) devices in an unencrypted state. (App. 3). The order made no mention of the Fifth Amendment privilege against self-incrimination.

Prior to the deadline provided in the order, Mr. Doe's attorney sought an extension of time to respond to the government's All Writs Act application. (App. 67). Over the government's opposition, the court stayed the order and granted counsel two weeks. (App. 68-69, 72). Counsel then filed a timely motion to quash on Fifth Amendment grounds, submitting that the foregone conclusion doctrine did

not apply because the government had not demonstrated "the existence of and possession of [the putative evidence] with 'reasonable particularity.'" (App. 76). The motion submitted that Mr. Doe could call upon Fifth Amendment protection because the government, in seeking to compel him to divulge the passcodes, was demanding that he "use the contents of his mind against himself." (App. 77).

The next day, the magistrate judge construed the motion to quash as a "motion for reconsideration," and denied it in a footnoted order adopting the government's 'foregone conclusion' argument. (App. 4-5). In support of his ruling, the Honorable Thomas J. Rueter cited representations put forward in an affidavit of a Homeland Security agent that had accompanied the federal warrant application made shortly in advance of the All Writs application. (App. 5; *see* App. 37-42). The judge treated the affidavit as sufficient to establish that "there are images on the electronic devices that constitute child pornography." (App. 5).

4. *The passcodes*

Following the magistrate judge's rejection of his motion, Mr. Doe appeared with counsel at the district attorney's office. In the interim, investigators had decrypted the Mac Pro using a recovery key discovered on the iPhone 5S seized

from Mr. Doe's home.[3] (App. 121-123, 129, 297-301, 390). There was no child pornography on the iPhone 5S or Mac Pro. (App. 119, 129). Remaining were the iPhone 6 seized at the family gathering and two external hard drives.

A forensic examiner from the district attorney's investigative division, Detective Christopher Tankelewicz, later testified regarding the process followed when Mr. Doe came in. (*See* App. 135-141, 150-152, 160, 318-320, 324, 327, 341-343). After several tries, Mr. Doe succeeded in unlocking the iPhone 6, as well as an encryption application on the phone. (App. 139, 151-152, 326-327, 341-343, 347-348). As to the hard drives, Mr. Doe reportedly stated that he could not recall the passcodes. (App. 136). Regardless, he "attempted to unencrypt the [first hard drive], and then he moved onto the [other], he went back and forth between them attempting to enter the pass codes." (App. 141-142, 151). Tankelewicz testified that the passcodes entered by Mr. Doe were lengthy, with the total number of characters scrolling past the edge of the interface's passcode 'box.' (App. 150-151).

Tankelewicz also testified that Mr. Doe had requested a legal pad to keep track of each entry he attempted, which Tankelewicz agreed he did "meticulously

---

[3] A recovery key is a computer-generated code for recovering encrypted contents. (App. 122). It appeared in a photograph stored on the phone. (App. 390).

line-by-line-by-line." (App. 160; *see* App. 141). The investigators eventually attempted to facilitate Mr. Doe's efforts by adjusting the configuration of the devices so that the graphical interface resembled the one a user would ordinarily see at a Mac Pro screen, instead of the screen presented by the district attorney's forensic application. (App. 155-156). In the end, none of the passcodes worked. (App. 328).

5. *The hearings*

The government haled Mr. Doe back in to court by motion for an order to show cause why he should not be held in contempt. (App. 79). It contended that Mr. Doe's unlocking of the iPhone 6 and entry of passcodes for the hard drives "was a deliberate façade designed to feign compliance with the Court's order." (App. 81). The government also renewed its submission that child pornography would be found on the hard drives. (App. 81). An initial hearing was convened before Magistrate Judge Rueter. After hearing testimony, Judge Rueter agreed with the government's deliberate-ruse theory and certified findings in support of a judgment of contempt. (App. 6-10). The matter proceeded to a hearing before the district court, the Honorable L. Felipe Restrepo presiding, which heard further evidence and then held Mr. Doe in contempt. *See* 28 U.S.C. § 636(e)(6); *Taberer v. Armstrong World Indus., Inc.*, 954 F.2d 888, 902-03 (3d Cir. 1992) (reviewing

procedure for adjudgment of civil contempt in proceedings before magistrate judge).

i. *Sister Doe*

At both hearings, evidence was heard as to whether the government could in fact demonstrate to a "foregone conclusion" that child pornography was encrypted on the hard drives. In this connection, the government first called Mr. Doe's younger sister. She claimed he had shown her child pornography using a Mac Pro more than a year before the seizure. (App. 96, 240). Later she moved in to his apartment. (App. 236, 240). She did not speak of having ever seen child pornography over the five months she lived there. (*See* App. 236, 277).[4]

Nor had Mr. Doe's sister made any mention of child pornography when police interviewed her at the time of the family gathering where the iPhone 6 with images of Mr. Doe's nieces was seized. (App. 104). More than a month later, in early July 2015, Mr. Doe's sister moved out of his apartment and he stopped paying her living expenses. (App. 106-107, 257-258). At around this time she approached police with the account of supposedly viewing child pornography at

[4] Mr. Doe's sister resided with him for two periods, once in December 2013 and once from February to July 2015. (App. 93-94, 234-236, 277). At one point she indicated her putative viewing of child pornography with Mr. Doe preceded the first period they lived together, but at another point she stated she believed it was between the two periods. (*See* App. 96, 240).

Mr. Doe's home. (App. 107, 268-271). In her testimony, she described the content as "mostly children in various states of dress, mostly nude or almost nude." (App. 248). The prosecutor elicited testimony that there were some images portraying children engaged in sexual activity. (App. 101, 248).

The defense urged the court that the sister's credibility was suspect, and pointed out that, in any event, she could not say whether child pornography was on the hard drives which the government sought to have decrypted, rather than some other digital storage device connected to the Mac Pro more than a year before the seizure. (App. 109-110, 196-197, 203-205, 245, 264-265, 375). The government ultimately contended that Mr. Doe's sister need not be credited to enforce the decryption order. (App. 370).

ii. *Forensic testimony*

On the government's view, there was sufficient forensic evidence to make it a "foregone conclusion" there was child pornography on the hard drives. In this regard, its sole witness was Detective Tankelewicz.

Tankelewicz testified it was his "best guess" that child pornography was on the hard drives. (App. 346). He based this opinion largely on what he called "content hash keys," meaning "a unique key for each individual image or movie you can potentially download from Freenet," the peer-to-peer network under

investigation. (App. 306).[5] Tankelewicz admitted he had no training in Freenet, (App. 305), but had discovered that each content hash key — consisting of a long sequence of characters — brings up a corresponding file when entered by a user to query the network. (App. 305-307, 350, 391).

According to Tankelewicz, there were "references" on the Mac Pro to some 20,000 content hash keys associated with Freenet message boards, some or all of which boards had names "consistent with child pornography." (App. 312; *see* App. 306, 339, 349).[6] By independent queries of Freenet, Tankelewicz determined that three of the content hash keys corresponded to child pornography files. (App. 307, 350, 391). As best as can be made out from the rather ambiguous testimony, Tankelewicz's opinion was not that these files were necessarily on the hard drives, (*see* App. 350), but that the "references" on the Mac Pro indicated a user had set up access to the message boards where the content hash keys or corresponding files resided. (App. 311-312, 339-340; *see also* App. 213 (representing that forensic

---

[5] In addition to Freenet, a software application called Parallels had been installed on the Mac Pro. (App. 304). Parallels allows users to set up a "virtual machine" on which a second operating system — in this case, Microsoft's Windows Vista — can be run simultaneously with Apple's operating system. (App. 304). The maker of Parallels describes it as "[t]he #1 choice of Mac users for over 8 years, with over 5 million copies sold." *See* www.parallels.com.

[6] The names stated by the prosecutor were "Toddler CP," "PTHC," "Hussie Fan," "PETO mom," and "Lolita." (App. 312-313).

examination showed use of Freenet "to access or attempt to access" message boards or files associated with the boards)).

The sole file Tankelewicz specifically described as possibly stored on a hard drive was a download of an image depicting "a four or five-year-old girl with her dress lifted up, but the image itself was small so you really couldn't see what was going on with the image." (App. 308). When asked by the prosecutor whether this image "went to the hard drives," Tankelewicz said it was "a possibility." (App. 309).[7]

6. *The contempt judgment*

Notwithstanding the reception of Detective Tankelewicz's forensic testimony at the two hearings, neither the magistrate nor district judge revisited the magistrate judge's earlier ruling that it was a "foregone conclusion" there was child pornography encrypted on the drives. In fact, neither the magistrate's certified findings nor the district court's contempt order cited Tankelewicz's testimony at all. (*See* App. 6-17). As a result, the only finding on this point is the one the magistrate judge had earlier based on the representations made by a

[7] While Detective Tankelewicz referred at one point to "two" child pornography images that he saw in the ''Downloads' folder," (App. 308), at other points he referred to a single file, (App. 340, 346). In any event, the only image he ever identified was the girl in the dress. (App. 308).

Homeland Security agent in the affidavit for the federal search warrant obtained in the days before the government's All Writs Act application. (App. 5).

The judges' post-hearing findings instead went strictly to whether Mr. Doe was able to recall the passcodes, such that he was in contempt of the decryption order. (App. 9-10; *see* App. 381-382). As noted above, the prosecution contended that Mr. Doe had engaged in a deliberate ruse when he appeared at the district attorney's office, unlocked the iPhone 6, and made numerous passcode entries in the several forensic interfaces set up by investigators for the hard drives. Ultimately, the district court indicated its view that Mr. Doe was able to recall the passcodes. (App. 381-384; *compare* App. 16).[8]

More formally, the court concluded that, Mr. Doe having "offer[ed] no on-the-record explanation for his failure to comply," he was in contempt of the decryption order. (App. 16). The court committed him to the custody of the United States Marshals, (App. 384-385; App. 11-12, 16-17), who are holding him at the Federal Detention Center in Philadelphia pursuant to the judgment of civil contempt. Under the order, he is to remain confined until such time as he recalls and divulges the passcodes to the hard drives. (App. 11 (requiring Mr. Doe to

[8] Nothing in this brief should be construed as an admission that Mr. Doe in fact does or does not recall the passcodes. He presently challenges the underlying decryption order, so that the issue here is the unlawfulness of compelling him to disclose the fact of such recollection, or lack of it, at all.

"permit[] access to the two external hard drives … in a fully unencrypted state"); App. 17).

This timely appeal follows. The validity of the decryption order is before the Court as it forms the basis for the judgment of contempt. *John T. ex rel. Paul T. v. Delaware County Intermediate Unit*, 318 F.3d 545, 559 (3d Cir. 2003); *see also In re Grand Jury*,705 F.3d 133, 142-50 (3d Cir. 2012) (applying rule that witness commonly *must* be held in contempt to raise claim of privilege).

## SUMMARY OF ARGUMENT

### I.

The district court lacked jurisdiction to issue a decryption order under the All Writs Act, 28 U.S.C. § 1651. That Act does not supply jurisdiction where another law specifically addresses the pertinent subject matter. Here, the subject matter is committed to the traditional grand jury procedure defined by the Federal Rules of Criminal Procedure and codified in the Fifth Amendment. It is through that procedure, not an ad hoc writ, that a suspect or witness may be compelled to give evidence in advance of potential criminal charges. Should he fail to comply, he is subject to a maximum of 18 months' imprisonment, *see* 28 U.S.C. § 1826(a), not perpetual confinement in an All Writs proceeding.

The reported decisions indicate that, prior to this case, the government has proceeded via the grand jury when seeking to compel a suspect to divulge his encryption passcode before possible indictment. This case should be no different. Because the district court was without jurisdiction to compel decryption pursuant to 28 U.S.C. § 1651, appellant is not in contempt of any valid order. The judgment of civil contempt must be vacated and appellant released.

### II.

The district court erred in failing to uphold Mr. Doe's claim of Fifth Amendment privilege. The privilege against self-incrimination bars the

government from forcing a suspect to disclose the contents of his own mind, and therefore protects against the compelled disclosure of the passcode for an encrypted device.

The Supreme Court has recognized that divulgence of the code to a combination lock is testimonial per se, so that the code's disclosure may not be compelled over a claim of privilege. The same rule necessarily applies to divulgence of an encryption passcode — a virtual combination lock — especially given the uniquely revealing nature of the contents of digital devices like smart phones and hard drives. In light of the controlling Supreme Court precedent, the district court erred.

Lower courts have typically failed to recognize that disclosure of a passcode is testimonial in itself, instead erroneously viewing decryption within the rubric of the "act-of-production" doctrine. That doctrine permits the government to compel the surrender of specifically defined documents whose existence, location, and authenticity are a "foregone conclusion." Because decryption involves not the production of a discrete set of documents but the disclosure of the entire contents of a digital device — including contents whose existence is altogether unknown to the government — the act-of-production doctrine has no place.

In any event, the act-of-production doctrine would support Mr. Doe's claim of privilege if applied here. The government has not, as required by the relevant

decryption precedents, demonstrated that the storage of any particular file or files on the hard drives is a foregone conclusion. Instead, it put forward only a suspect witness who gave attenuated testimony and a forensic examiner who was unable to offer any authoritative opinion regarding the contents of the hard drives.

## ARGUMENT

### I.

### The district court exceeded its jurisdiction in issuing the decryption order, in that proceedings to compel the giving of evidence in advance of potential criminal charges are entrusted by federal law to the grand jury.

Standard of Review

Review of a district court order's authority to grant relief pursuant to the All Writs Act is plenary. *See Grider v. Keystone Health Plan Central, Inc.*, 500 F.3d 322, 328 (3d Cir. 2007) (reviewing injunction). Review of subject matter jurisdiction is likewise plenary. *United States v. Merlino*, 785 F.3d 79, 82 (3d Cir. 2015).

Discussion

Ordinarily, when the United States seeks to compel a witness to testify or produce records in a criminal investigation that has not advanced to the filing of charges, a prosecutor subpoenas the witness to appear before a grand jury. *See, e.g.*, *In re Grand Jury &c.*, 171 F.3d 826, 831-32 (3d Cir. 1999). Reported cases

indicate this is as true of the decryption of digital storage media as the compelled production of any other evidence. *See In re Grand Jury Subpoena Duces Tecum Dated Mar. 25*, 670 F.3d 1335 (11th Cir. 2012); *In re Grand Jury Subpoena to Sebastian Boucher*, No. 06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009).

In this case, however, the United States chose a different course, applying to a magistrate judge pursuant to the All Writs Act, 28 U.S.C. § 1651, for an order compelling appellant to divulge the passcodes for two external hard drives, a smart phone, and a computer. The order that subsequently issued was invalid because the All Writs Act does not supply jurisdiction to circumvent the pre-indictment investigative powers properly lodged in the grand jury.

### A. The All Writs Act does not supply jurisdiction over subject matter specifically addressed by other provisions of law.

Originally enacted as part of the Judiciary Act of 1789, the All Writs Act authorizes federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651; *see Pennsylvania Bureau of Correction v. United States Marshals Service*, 474 U.S. 34, 40-42 (1985) (reviewing history of provision). Two limitations upon this authority are virtually as venerable as the statute itself.

First, while authorizing writs "in aid of" jurisdiction, the Act does not confer "any federal subject-matter jurisdiction in its own right[.]" *Sygenta Crop Protection, Inc. v. Henson*, 537 U.S. 28, 31 (2002) (citation omitted); *see Price v.*

*Johnston*, 334 U.S. 266, 279 (1948); *United States v. Plumer*, 27 F. Cas. 561, 573 (C.C. Mass. 1859) (No. 16,056).

Second, where "a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling." *Pennsylvania Bureau of Correction*, 474 U.S. at 43; *Massey v. United States*, 581 F.3d 172, 174 (3d Cir. 2009) (per curiam); *see McIntire v. Wood*, 7 Cranch (11 U.S.) 504, 506 (1813). Indeed, as originally written, the Act authorized "writs not specifically provided for by statute." Judiciary Act of 1789, § 14, 1 Stat. 81-82, *quoted in Pennsylvania Bureau of Correction*, 474 U.S. at 40.

Today, while the Act "empowers federal courts to fashion extraordinary remedies when the need arises, it does not authorize them to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate." *Pennsylvania Bureau of Correction*, 474 U.S. at 31. Rather, it "invests a court with a power essentially equitable and, as such, not generally available to provide alternatives to other, adequate remedies at law." *Clinton v. Goldsmith*, 526 U.S. 529, 537 (1996).

These twin precepts make clear that the All Writs Act cannot supply jurisdiction over subject matter specifically addressed by other provisions of law. *See Sygenta Crop Protection, Inc.*, 537 U.S. at 33 (holding All Writs Act does not vest district courts with the "original subject-matter jurisdiction" required by 28

U.S.C. § 1441(a) to support removal of civil actions brought in state courts); *Council Tree Communications, Inc. v. FCC,* 503 F.3d 284, 293 (3d Cir. 2007) (holding All Writs Act not to supply jurisdiction to entertain untimely petition for review of administrative action where filing window defined by 28 U.S.C. § 2344).

Among the provisions of law that may bar recourse to the All Writs Act are rules adopted under the Rules Enabling Act. *See* 28 U.S.C. § 2071 *et seq.*; *Carlisle v. United States*, 517 U.S. 416, 429 (1996) (Rules of Criminal Procedure); *Grider v. Keystone Health Plan Central, Inc.*, 500 F.3d 322, 328 (3d Cir. 2007) (Rules of Civil Procedure). In *Carlisle*, the defendant contended that the All Writs Act conferred power upon the district court to entertain a motion for judgment of acquittal that was untimely under Criminal Procedure Rule 29. *See* 517 U.S. at 428. The Supreme Court held that this argument "need not detain us long," explaining that Rule 29 provides "the applicable law" for purposes of the limitation upon recourse to the All Writs Act where "a statute specifically addresses the particular issue at hand." *Id.* at 429. *See also Grider*, 500 F.3d at 332 (Civil Procedure Rule 23(e) supplied "adequate remedy at law" foreclosing "relief under the All Writs Act").

### B. The grand jury procedure established by law addresses the compelled production of evidence in advance of criminal charges.

Here, the applicable law is not the All Writs Act, but the well-established grand jury procedure for compelling witnesses to give evidence in criminal

investigations before return of any indictment. The procedure is today enshrined in Rules 6 and 17 of the Rules of Criminal Procedure, in statutory provisions including 28 U.S.C. § 1826, and of course in the Fifth Amendment.[9] In American law, the "grand jury's historic functions survive to this day." *United States v. Calandra*, 414 U.S. 338, 343 (1974); *see id.* at 346 n.4.

The role of the grand jury subpoena in the early stages of criminal investigation is "unique," encompassing inquiry "into all information that might possibly bear on its investigation." *United States v. R. Enterprises*, 498 U.S. 292, 297 (1991); *see Branzburg v. Hayes*, 408 U.S. 665, 688 (1972) (subpoena power "essential" to grand jury). This subpoena power, moreover, is exceedingly broad: "In the context of a grand jury inquiry, the public has a right to every man's evidence, except for those persons protected by a constitutional, common-law, or statutory privilege." *United States v. Nixon*, 418 U.S. 683, 709 (1974) (approving subpoena to President of United States) (internal quotation marks, brackets, and ellipses omitted).[10]

---

[9] United States Const. amend. V ("No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury[.]").

[10] It bears pausing to note that "the privilege against self-incrimination carves out a significant exception to the government's ability to obtain every man's evidence." *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25*, 670 F.3d

*continued…*

Under Criminal Procedure Rule 6, the district court "must" summon a grand jury "[w]hen the public interest so requires." Fed. R. Crim. P. R. 6(a). The Rule specifies the size of the body, limits its term of service, and defines the vote required to indict. Fed. R. Crim. P. R. 6(a)(1), (f), (g). It also provides for confidentiality by limiting the disclosure that may be made of "matter[s] occurring before the grand jury." Fed. R. Crim. P. R. 6(e)(2)(B).

Rule 17, in turn, governs the issuance and enforcement of grand jury subpoenas. *See In re Grand Jury Proceedings (Schofield II)*, 507 F.2d 963, 964 n.2 (3d Cir. 1975). A motion remedy is provided by which a witness may seek to quash or modify a subpoena. Fed. R. Crim. P. R. 17(c)(2). Where a subpoena is challenged, the government must make a preliminary showing by affidavit that the demand for evidence is a valid one. *See In re Impounded*, 178 F.3d 150, 158-59 (3d Cir. 1999) (reviewing procedure followed under *In re Grand Jury Proceedings (Schofield I)*, 486 F.2d 85, 93 (3d Cir. 1973), and *Schofield II*, 507 F.2d at 966).

Reliance on the grand jury's subpoena power not only facilitates effective investigation, but affords several protections to summoned witnesses. In addition to the motion-to-quash procedure and requirement that the government make a

---

1335, 1341 (11th Cir. 2012). The Fifth Amendment privilege is the "most important" of the exemptions from the customary duty to give evidence before the grand jury. *Kastigar v. United States*, 406 U.S. 441, 444 (1972).

preliminary showing by affidavit, the body's secrecy protects a target "who is exonerated from disclosure of the fact that he has been under investigation." *In re Grand Jury Subpoena*, 223 F.3d 213, 218 (3d Cir. 2000) (internal quotation marks and brackets omitted). In challenging a grand jury subpoena, moreover, a witness has at least a qualified right to discovery. *Schofield I*, 486 F.2d at 93; *see also In re Grand Jury Investigation (DiLoreto)*, 903 F.2d 180, 183 (3d Cir. 1990) (holding contemnor entitled to disclosure of grand jury's commencement and termination dates).

Perhaps most importantly, Congress has provided a maximum penalty of 18 months' confinement for "recalcitrant witnesses" who refuse without just cause to comply with orders enforcing grand jury subpoenas. *See* 28 U.S.C. § 1826(a); *In re Grand Jury Investigation (Oreski)*, 865 F.2d 578, 579 (3d Cir. 1989); *see also Schofield I*, 486 F.2d at 88-93 (reviewing witness's rights in Section 1826 proceeding). Indeed, confinement may in no event exceed the remaining "term of the grand jury," so that the maximum will commonly be far less than 18 months. 28 U.S.C. § 1826(a)(2); *see Gelbard v. United States*, 408 U.S. 41, 45 (1972); *Harris v. United States*, 582 F.3d 512, 516 (3d Cir. 2009). The recalcitrant witness statute also contemplates bail pending appeal and calls for appeals to be resolved within 30 days. 28 U.S.C. § 1826(b).

### C. In proceeding under the All Writs Act, the district court exceeded its jurisdiction and deprived Mr. Doe of rights afforded targets who have not been charged with any offense.

Here, the All Writs Act did not supply jurisdiction to enter an order compelling Mr. Doe to recall and divulge passcodes to the hard drives because recourse to the Act displaced the grand jury from its "essential" role in the "federal criminal justice system." *In re Grand Jury Subpoena*, 223 F.3d at 216.

As much is clear from other reported decryption cases. Whenever the issue has arisen in advance of potential federal charges, it has been by way of a grand jury subpoena. *See In re Grand Jury Subpoena Duces Tecum Dated Mar. 25*, 670 F.3d 1335 (11th Cir. 2012); *In re Grand Jury Subpoena to Sebastian Boucher*, No. 06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009). There is no sign the government has ever before sought or obtained an All Writs order to compel an uncharged suspect to give up his passcode. In the one reported case where the government proceeded under the All Writs Act, the defendant had already been indicted, so recourse to the grand jury was no longer available. *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012); *see In re Grand Jury Proceedings (Johanson)*, 632 F.2d 1033, 1041 (3d Cir. 1980) ("It is a firmly entrenched rule that once a defendant has been indicted, a prosecutor may not use a grand jury's investigative powers for the purpose of securing additional evidence against the defendant for use in the upcoming trial."). Conversely, the indictment having been

filed in *Fricosu*, the district court had no need of the All Writs Act to exercise jurisdiction over the federal criminal matter. *See* 18 U.S.C. § 3231.

Though the government has affirmatively represented that Mr. Doe is "the target of multiple state and federal grand jury investigations," (App. 53), it bypassed the federal grand jury for decryption purposes. In doing so, the government has stripped appellant of significant protections. Though Mr. Doe sought to challenge the All Writs order by a motion to quash of the kind that will be entertained in opposition to a grand jury subpoena, *see* Fed. R. Crim. P. R. 17(c)(2), the judge construed the filing as a motion for reconsideration, (App. 4), thus affording only sharply circumscribed review to his claim of Fifth Amendment privilege. *See United States ex rel. Schumann v. AstraZeneca Pharmaceuticals LP*, 769 F.3d 837, 848 (3d Cir. 2014) (delineating limited circumstances under which motion for reconsideration may be granted).[11] In rejecting that claim, the district court entertained no testimony but instead relied on an affidavit sworn before another magistrate judge by an agent who has since disappeared from this case. (*See* 8/27 Order 2; Warrant Application 1). Though the government later put on testimony relating to the contents of the hard drives, neither the magistrate nor

[11] The magistrate judge's order did not specifically state the standard of review implied by its construction of the motion as one for reconsideration rather than to quash.

district judge ever revisited the denial of the motion to quash and consequent overriding of the privilege.

Now, based on a putative contempt, appellant has been committed to custody in perpetuity, instead of for the limited term of 18 months, or less, properly fixed by statute. The manner of proceeding has also risked publication of appellant's identity and the opprobrium that will follow from revelation of the nature of the uncharged allegations. Worst of all, these consequences have resulted from a proceeding that was beyond the district court's jurisdiction ever to entertain.

It is with the grand jury, not the district court, that responsibility lays for criminal investigations that have not advanced to the filing of charges. *See Calandra*, 414 U.S. at 343. The All Writs Act does not change that. Because the district court was without jurisdiction under the Act to compel the giving of evidence in advance of charges, the decryption order must be vacated. As no valid order underlies the contempt judgment, Mr. Doe must be released from custody forthwith.

### D. The decryption order is not equivalent to the conscription of a third party's assistance to facilitate the execution of a warrant.

The government contended below that the court had the power to enter the requested order under *United States v. New York Telephone Co.*, 434 U.S. 159 (1977). That is mistaken because the order considered in *New York Telephone* was

not, like the order here, a command to a witness to testify or otherwise produce evidence. Rather, it was a command to a third party to facilitate the off-site execution of a warrant. *See* 434 U.S. at 161-63.

More specifically, *New York Telephone* approved an All Writs order commanding a closely regulated public utility to help install a "pen register," meaning a device that would record the numbers dialed on a particular rotary telephone. 434 U.S. at 161-162 & n.1; *id.* at 174. The Court described the assistance impressed by the writ as "meager," *id.* at 174, and its object as manifestly consistent with the intent of Congress, *id.* at 176-78. Based on these several considerations, the Court upheld the exercise of All Writs Act jurisdiction. *Id.* at 178.

Here, the government has sought to evoke *New York Telephone* by framing its All Writs application as if it seeks only to have Mr. Doe "assist in the execution of previously issued search warrants." (App. 64; *see* App. 59). This badly misconceives the issue at hand. Mr. Doe is of course a target, not a third party of the kind considered in *New York Telephone*. Moreover, he is not being asked simply to allow a monitoring instrument to be connected to a device. Rather, the government demands that he call upon the contents of his own mind and disclose passcodes as a witness against himself.

When the government seeks to compel the giving of evidence in advance of possible criminal charges, the process afforded by law is a grand jury subpoena. To permit the government to proceed under the All Writs Act would circumvent this basic principle, and displace the grand jury from its essential role in the federal criminal justice system. The All Writs Act does not supply such jurisdiction.

## II.

## Compelling the target of a criminal investigation to recall and divulge an encryption passcode transgresses the Fifth Amendment privilege against self-incrimination.

### Standard of Review

Where the question presented by a claim of Fifth Amendment privilege is purely one of law, this Court reviews *de novo*. *United States v. Chabot*, 793 F.3d 338, 341-42 (3d Cir.) *cert. denied*, 136 S. Ct. 559 (2015). The privilege's application in the context of compelled decryption is a legal issue subject to plenary review. *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25*, 670 F.3d 1335, 1338 (11th Cir. 2012).

### Discussion

Even had this matter been within the district court's jurisdiction, enforcement of the decryption order would offend the Constitution. The government proposes to force Mr. Doe to recall and divulge the passcodes to two

hard drives in hopes that by doing so he will reveal evidence of the possession of child pornography. This transgresses the constitutional guarantee that no person shall be compelled "to be a witness against himself." U.S. Const. amend. V.

### A. The privilege against self-incrimination protects against compulsion to divulge the contents of one's own mind.

The Fifth Amendment privilege against self-incrimination guarantees that "no person … shall be compelled in any criminal case to be a witness against himself." A complex of values finds expression in the privilege. *See Murphy v. Waterfront Commission*, 378 U.S. 52, 55 (1964). At the most profound level, the privilege reflects the Constitution's "respect for the inviolability of the human personality." *Id.* More concretely, it keeps persons from being put to "the cruel trilemma of self-accusation, perjury or contempt." *Id.* To avoid that intolerable situation, the privilege holds that the government may not obtain its evidence by "the cruel, simple expedient of compelling it from [a suspect's] own mouth." *Miranda v. Arizona*, 384 U.S. 436, 460 (1966). Such protection is essential to an "accusatorial rather than … inquisitorial system of criminal justice." *Murphy*, 378 U.S. at 55.

As defined in the case law, the privilege applies when three elements are satisfied: no person may "be [1] incriminated by his own [2] compelled [3] testimonial communications." *Fisher v. United States*, 425 U.S. 391, 409 (1976). The only element at issue in this case is the requirement that a communication be

"testimonial." (*See* App. 4-5, 61-64). To be testimonial, a communication must "explicitly or implicitly relate a factual assertion or disclose information." *Doe v. United States*, 487 U.S. 201, 210 (1988). Thus, the privilege "usually operates to allow a citizen to remain silent when asked a question requiring an incriminatory answer." *Kastigar v. United States*, 406 U.S. 441, 461 (1972).

The Court's discussion in *Curcio v. United States*, 354 U.S. 118 (1957), helps articulate the concept of the 'testimonial.' In *Curcio*, the secretary-treasurer of a union local was subpoenaed to produce the local's books and records before a grand jury. The official had no standing to invoke the privilege with regard to the documents themselves — as the records' custodian, he was required to turn them over even if in doing so he incriminated himself. 354 U.S. at 119, 122. But the Court unanimously concluded he could not be compelled to answer questions about the location of missing documents because to do so would require him to divulge "the contents of his own mind," contrary "to the spirit and letter of the Fifth Amendment." *Id.* at 128.

Since *Curcio*, the Court has repeated the "contents of his own mind" formulation. *Doe*, 487 U.S. at 211; *United States v. Hubbell*, 530 U.S. 27, 43 (2000). Because the privilege exists to protect "'the dignity of the human mind,'" *United States v. Hubbell*, 167 F.3d 552, 580 (D.C. Cir. 1999), *affirmed*, *supra*, it does not extend to purely physical acts that do not reveal a suspect's knowledge or

belief. Thus, it has been held that a suspect may be compelled to "submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture." *United States v. Dionisio*, 410 U.S. 1, 6 (1973) (internal quotation marks omitted).

### B. An encryption passcode represents the contents of a person's mind, so that the privilege protects against its compelled disclosure.

To illustrate the difference between purely physical acts and acts that express the contents of an individual's mind, the Supreme Court has offered a distinction that is particularly apt with regard to decryption: the difference between handing over the key for a manual lock and divulging the sequence of numbers for a combination lock. *Hubbell*, 530 U.S. at 43. The former is not testimonial while the latter is. *Id.*; *see also United States v. Green*, 272 F.3d 748, 753 (5th Cir. 2001) (holding suspect's opening of combination locks, and consequent revelation of unlawfully possessed firearms, to be testimonial because under Supreme Court precedent "this precise behavior was testimonial communication so expressing the defendant's mind as to constitute compelled [self-incrimination]").

Justice Stevens pioneered the combination lock metaphor, writing that 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*, 487 U.S. at 219 (Stevens, J., dissenting). The majority quoted the distinction with approval. *Id.* at 210 n.9. The Court as a whole then adopted the metaphor in *United States v. Hubbell*. There, the defendant had been required "to make extensive use of 'the contents of his own mind' in identifying … hundreds of documents" responsive to a subpoena. 530 U.S. at 43. "The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." *Id.* By compelling disclosure, the government had violated the Fifth Amendment. *Id.* at 43-45.

The combination lock analogy demonstrates that the divulgence of an encryption passcode for a hard drive, smartphone, or other personal computing device is testimonial per se. *See* 3 Wayne R. LaFave et al., *Criminal Procedure* § 8.13(a) at 388-89 n.42 (4th ed. 2015) ("revealing the combination stored in one's mind is testimonial"). In a case like this one, the government does not propose to have a suspect undertake a strictly physical act like turning a bolt or touching a digital thumbprint detector on a smart phone. It proposes to force him to recall and divulge the contents of his own mind. Such compulsion violates the Fifth Amendment.

The court so held in *United States v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich. 2010), where Judge Borman relied on the combination lock analogy to

uphold a claim of privilege in response to a demand for the defendant's encryption passcode. The court reasoned that "forcing the Defendant to reveal the password for the computer communicates that factual assertion to the government, and thus, is testimonial — it requires Defendant to communicate 'knowledge,' unlike the production of a handwriting sample or a voice exemplar." 823 F. Supp. 2d at 669. *See also Commonwealth v. Baust*, 89 Va. Cir. 267, at *3-*4 (2014) (disclosure of passcode testimonial whenever passcode "is not known outside of Defendant's mind").

While *Kirschner* involved a grand jury subpoena *ad testificandum*, neither in this case nor elsewhere in the country has the government seriously disputed the premise that divulging an encryption passcode — be it by speaking or by typing — can be testimonial. *See* Reply of United States (DDE #15) in *In Re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant*, E.D.N.Y. Case No. 15-mc-1092, at 21 ("Compelled decryption raises significant Fifth Amendment issues[.]") (Oct. 22, 2015); *SEC v. Huang*, No. 15-cv-269, 2015 WL 5611644, at *2 (E.D. Pa. Sept. 23, 2015) (stating that government agency did "not necessarily disagree" with *Kirschner* and second decryption precedent, discussed below, upholding claim of Fifth Amendment privilege); *see also* Allison Grande, *AG Lynch Rejects 'Parade of Horribles' in Apple Phone Fight*, Law360, Mar. 2, 2016 (reporting statement of Attorney General that order to Apple to assist

decryption does not implicate Fifth Amendment because Apple is third party). Indeed, the government has recognized here that decryption, unlike opening a traditional combination lock, discloses "literally every bit of … personal data" about the user of a device. (App. 223).

This candor highlights the stakes raised by compelled decryption. It is in the very nature of encrypted devices like smart phones and hard drives to create and store an exceptionally broad, sometimes even comprehensive, digital record of a person's life. *See Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (recognizing contents of smart phone to supply "revealing montage of the user's life"). When forensic investigators examine these devices, they conduct a wide-ranging examination of a kind that has caused virtually all of the Circuits to voice Fourth Amendment concerns. *See, e.g.*, *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc); *see also United States v. Stabile*, 633 F.3d 219, 237-38 (3d Cir. 2011). In effect, when the government compels a suspect to divulge his passcode, it compels him to incriminate himself as to each and every aspect of his life, down to the last detail or secret whose revelation might come at a personal cost.

Though the government insists it has no interest in the passcodes themselves, it is wordplay to pretend that it seeks instead to have Mr. Doe "produce" the hard drives in an "unencrypted state." (App. 3). 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 divulge passcodes that will permit access to all of the drives' contents. The fact that the government seeks to have the codes entered into a forensic interface rather than spoken aloud does not change the analysis. It still demands that Mr. Doe divulge the contents of his mind, not demonstrate his typing skills.

In short, because the divulgence of a code — be it to a combination lock or an encryption application — is testimonial per se, the analysis need go no further. Forcing such information from a person's mouth or fingertips in hopes it will lead to the discovery of evidence is a "cruel, simple expedient" of the kind our accusatorial system of criminal justice does not abide. *Miranda*, 384 U.S. at 460. The decryption order unlawfully transgressed the Fifth Amendment privilege against self-incrimination.

### C. The act-of-production doctrine does not apply to compelled decryption.

Although the divulgence of a code is testimonial per se, the lower courts have for the most part erroneously framed decryption as an "act of production." That doctrine properly applies only when the government seeks to compel the disclosure of specifically defined files, not when it seeks to decrypt the entire contents of a smart phone, hard drive, or other digital device.

The act-of-production doctrine was conceived strictly in relation to the Fifth Amendment's application to demands for incriminatory paper documents. *See Fisher v. United States*, 425 U.S. 391 (1976). It integrates two underlying precepts. On the one hand, a person may "be required to produce *specific* documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the privilege." *Hubbell*, 530 U.S. at 35-36 (emphasis added).

On the other hand, demands to turn over files transgress the Fifth Amendment when the act of production may itself tacitly "communicate information about the existence, custody, and authenticity of the documents." *Hubbell*, 530 U.S. at 37. By "producing documents, one acknowledges that the documents exist, admits that the documents are in one's custody, and concedes that the documents are those that the subpoena requests." *United States v. Chabot*, 793 F.3d 338, 342 (3d Cir.), *cert. denied*, 136 S. Ct. 559 (2015).

Within the rubric of the act-of-production doctrine, *Fisher* further articulated a so-called 'foregone conclusion' rule, whereby an act of production may be compelled insofar as "[t]he existence and location of the papers are a foregone conclusion." 425 U.S. at 411. In *Fisher*, "the Government knew exactly what documents it sought to be produced," *Grand Jury Subpoena Dated Mar. 25*, 670 F.3d at 1347, specifically, "working papers prepared by the [target] taxpayers'

accountants that the IRS knew were in the possession of the taxpayers' attorneys," *Hubbell*, 530 U.S. at 44. Because neither the records' existence nor their location were in dispute, and because their authenticity could be established by the accountants rather than the suspects, compelling these particular records' production "add[ed] little or nothing to the sum total of the Government's information." 425 U.S. at 411. The question, *Fisher* explained, was "not of testimony but of surrender." *Id.* (quoting *In re Harris*, 221 U.S. 274, 279 (1911)).

In *Hubbell*, by contrast, the 'foregone conclusion' doctrine did not apply because "[w]hatever the scope of this 'foregone conclusion' rationale…., here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent." 530 U.S. at 44-45; *see also Grand Jury Subpoena Dated Mar. 25*, 670 F.3d at 1345 (explaining that in *Hubbell*, government had no knowledge "other than a suspicion that documents likely existed").

*Fisher* and *Hubbell* make clear that the act-of-production doctrine applies strictly when the government seeks specifically identified files. The act of decryption is not the same thing at all. It does not involve turning over specific files, but revealing *all* of the contents of a smart phone, hard drive, or other digital device. Here, the government is demanding the passcodes so that it can unscramble every last bit of data on two hard drives that together house four

terabytes of storage space, (App. 131, 315) — enough to store a lifetime's worth of personal writings and communications. The revelation of such an extraordinary cache of data does not bear any resemblance to the surrender of a discrete set of paper files whose production is called for in a subpoena. The mismatch between compelled decryption and the act-of-production doctrine is obvious.

### D. Were the act-of-production doctrine to be applied, Mr. Doe's claim of privilege would nonetheless be sustained.

As reviewed in the foregoing, the act-of-production doctrine holds that the government may compel the surrender of any specifically defined file or files whose existence has been shown a "foregone conclusion." To satisfy the foregone conclusion standard, the government must demonstrate "it knows, as a certainty, that each of the myriad documents demanded … in fact is in the appellee's possession or subject to his control." *Matter of Grand Jury Empaneled Mar. 19*, 680 F.2d 327, 335-36 (3d Cir. 1982), *affirmed in relevant part sub nom United States v. Doe*, 465 U.S. 605 (1984). As cases applying the act-of-production doctrine to compelled decryption demonstrate, that standard could not be met were the act-of-production doctrine to be applied.

### 1. As regards decryption, the act-of-production doctrine holds that the government must identify with "reasonable particularity" the file or files whose storage on a device is known to a certainty.

The leading decryption case applying the act-of-production doctrine is the Eleventh Circuit's decision in *Grand Jury Subpoena Duces Tecum Dated March 25*, 670 F.3d 1335 (2012). That case arose in the same posture as this one: on appeal by an investigative target who had been jailed for contempt after invoking his Fifth Amendment privilege in response to a demand for his passcode (albeit by means of a grand jury subpoena rather than an All Writs Act order). The Eleventh Circuit concluded that the decryption order underlying the contempt judgment violated the Fifth Amendment. At oral argument, it ordered the target released from custody. 670 F.3d at 1340 n.12.

The target had come under suspicion after investigators discovered he was the sole guest registered at each of three hotels on occasions when these hotels' Internet Protocol, or 'IP,' addresses had been used by a YouTube.com account suspected of sharing explicit materials involving underage girls. 670 F.3d at 1339. Executing a search warrant, investigators seized two laptops and five external hard drives from the suspect's room at a fourth hotel. *Id.* The devices were encrypted, so that officers could not say anything about their content.

In upholding the suspect's privilege claim, the Eleventh Circuit first concluded that decryption "would require the use of the contents of Doe's mind

and could not be fairly characterized as a physical act that would be nontestimonial in nature." 670 F.3d at 1346. Calling upon the physical lock metaphor, the court stated that "[r]equiring Doe to use a decryption password is most certainly more akin to requiring the production of a combination" than a key. *Id.*

The court went on to hold that the 'foregone conclusion' doctrine did not apply under the longstanding rule that "the location, existence, and authenticity of the purported evidence" must be "known with reasonable particularity." 670 F.3d at 1344 (citing *United States v. Ponds*, 454 F.3d 313, 320–21 (D.C. Cir. 2006), and *In re Grand Jury Subpoena Dated Apr. 18*, 383 F.3d 905, 910 (9th Cir. 2004)). *See also In re Grand Jury Subpoena Duces Tecum Dated Oct. 29*, 1 F.3d 87, 93 (2d Cir. 1993). In the context of decryption, the Eleventh Circuit explained, the reasonable particularity rule does not require the government to know the name of a particular file, but it does require the government "to establish that a file or account, whatever its label, … in fact exist[s]." *Id.* at 1349 n.28. More fully, the government "must show with some reasonable particularity that it seeks a certain file and is aware, based on other information, that (1) the file exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic." *Id.*

The Eleventh Circuit concluded that under the circumstances presented, the government had not shown that "at the time it sought to compel production, [it]

knew to any degree of particularity what, if anything, was hidden behind the encrypted wall." 670 F.3d at 1349; *see also id.*at 1347 (no showing "that the drives actually contain any files," nor "which of the estimated twenty million files the drives are capable of holding may prove useful"). The court thus concluded that the target was entitled to invoke his Fifth Amendment privilege.

Alongside the Eleventh Circuit's analysis, the most thoughtful decision applying the act-of-production doctrine to compelled decryption comes from a district court in this Circuit. In *SEC v. Huang*, No. 15-cv-269, 2015 WL 5611644 (E.D. Pa. Sept. 23, 2015), the issue arose in the context of a motion to compel discovery in a civil action to enforce securities regulations. 2015 WL 5611644 at *1. Judge Kearney described "the personal thought process defining a smartphone passcode" to be testimonial in nature, *id.* at *2, and concluded that the 'foregone conclusion' rule did not apply, *id.* at *4. While the government had shown that the targets "were the sole users and possessors of their respective work-issued smartphones," it had not demonstrated with "'reasonable particularity' the existence or location of the documents it seeks." *Id.* The motion to compel was accordingly denied.

Two other district courts have likewise recognized compelled decryption to implicate the Fifth Amendment, but applied the foregone conclusion doctrine to overrule a claim of privilege. *See United States v. Fricosu*, 841 F. Supp. 2d 1232,

1236 (D. Colo. 2012); *In re Grand Jury Subpoena to Sebastian Boucher*, No. 06-mj-91, 2009 WL 424718, at *3 (D. Vt. Feb. 19, 2009). In *Boucher*, the suspect had been stopped at a border crossing and directed to a secondary inspection area. In course of the inspection, he showed an agent the "Z drive" on his laptop computer, where the agent located what appeared to be child pornography. 2009 WL 424718 at *2. After the laptop was seized, agents discovered that the Z drive had become encrypted. *Id.* In light of the agent's earlier inspection, Judge Sessions held the foregone conclusion doctrine to apply, reasoning that it would add "little or nothing to the sum total of the Government's information" for the suspect to "[a]gain provid[e] access to the unencrypted Z drive." *Id.* at *3. In *Fricosu*, the defendant had been caught on a prison call stating that the evidence sought by investigators was encrypted on her laptop. 841 F. Supp. 2d at 1235. Judge Blackburn ordered decryption, finding "little question here but that the government knows of the existence and location of the computer's files." *Id.* at 1237.[12]

[12] Several other courts have applied the foregone conclusion doctrine in a less rigorous manner. *See Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 615 (Mass. 2014) (approving compelled decryption where defendant's "ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key" were already known to investigators); *United States v. Gavegnano*, 305 F. App'x 954, 956 (4th Cir. Jan. 16, 2009) (not precedential) (approving compelled decryption where target was "sole user and possessor of the computer"); *United States v. Pearson*, No. 04-cr-340, 2006 U.S. Dist. LEXIS 32982, at *58-*59 (N.D.N.Y. May 24, 2006) (arguably approving

*continued…*

### 2. Here, the government has not identified with "reasonable particularity" any file known to a certainty to be stored on the hard drives.

As reviewed above, the decryption of a hard drive is not properly commensurate with an act of production. A demand for a passcode calls upon the contents of a person's own mind to gain access to an intimate portrait of that person's life. It does not call merely for the production of specifically identified papers. That said, were doctrines governing the surrender of hard-copy papers to be applied here, Mr. Doe's invocation of his Fifth Amendment privilege would be upheld because the government has not identified with reasonable particularity any files whose storage on the hard drives is a foregone conclusion.

Unlike in most child pornography investigations, the seizure here apparently did not involve any controlled or documented exchange of known files whose recovery was the object of a search warrant. In fact, there was no evidence as to how the Freenet investigation "led to" Mr. Doe at all. (*See* App. 37). Instead, the government has relied on after-the-fact testimony from Mr. Doe's estranged sister and a detective who admitted he was not trained in Freenet. This evidence failed

---

compelled decryption on ground that subject devices had already been seized). None of these cases can be squared with this Court's recognition that the foregone conclusion doctrine requires the government to conclusively demonstrate the existence of "each of the … documents" it seeks to have disclosed. *Grand Jury Empaneled Mar. 19*, 680 F.2d at 335.

to establish the existence of any files with "reasonable particularity." *Grand Jury Subpoena Dated Mar. 25*, 670 F.3d at 1349 n.28.

Mr. Doe's sister's testimony contributed little to the requisite showing. Critically, she did not claim to be able to say that any images had been stored on the hard drives which the government seeks to have decrypted. She testified that she had viewed child pornography on the Mac Pro more than a year before the seizure and agreed she did not know what devices, if any, had been connected to the computer at that time.

While Ms. Doe was candid in this respect, her credibility was in the main open to question. When she first met with police, she said nothing about child pornography even though that was the subject of the police investigation. She later claimed this was because child pornography "just didn't come up." (App. 104). A month later, as Mr. Doe was ceasing to provide her with financial support, she contacted a detective to say she had left something out. Between her questionable credibility and the attenuated nature of her testimony, Ms. Doe's testimony fell far short of establishing anything to a foregone conclusion.

As to the forensic testimony, Detective Tankelewicz himself said that all he could offer was a "best guess" as to whether there was child pornography on the hard drives. (App. 346). He likewise admitted that he had no training in Freenet, even though his opinion was based largely on an interpretation of Freenet "content

hash keys." Neither the keys themselves, nor the "references" to them on the Mac Pro, were said by Tankelewicz to be child pornography. Tankelewicz could describe only one download, and he did so in terms that leave some doubt as to its exact character: "a four or five-year-old girl with her dress lifted up, but the image itself was small so you really couldn't see what was going on with the images." (App. 308). Even as to this image, Detective Tankelewicz testified only to a "possibility" it was on a hard drive. (App. 308-309).

In sum, the government did not offer strong reason to suppose child pornography was on the hard drives, much less did it offer reasonably particularized evidence of known files that could be identified as child pornography. Thus, the act-of-production doctrine, to the extent it applies in the decryption context at all, protects Mr. Doe from being forced to decrypt the hard drives here.

### E. Were the act-of-production doctrine to be applied, safeguards would be required to secure files whose existence is not a foregone conclusion.

For the sake of argument, counsel addresses the proposition that the 'foregone conclusion' doctrine would permit the government to compel disclosure of the one download vaguely described by Detective Tankelewicz: the thumbnail image of a girl in a dress. Were the "production" of that image to be compelled by means of compelled decryption, there would arise a need for safeguards sufficient

to ensure the government does not make use of the other contents of the hard drives.

The most obvious approach is the one established by the immunity statute, 18 U.S.C. §§ 6002 and 6003, whereby the government may compel disclosure by a grant of immunity that prohibits the use or derivative use of all "testimony or other information compelled." 18 U.S.C. § 6002; *see Kastigar*, 406 U.S. at 457-59. In the context of decryption, this statutory immunity prohibits use of all digital contents produced over a valid claim of privilege. *Grand Jury Subpoena Dated Mar. 25*, 670 F.3d at 1351-52; *see also Hubbell*, 530 U.S. at 42-43 (no use or derivative use could be made of paper documents whose production was unlawfully compelled). That is to say, the government would not be permitted to try Mr. Doe by use of any data recovered from the hard drives apart from the single image described by Detective Tankelewicz. Nor could the government pursue any leads generated by the hard drives' decryption. *Kastigar*, 406 U.S. at 460.

Alternatively, there might be devised some means for an independent monitor or "taint team" to recover any image subject to disclosure. As Judge Kozinski has explained, the unique nature of digital storage media — where over-seizure of private information is commonly unavoidable — makes the use of taint teams or an independent third party the best practice. *Comprehensive Drug Testing*, 621 F.3d at 1179-80 (Kozinski, CJ., concurring). By this means, such

matter as the government lacks entitlement to access can be protected from unlawful inspection. *Id.* While *Comprehensive Drug Testing* arose in the Fourth Amendment context, taint teams have also regularly been used to safeguard Fifth Amendment rights. *See, e.g.*, *United States v. Bowen*, 969 F. Supp. 2d 546, 583-84 (E.D. La. 2013) (describing use of taint teams in connection with immunized testimony as "long established standard practice"); *United States v. Stanfa*, No. 94-cr-127, 1996 WL 417168, at *13 (E.D. Pa. July 18, 1996). Accordingly, this approach may be well-suited to the present context in the event the government is not prepared to apply for a grant of immunity.

## CONCLUSION

For the reasons stated in the foregoing, the judgment of contempt and decryption order should each be vacated and Mr. Doe released from custody. The application pursuant to the All Writs Act should be dismissed for lack of jurisdiction.

In the event the All Writs application is not dismissed for lack of jurisdiction, and should the Court determine that Mr. Doe may at an appropriate juncture be ordered to "produce" a file identified with reasonable particularity, the matter should be remanded for the district court to hear from the parties regarding the design of protocols to ensure that forcing Mr. Doe to recall (if he is able) and

divulge the passcodes does not result in any disclosure beyond what may be compelled over his claim of Fifth Amendment privilege.

Respectfully submitted,

/s/ Keith M. Donoghue
KEITH M. DONOGHUE
Assistant Federal Defender

BRETT G. SWEITZER
Assistant Federal Defender
Chief of Appeals

LEIGH M. SKIPPER
Chief Federal Defender

**CERTIFICATE OF BAR MEMBERSHIP**

It is hereby certified that Keith M. Donoghue, Assistant Federal Defender is a member of the bar of the Court of Appeals for the Third Circuit.

/s/ Keith M. Donoghue
Assistant Federal Defender

DATE: March 30, 2016

**CERTIFICATION**

I, Keith M. Donoghue**,** Assistant Federal Defender, Federal Community Defender Office for the Eastern District of Pennsylvania, hereby certify that the electronic version of the attached brief was automatically scanned by Symantec Endpoint Protection, version 12.1, and found to contain no known viruses. I further certify that the text in the electronic copy of the brief is identical to the text in the paper copies of the brief filed with the Court.

/s/ Keith M. Donoghue
Assistant Federal Defender

DATE: March 30, 2016

## CERTIFICATE OF COMPLIANCE

I, Keith M. Donoghue, Assistant Federal Defender, Federal Community Defender Office for the Eastern District of Pennsylvania, hereby certify that appellant's brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 11,217 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Word 2010 for Windows 7 word count software in font size 14, type style Times New Roman.

/s/ Keith M. Donoghue
Assistant Federal Defender

DATE: March 30, 2016

## CERTIFICATE OF SERVICE

I, Keith M. Donoghue, Assistant Federal Defender, Federal Community Defender Office for the Eastern District of Pennsylvania, hereby certify that I have electronically filed the *Brief for Appellant and Joint Appendix* and served copies upon Filing User Michelle Rotella, Assistant United States Attorney, through the Third Circuit Court of Appeals' Electronic Case Filing (CM/ECF) system.

/s/ Keith M. Donoghue
Assistant Federal Defender

DATE: March 30, 2016