PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

_____

No. 15-3537

_____

UNITED STATES OF AMERICA

v.

APPLE MACPRO COMPUTER,
APPLE MAC MINI COMPUTER,
APPLE I PHONE 6 PLUS,
ELLULAR TELEPHONE WESTERN DIGITAL
MY BOOK FOR MAC EXTERNAL HARD DRIVE,
Western Digital My Book Velociraptor Duo External
Hard Drive

*John Doe,
Appellant
*(Pursuant to Rule 12(a), Fed. R. App. P.)

_____

On Appeal from the United States District Court
for the Eastern District of Pennsylvania
(D.C. No. 15-mj-00850-001)
District Judge: Hon. L. Felipe Restrepo

_____

Argued September 7, 2016

Before: JORDAN, VANASKIE, and NYGAARD,
Circuit Judges.

(Filed: March 20, 2017)

Keith M. Donoghue [ARGUED]
Brett G. Sweitzer
Leigh M. Skipper
Federal Community Defender Office
for the Eastern District of Pennsylvania
601 Walnut Street, Suite 540 West
Philadelphia, PA 19106
Counsel for Defendant-Appellant

Christopher C. Walsh
Adam Schwartz
Mark Rumold [ARGUED]
Andrew Crocker
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Counsel for Amicus Curiae

Leslie Caldwell
Nathan Judish [ARGUED]
Bernadette McKeon
Michelle Rotella
Office of the United States Attorney
615 Chestnut Street, Suite 1250
Philadelphia, PA 19106

Counsel for Plaintiff-Appellee

OPINION

VANASKIE, *Circuit Judge.*

This appeal concerns the Government's ability to compel the decryption of digital devices when the Government seizes those devices pursuant to a valid search warrant. The District Court found Appellant John Doe in civil contempt for refusing to comply with an order issued pursuant to the All Writs Act, 28 U.S.C. § 1651, which required him to produce several seized devices in a fully unencrypted state. Doe contends that the court did not have subject matter jurisdiction to issue the order and that the order itself violates his Fifth Amendment privilege against self-incrimination. For the reasons that follow, we will affirm the District Court's order.

I.

During an investigation into Doe's access to child pornography over the internet, the Delaware County Criminal Investigations Unit executed a valid search warrant at Doe's residence. During the search, officers seized an Apple iPhone 5S and an Apple Mac Pro Computer with two attached Western Digital External Hard Drives, all of which had been

protected with encryption software.[1] Police subsequently seized a password-protected Apple iPhone 6 Plus as well.

Agents from the Department of Homeland Security then applied for a federal search warrant to examine the seized devices. Doe voluntarily provided the password for the Apple iPhone 5S, but refused to provide the passwords to decrypt the Apple Mac Pro computer or the external hard drives. Despite Doe's refusal, forensic analysts discovered the password to decrypt the Mac Pro Computer, but could not decrypt the external hard drives. Forensic examination of the Mac Pro revealed an image of a pubescent girl in a sexually provocative position and logs showing that the Mac Pro had been used to visit sites with titles common in child exploitation, such as "toddler_cp," "lolicam," "tor-childporn,"

[1] Encryption technology allows a person to transform plain, understandable information into unreadable letters, numbers, or symbols using a fixed formula or process. Only those who possess a corresponding "key" can return the information into its original form, *i.e.* decrypt that information. Encrypted information remains on the device in which it is stored, but exists only in its transformed, unintelligible format. Although encryption may be used to hide illegal material, it also assists individuals and businesses in lawfully safeguarding the privacy and security of information. Many new devices include encryption tools as standard features, and many federal and state laws either require or encourage encryption to protect sensitive information.

and "pthc."[2] (App. 39.) The Forensic examination also disclosed that Doe had downloaded thousands of files known by their "hash" values to be child pornography.[3] The files, however, were not on the Mac Pro, but instead had been stored on the encrypted external hard drives. Accordingly, the files themselves could not be accessed.

As part of their investigation, the Delaware County law enforcement officers also interviewed Doe's sister, who had lived with Doe during 2015. She related that Doe had shown her hundreds of images of child pornography on the encrypted external hard drives. She told the investigators that

---

[2] According to the affidavit submitted in support of the federal Government's search warrant application, "cp" stands for "child pornography" and "pthc" stands for "'pre-teen hard core." (App. 39.)

[3] A "hash" is "[a] mathematical algorithm that calculates a unique value for a given set of data, similar to a digital fingerprint, representing the binary content of the data to assist in subsequently ensuring that data has not been modified." *The Sedona Conference Glossary for E-Discovery and Digital Information Management* 21 (Cheryl B. Harris, et al. eds., 4th ed. 2014). Hash values are commonly used in child pornography investigations. *See, e.g.*, *United States v. Ross*, 837 F.3d 85, 87 (1st Cir. 2014), *United States v. Ackerman,* 831 F.3d 1292, 1294 (10th Cir. 2016); *United States v. Thomas*, 788 F.3d 345, 348 n. 5 (2nd Cir. 2015); *United States v. Brown,* 701 F.3d 120, 122 (4th Cir. 2012); *United States v. Cunningham*, 694 F.3d 372, 376 (3d Cir. 2012; *United States v. Cartier*, 543 F.3d 442, 444-45 (8th Cir. 2008).

the external hard drives included "videos of children who were nude and engaged in sex acts with other children." (App. 40.) Doe provided the password to access the iPhone 6 Plus, but did not grant access to an application on the phone which contained additional encrypted information. Forensic analysts concluded that the phone's encrypted database contained approximately 2,015 image and video files.

On August 3, 2015, upon application of the Government, a Magistrate Judge issued an order pursuant to the All Writs Act requiring Doe to produce his iPhone 6 Plus, his Mac Pro computer, and his two attached external hard drives in a fully unencrypted state (the "Decryption Order"). Doe did not appeal the Decryption Order. Instead, he filed with the Magistrate Judge a motion to quash the Government's application to compel decryption, arguing that his act of decrypting the devices would violate his Fifth Amendment privilege against self-incrimination.

On August 27, 2015, the Magistrate Judge denied Doe's Motion to Quash and directed Doe to fully comply with the Decryption Order (the "Quashal Denial"). The Magistrate Judge acknowledged Doe's Fifth Amendment objection but held that, because the Government possessed Doe's devices and knew that their contents included child pornography, the act of decrypting the devices would not be testimonial for purposes of the Fifth Amendment privilege against self-incrimination. The Quashal Denial stated that a failure to file timely objections could result in the waiver of appellate rights. Doe did not file any objections to the Quashal Denial and did not seek review by way of appeal, writ of mandamus, or otherwise.

Approximately one week after the Quashal Denial, Doe and his counsel appeared at the Delaware County Police Department for the forensic examination of his devices. Doe produced the Apple iPhone 6 Plus, including the files on the secret application, in a fully unencrypted state by entering three separate passwords on the device. The phone contained adult pornography, a video of Doe's four-year-old niece in which she was wearing only her underwear, and approximately twenty photographs which focused on the genitals of Doe's six-year-old niece. Doe, however, stated that he could not remember the passwords necessary to decrypt the hard drives and entered several incorrect passwords during the forensic examination. The Government remains unable to view the decrypted content of the hard drives without his assistance.

Following the forensic examination, the Magistrate Judge granted the Government's Motion for Order to Show Cause Why Doe Should Not Be Held in Contempt, finding that Doe willfully disobeyed and resisted the Decryption Order. Based on the evidence presented at the hearing, the Magistrate Judge found that Doe remembered the passwords needed to decrypt the hard drives but chose not to reveal them because of the devices' contents. The Magistrate Judge ordered Doe to appear before the District Court to show cause as to why he should not be held in civil contempt.

On September 30, 2015, after a hearing, the District Court granted the Government's motion to hold Doe in civil contempt. On October 5, 2015, the District Court issued a "Supplemental Order to articulate the reasons for its September 30th Order." (App. at 12.) The District Court noted that the Government's prima facie case of contempt was largely, if not entirely, uncontested. While the

Government presented several witnesses to support its motion, Doe neither testified nor called witnesses. He offered no physical or documentary evidence into the record and provided no explanation for his failure to comply with the Decryption Order. The District Court remanded Doe to the custody of the United States Marshals to be incarcerated until he fully complies with the Decryption Order. This timely appeal followed.

II.

We have appellate jurisdiction under 28 U.S.C. § 1291. We ordinarily exercise plenary review over the District Court's authority to issue an order pursuant to the All Writs Act, *Grider v. Keystone Health Plan Cent., Inc*., 500 F.3d 322, 327 (3d Cir. 2007), and "review a district court's decision on a motion for contempt for abuse of discretion." *Marshak v. Treadwell*, 595 F.3d 478, 485 (3d Cir. 2009). However, when the party seeking review has failed to preserve the issue in the trial court, we review only for plain error. *See Brightwell v. Lehman*, 637 F.3d 187, 193 (3d Cir. 2011); *Nara v. Frank*, 488 F.3d 187, 194 (3d Cir. 2007). We nonetheless exercise plenary review over challenges concerning subject matter jurisdiction. *United States v. Merlino*, 785 F.3d 79, 82 (3d Cir. 2015).

III.

Doe raises two primary arguments as to why he should not be held in contempt. First, he asserts that the District Court lacked subject matter jurisdiction to issue the Decryption Order under the All Writs Act. Thus, he argues that he is not in contempt of any valid order and the judgment of contempt must be vacated. Second, Doe contends that the

Decryption Order violates his Fifth Amendment privilege against self-incrimination.

A.

Doe's first challenge concerns the All Writs Act, which permits 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(a). The All Writs Act does not itself confer any subject matter jurisdiction, but rather only allows a federal court to issue writs "in aid of" its existing jurisdiction. *Clinton v. Goldsmith*, 526 U.S. 529, 534 (1999); *Sygenta Crop Prot., Inc. v. Henson*, 537 U.S. 28, 31 (2002); *see also In re Arunachalum*, 812 F.3d 290, 292 (3d Cir. 2016) (per curiam). Therefore, a court has subject matter jurisdiction over an application for an All Writs Act order only when it has subject matter jurisdiction over the underlying order that the All Writs Act order is intended to effectuate. Additionally, a federal court may only issue an All Writs Act order "as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained." *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 172 (1977).

Doe contends that the Magistrate Judge did not have subject matter jurisdiction to issue the Decryption Order because the Government should have compelled his compliance by means of the grand jury procedure and not the All Writs Act. The grand jury process, however, is not the exclusive means by which the Government may collect evidence prior to indictment. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 559 (1978) (allowing the Government to proceed by search warrant despite insistence that the

investigation should proceed by subpoena); *United States v. Educ. Dev. Network Corp.*, 884 F.2d 737, 743 (3d Cir. 1989) (rejecting the argument that the Government could not obtain evidence by means of a search warrant and must proceed solely by grand jury). Here, the Magistrate Judge had subject matter jurisdiction under Federal Rule of Criminal Procedure 41 to issue a search warrant[4] and therefore had jurisdiction to issue an order under the All Writs Act that sought "to effectuate and prevent the frustration" of that warrant. *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 172 (1977).

In arguing that the Magistrate Judge did not have subject matter jurisdiction to issue the Decryption Order, Doe also challenges the merits of that order, contending that it was not a "necessary and appropriate means" of effectuating the original warrant as required by the Supreme Court in *New York Telephone*. A contempt proceeding, however, generally "'does not open to reconsideration the legal or factual basis of the order alleged to have been disobeyed.'"[5] *United States v.*

---

[4] Doe does not dispute the validity of the underlying search warrant issued by a Magistrate Judge under Fed. R. Crim. P. 41.

[5] There are, of course, instances when a contempt proceeding may be the only avenue for challenging the underlying order to produce information. For example, judicial review of a grand jury subpoena may be obtained only by refusal to comply with the subpoena, with the validity of the subpoena being litigated in the ensuing contempt proceeding. *See, e.g., United States v. Ryan*, 402 U.S. 530, 532-33 (1971) ("[W]e have consistently held that the necessity for expedition in the administration of the criminal

Rylander, 460 U.S. 752, 756 (1983) (quoting *Maggio v. Zeitz*, 333 U.S. 56, 69 (1948)); *In re Contemporary Apparel, Inc*., 488 F.2d 794, 798 (3d Cir. 1973) (same). Furthermore, Doe did not argue in the District Court that the Decryption Order was not an appropriate exercise of authority under the All Writs Act. Thus, even if the propriety of the Decryption Order was before us, our review would be limited to plain error. *Brightwell*, 637 F.3d at 193. Under this framework, an appellant must show four elements: "(1) there is an 'error'; (2) the error is 'clear or obvious, rather than subject to reasonable dispute'; (3) the error 'affected the appellant's substantial rights, which in the ordinary case means' it 'affected the outcome of the district court proceedings'; and (4) 'the error seriously affect[s] the fairness, integrity or public reputation of judicial proceedings.'" *United States v. Marcus*, 560 U.S. 258, 262 (2010) (quoting *Puckett v. United States*, 556 U.S. 129, 135 (2009)).

In *New York Telephone*, the district court had issued an order authorizing federal agents to install pen registers in two telephones and directed the New York Telephone Company

---

law justifies putting one who seeks to resist the production [to a grand jury] of desired information to a choice between compliance with a trial court's order to produce prior to any review of that order, and resistance to that order with the concomitant possibility of an adjudication of contempt if his claims are rejected on appeal."); *In re Grand Jury Subpoena*, 709 F.3d 1027, 1029 (10th Cir. 2013)("A protesting [grand jury] witness may seek appellate review only after he refuses to obey the subpoena and is held in contempt.").

to furnish "all information, facilities and technical assistance" necessary to accomplish the installation. *N.Y. Tel. Co.*, 434 U.S. at 161. The Company argued that neither Fed. R. Crim. P. 41 nor the All Writs Act "provided any basis for such an order." *Id*. at 163. The Supreme Court, however, found that this order was "clearly authorized by the All Writs Act" as a necessary and appropriate means of effectuating the installation of the pen registers. *Id.* at 172.

Here, the Magistrate Judge issued a search warrant for the devices seized at Doe's residence. When law enforcement could not decrypt the contents of those devices, and Doe refused to comply, the Magistrate Judge issued the Decryption Order pursuant to the All Writs Act. The Decryption Order required Doe to "assist the Government in the execution of the…search warrant" by producing his devices in "a fully unencrypted state." As was the case in *New York Telephone*, the Decryption Order here was a necessary and appropriate means of effectuating the original search warrant.

Doe asserts that *New York Telephone* should not apply because the All Writs Act order in that case compelled a third party to assist in the execution of that warrant, and not the target of the government investigation. The Supreme Court explained, however, that the Act extends to anyone "in a position to frustrate the implementation of a court order or the proper administration of justice" as long as there are "appropriate circumstances" for doing so. *Id.* at 174. Here, as in *New York Telephone*: (1) Doe is not "far removed from the underlying controversy;" (2) "compliance with [the Decryption Order] require[s] minimal effort;" and (3) "without [Doe's] assistance there is no conceivable way in which the [search warrant] authorized by the District Court

could [be] successfully accomplished." *Id.* at 174-175. Accordingly, the Magistrate Judge did not plainly err in issuing the Decryption Order.

B.

Doe also contends that the Decryption Order violates his Fifth Amendment privilege against self-incrimination and that this challenge is subject to plenary review. Doe raised a Fifth Amendment challenge in his Motion to Quash the Decryption Order. The Magistrate Judge denied that challenge, rejecting the argument that Doe's Fifth Amendment privilege would be violated. Doe did not file objections to that order, nor did he seek review by way of appeal, writ of mandamus or otherwise, despite the Quashal Denial order informing Doe that failure to file a timely objection may constitute a waiver of appellate rights. Doe also did not renew this self-incrimination claim during the contempt proceedings before the Magistrate Judge and the District Judge.[6] Instead, Doe only reasserted his Fifth Amendment claim in this appeal.

While Doe persists that his challenge to the contempt order entitles him to plenary consideration of the Fifth Amendment issue, we disagree. As noted above, it is

[6] In its Order explaining the contempt ruling, the District Judge observed that Doe had failed to object to the Magistrate Judge's determination that Doe's Fifth Amendment rights were not violated by the Decryption Order despite being warned that such failure "may constitute a waiver of appellate rights." (App. at 15 (citing *United States v. Polishan*, 336 F.3d 234, 240 (3d Cir. 2003).) Thus, the District Court did not address the Fifth Amendment issue.

generally the case that "a contempt proceeding does not open to reconsideration the legal or factual basis of the order alleged to have been disobeyed." *Rylander*, 460 U.S. at 756 (internal quotation marks and citation omitted).

Even if we could assess the Fifth Amendment decision of the Magistrate Judge, our review would be limited to plain error. *See United States v. Schwartz*, 446 F.2d 571, 576 (3d Cir. 1971) (applying plain error review to unpreserved claim of violation of privilege against self-incrimination). Doe's arguments fail under this deferential standard of review.

The Fifth Amendment states that "[n]o person…shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. The Fifth Amendment, however, "does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a Testimonial Communication that is incriminating." *Fisher v. United States*, 425 U.S. 391, 408 (1976). To be testimonial, a communication must either "explicitly or implicitly . . . relate a factual assertion or disclose information." *Doe v. United States*, 487 U.S. 201, 210 (1988).

The Supreme Court has recognized that in some instances, the production of evidence can implicate the Fifth Amendment. In *Fisher*, the Court stated that "[t]he act of producing evidence in response to a subpoena . . . has communicative aspects of its own, wholly aside from the contents of the papers produced." 425 U.S. at 410. The Court reasoned that compliance with a request for evidence may "tacitly concede[ ] the existence of the documents demanded and their possession and control by the [defendant]." *Id.* 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 [Government] requests." *United States v. Chabot*, 793 F.3d 338, 342 (3d Cir.), *cert. denied*, 136 S. Ct. 559 (2015). When the production of evidence does concede the existence, custody, and authenticity of that evidence, the Fifth Amendment privilege against self-incrimination applies because that production constitutes compelled testimony.

In *Fisher*, however, the Court also articulated the "foregone conclusion" rule, which acts as an exception to the otherwise applicable act-of-production doctrine. *Fisher*, 425 U.S. at 411. Under this rule, the Fifth Amendment does not protect an act of production when any potentially testimonial component of the act of production—such as the existence, custody, and authenticity of evidence—is a "foregone conclusion" that "adds little or nothing to the sum total of the Government's information." *Id.* For the rule to apply, the Government must be able to "describe with reasonable particularity" the documents or evidence it seeks to compel. *Hubbell*, 530 U.S. at 30.

Although we have not confronted the Fifth Amendment implications of compelled decryption, the Eleventh Circuit has addressed the issue and found that the privilege against self-incrimination should apply. In that case, a suspect appealed a judgment of contempt entered after he refused to produce the unencrypted contents of his laptop and hard drives. *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1337 (11th Cir. 2012). The court found that "(1) [the suspect's] decryption and production of the contents of the drives would be testimonial, not merely a physical act; and (2) the explicit and implicit

factual communications associated with the decryption and production are not foregone conclusions." *Id.* at 1346. The court reached this decision after noting that the Government did not show whether any files existed on the hard drives and could not show with any reasonable particularity that the suspect could access the encrypted portions of the drives. *Id.* Although the court did not require the Government to identify exactly the documents it sought, it did require that, at the very least, the Government be able to demonstrate some knowledge that files do exist on the encrypted devices. *Id.* at 1348–49.

Despite Doe's argument to the contrary, the Eleventh Circuit's reasoning in *In re Grand Jury Subpoena* does not compel a similar result here. In the Quashal Denial, the Magistrate Judge found that, though the Fifth Amendment may be implicated by Doe's decryption of the devices, any testimonial aspects of that production were a foregone conclusion. According to the Magistrate Judge, the affidavit supporting the application for the search warrant established that (1) the Government had custody of the devices; (2) prior to the seizure, Doe possessed, accessed, and owned all devices; and (3) there are images on the electronic devices that constitute child pornography. Thus, the Magistrate Judge concluded that the Decryption Order did not violate Doe's Fifth Amendment privilege against self-incrimination.

Unlike *In re Grand Jury Subpoena*, the Government has provided evidence to show both that files exist on the encrypted portions of the devices and that Doe can access them. The affidavit supporting the search warrant states that an investigation led to the identification of Doe as a user of an internet file sharing network that was used to access child pornography. When executing a search of Doe's residence,

forensic analysts found the encrypted devices, and Doe does not dispute their existence or his ownership of them. Once the analysts accessed Doe's Mac Pro Computer, they found one image depicting a pubescent girl in a sexually suggestive position and logs that suggested the user had visited groups with titles common in child exploitation. Doe's sister then reported that she had witnessed Doe unlock his Mac Pro while connected to the hard drives to show her hundreds of pictures and videos of child pornography. Forensic analysts also found an additional 2,015 videos and photographs in an encrypted application on Doe's phone, which Doe had opened for the police by entering a password. Based on these facts, the Magistrate Judge found that, for the purposes of the Fifth Amendment, any testimonial component of the production of decrypted devices added little or nothing to the information already obtained by the Government. The Magistrate Judge determined that any testimonial component would be a foregone conclusion. The Magistrate Judge did not commit a clear or obvious error in his application of the foregone conclusion doctrine. In this regard, the Magistrate Judge rested his decision rejecting the Fifth Amendment challenge on factual findings that are amply supported by the record.[7]

[7] It is important to note that we are not concluding that the Government's knowledge of the content of the devices is necessarily the correct focus of the "foregone conclusion" inquiry in the context of a compelled decryption order. Instead, a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production. In this case, the fact known to the government that is implicit in the act of providing the password for the devices is "I, John Doe, know the password

Accordingly, Doe's challenges to the Decryption Order and Quashal Denial fail.

So, too, does Doe's challenge to the contempt order. At the hearing on the contempt motion, Doe maintained that he could not remember the passwords to decrypt the hard drives. In a civil contempt proceeding, when a defendant raises a challenge of impossibility of compliance, "the defendant bears the burden of production." *United States v. Rylander*, 460 U.S. 752, 757 (1983). At the contempt hearing, the Government presented several witnesses to support its prima facie case of contempt. Doe's sister testified to the fact that, while in her presence, Doe accessed child pornography files on his Mac Pro computer by means of entering passwords from memory. Further, a detective who executed the original search warrant stated that Doe did not provide his password at the time because he wanted to prevent the police from accessing his computer. Doe never asserted an inability to remember the passwords at that time. Doe presented no evidence to explain his failure to comply or

---

for these devices." Based upon the testimony presented at the contempt proceeding, that fact is a foregone conclusion. However, because our review is limited to plain error, and no plain error was committed by the District Court in finding that the Government established that the contents of the encrypted hard drives are known to it, we need not decide here that the inquiry can be limited to the question of whether Doe's knowledge of the password itself is sufficient to support application of the foregone conclusion doctrine.

to challenge the evidence brought by the Government. The District Court thus found Doe in contempt and ordered he be held in custody until he complies with the Decryption Order. The District Court did not abuse its discretion in finding Doe to be in contempt of the Decryption Order.

IV.

For the foregoing reasons, we will affirm the District Court's order of September 30, 2015 holding Appellant John Doe in civil contempt.