NO. 15-3537

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

UNITED STATES OF AMERICA,
Appellee

v.

APPLE MAC PRO COMPUTER, et. al.

JOHN DOE, Appellant

APPEAL FROM JUDGMENT OF CIVIL CONTEMPT
IN CASE NO. 15-MJ-850
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

BRIEF FOR APPELLEE UNITED STATES OF AMERICA

LESLIE R. CALDWELL
Assistant Attorney General
Criminal Division

NATHAN JUDISH
Attorney, Computer Crime
and Intellectual Property
Section, Criminal Division

ZANE DAVID MEMEGER
United States Attorney

BERNADETTE MCKEON
Assistant United States Attorney
Acting Chief of Appeals

MICHELLE ROTELLA
Assistant United States Attorney
615 Chestnut Street, Suite 1250
Philadelphia, PA 19106
(215) 861-8471

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Rules

JURISDICTIONAL STATEMENT

I. Subject Matter Jurisdiction

Below, the district court jurisdiction over this case derived from 18 U.S.C. § 3231. The magistrate judge had jurisdiction to issue the search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure. The magistrate judge had jurisdiction to issue the order requiring Doe to assist with the search warrant pursuant to the All Writs Act, 28 U.S.C. § 1651. The magistrate judge had jurisdiction over contempt proceedings against Doe under 28 U.S.C. § 636(e)(6). The district court had jurisdiction to hold Doe in contempt under 18 U.S.C. § 401.

II. Appellate Jurisdiction

Based upon the timely filing of a notice of appeal from the order of judgment of civil contempt from the district court entered on September 30, 2015, this Court has jurisdiction over this matter under 28 U.S.C. § 1291.

STATEMENT OF ISSUES

1. Is the government confined to conducting pre-indictment investigations using the grand jury's subpoena power only, or was the All Writs Act a proper investigative tool to compel Doe's assistance with the search warrant?

2. Does the "foregone conclusion doctrine" apply to Doe's act of producing decrypted devices where the government knows of the existence of encrypted devices, knows that child pornography is stored on the devices, and knows that Doe has the ability to decrypt the devices but refuses to do so?

STATEMENT OF THE CASE

A. The Delaware County Case.

In March 2015, the Criminal Investigation Division ("CID") of the Delaware County District Attorney's Office conducted a child pornography investigation regarding users of the peer-to-peer Freenet Network. App. 37. Freenet is an Internet-based network which lets users anonymously share files and chat by encrypting their communications. *Id.* Because Freenet attempts to hide what the user is requesting, the network has attracted individuals who wish to collect and/or distribute child pornography. *Id.* The investigation led to the identification of appellant John Doe as a Freenet user who was routing and/or requesting child pornography files. App. 37, 305-06. Doe was at the time employed as a Sergeant in the Philadelphia Police Department. App. 37, 352-53, 386.

Based on Doe's Freenet activities, detectives from the Delaware County CID obtained a search warrant for his residence, which they executed on March 30, 2015. App. 37, 290. Police seized Doe's iPhone 5S, Apple Mac Pro computer, an external hard drive that was unconnected and powered off, an Apple iPad, a cell phone, and other electronic equipment. App. 116-17, 290-91. Significantly, detectives also seized two external hard

drives that were attached to the Mac Pro computer and running at the time of the execution of the warrant. App. 40, 132-33.

Prior to the execution of the search warrant on his home, detectives approached Doe at the Philadelphia Police Department, advised him of his Miranda rights, and interviewed him. App. 38, 352-53. Doe told detectives that he had the Freenet program running on his Apple Mac Pro computer at his residence, and that his computer was protected by FileVault encryption. App. 38, 355. He also admitted that he may have received child pornography through his email account, but he claimed to have deleted it immediately. App. 38. Doe refused to provide investigators with the password or encryption codes to his computer or computer equipment, telling detectives that he "didn't want [the detectives] looking" at his computer. App. 38, 118-19, 354-55. Doe then requested an attorney. *Id.*

Later that same day, while at Doe's residence during the execution of the search warrant, Doe volunteered the password for his iPhone 5S cellular telephone and his Apple iPad. App. 38, 118, 294-95, 332-333. He did not advise that a portion of his iPhone 5S was protected by an application called Secret Apps, nor did Doe provide the passcode for this application. App. 297. Secret Apps allows users to hide files, but forensic analysts can break the password. App. 120. Forensic agents later accessed the information

Secret Apps stored on Doe's iPhone 5S. App. 39, 120-21, 297. They discovered a screen shot of a recovery key, App. 121, 390, which is a code that can be used as a substitute for a computer password so that a user may gain access to a computer. App. 39, 120-21, 297-300. Forensic examiners later used that 24-character recovery key to decrypt Doe's Mac Pro computer. App. 39, 123, 300-301.

A subsequent forensic exam of his Mac Pro computer revealed that Doe had installed a virtual machine (software that emulates a separate computer within his computer). App. 304. Within the virtual machine the examiner found one image of what appeared to be a 14-year-old child wearing a bathing suit and posed in a sexually suggestive position. App. 39. There were also log files that indicated that Doe had visited groups titled: "toddler_cp," "lolicam," "hussy," "child models – girls," "pedomom," "tor-childporn," and "pthc," terms that are commonly used in child exploitation. *Id*.

The exam also found that Freenet, the peer-to-peer file sharing program used by Doe to obtain child pornography from other users, had been installed within the virtual machine. App. 305-06. The exam showed that Doe accessed or attempted to access more than 20,000 files with file names consistent with obvious child pornography, App. 306-07, and that

he used the external hard drives seized by Delaware County detectives to access and store the images. App. 303-05, 308-10, 337, 339-40.

However, because the external hard drives were encrypted, the images themselves could not be accessed. App. 301-03. Despite not having the actual images, investigators confirmed that it was child pornography Doe sought based on the hash values[1] of the files requested by Doe. App. 306-10, 337, 339-40, 349, 391. A sample of three of the 20,000 files sought by Doe were known by investigators to contain child pornography, and were described as follows: 4- and 6-year-old children, 10- and 13-year-old children, and 8- and 10-year-old children, all engaged in oral sex and being sexually abused by adults. App. 306-07, 339, 391. The forensic exam of the Mac Pro computer confirmed that Doe successfully downloaded child

[1] A hash value has been defined as a "unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion." *Managing Discovery of Electronic Information: A Pocket Guide for Judges,* Federal Judicial Center, at 38 (2007); *United States v. Hawkins*, 2014 WL 7335638, at *1 n.2 (W.D. Pa. Dec. 19, 2014) ("It is computationally infeasible for two different computer files with different content to produce or have the same SHA1 hash values."); *United States v. Crist*, 627 F. Supp. 2d 575, 578 (M.D. Pa. 2008) (recognizing that a hash value is a unique alphanumeric representation of data, similar to a fingerprint or DNA).

pornography, and that he stored the downloaded child pornography on his external hard drives. App. 308-310, 336-37, 339-40, 349. The forensic exam of the Mac Pro computer also revealed that Doe used numerous message boards related to child pornography to communicate with others who had an interest in child pornography. App. 311-13.

Lastly, the forensic exam also confirmed that both external hard drives contained large amounts of data. App. 315-16. Together they were capable of storing two terabytes of information each, comparable to the same amount of data as eight average computers. *Id.* The exam confirmed that one external hard drive was more than 51 percent filled, and the second external hard drive was approximately 23 percent filled. *Id.*

On June 26, 2015, approximately one week before Doe's sister moved out of John Doe's apartment, detectives from Delaware County CID interviewed her. App. 40. Doe's sister resided with Doe in Lansdowne from approximately February 2015 to approximately July 3, 2015. App. 40, 236. Ms. Doe reported that John Doe's computers seized by Delaware County detectives during the search warrant in March 2015 contained at least part of John Doe's collection of child pornography. App. 40, 240, 247-49. Specifically, Ms. Doe reported that in the summer of 2014, John Doe unlocked his Mac Pro computer that was later seized by Delaware County

detectives to show her hundreds of pictures and videos of children who were nude and engaged in sex acts with other children. App. 40, 96, 100-01, 240, 247-48, 280-81. Some of the children in the images were toddler age. App. 248. Ms. Doe stated that John Doe openly acknowledged to her and to the family that he has had a problem with child pornography for years. App. 40-41, 94-95, 237, 239-40. She knew Doe was sexually attracted to children since at least 2010, in part because Doe made sexual comments about children in front of her. App. 95, 238-239, 267. She also reported that John Doe obtained a new cell phone shortly after Delaware County police seized his equipment. App. 41, 251. Ms. Doe advised that the reason she contacted Delaware County CID was because John Doe refused to seek treatment for his issues with child pornography. App. 271.

B. The Philadelphia County Case.

Less than two months after Delaware County investigators executed the search warrant on John Doe's home and seized his equipment, Philadelphia Police officers seized Doe's new iPhone 6 cell phone after confirming it contained child pornography. App. 41. Doe's family members came to learn that Doe was again involved in child pornography, and they had suspicions that Doe had pictures of their nephews and nieces. App. 252. A family "intervention" meeting was called shortly after Memorial Day

2015 at Doe's brother's home to address this issue, with John Doe in attendance. App. 41, 252-53. John Doe admitted to his family that he had already taken photos of his nieces,[2] and he told them that he still had the photos on his iPhone 6 cell phone. App. 41, 253-54. At the family's request he unlocked his phone and turned it over to his family. App. 41, 254-55. What they discovered was a video – not a photograph – of his 4-year-old niece. App. 255-56. The child was in her bed wearing only underpants. The focus of the video was on the child's genital area, and as she moved her legs around her underwear pulled to the side and her genitals were exposed for the camera. App. 41-42, 327. Also found on Doe's cell phone were approximately 15 to 25 images of his 6-year-old niece, taken at an angle where the camera was aimed underneath her dress. App. 42, 327. The child's legs were open, and the focus of each of the images was on the child's genital area. App. 42, 327.

The video and photos of the two children were viewed by other family members of John Doe who were in attendance at the family meeting. App. 255. The Philadelphia Police were also called to the home, and the responding officer also viewed the video and some of the photographs. App.

[2] Doe described these photos he took of his nieces as "inappropriate." App. 103, 254.

41, 327. Police confiscated Doe's iPhone 6 cell phone based on the images contained on the phone, and they later obtained a warrant to search the phone, but at that point the phone had locked. App. 41-42.

Police then obtained a second search warrant for John Doe's fingerprint to unlock the phone. App. 42, 124-25, 318. Once they accessed the cell phone, however, the forensic analysts discovered that as in all of his other cell phone and computer equipment, Doe had additional layers of encryption on this iPhone 6 as well. App. 42, 125, 318. The video and photos of the children that Doe had unlocked and shown to his family members were not accessible on the unencrypted portion of Doe's cell phone, and the forensic experts were not able to decrypt the additional encryption application on his cell phone. App. 42-43.

C. The Contempt Motion.

On July 29, 2015, federal investigators obtained a federal search warrant for Doe's encrypted devices. App. 24-51. Thereafter, on August 3, 2015, the government filed an application for an order pursuant to the All Writs Act, 28 U.S.C. § 1651, to compel John Doe to assist in the execution of the federal search warrant by decrypting the devices seized from him, namely his Apple Mac Pro computer and two connected Western Digital external hard drives (seized by Delaware County), and his iPhone 6 cell

phone (seized by Philadelphia Police). App. 53-66. Magistrate Judge Thomas J. Rueter granted the government's application and ordered Doe to appear at Delaware County CID by August 14, 2015, to decrypt his devices. App. 3. On August 12 and 13, 2015, by way of letters directed to the court, John Doe requested the magistrate court to stay its August 14th deadline to permit him to challenge the court's order that he be compelled to decrypt his devices. App. 67, 70. The court granted that request. App. 72. On August 27, 2015, after consideration of Doe's Motion to Quash the Government's Application to Compel, App. 73, the magistrate judge ordered that John Doe must decrypt his devices by September 4, 2015. App. 4.

Defendant Doe did not appeal the magistrate's order to decrypt the devices. Instead, he appeared on September 4, 2015, at the Criminal Investigation Division of the Delaware County District Attorney's Office. App. 318-19. The court order compelled Doe to decrypt the devices, not to disclose the password, so Doe was permitted a private space in the forensic laboratory to enter his password information so that the password would not be detected by law enforcement. App. 136-37.

Immediately upon entering the forensic lab, Doe pointed to the two external hard drives named in the court's order and stated that he could not remember the passwords. App. 136, 319-20. Doe arrived with no

documents and appeared to be working solely from memory. App. 324. Doe was first given the two external hard drives. App. 323-24. Doe pressed keys on the keyboard, but he did not unlock either external hard drive. *Id*. He eventually told examiners that he could not remember the passwords. *Id*. Doe was next given the iPhone 6 to decrypt. App. 324. There were three passcodes needed for this phone – the passcode to unlock the phone, and both an initial passcode and an additional alphanumeric passcode to unlock an encryption application called Kycalc. App. 42, 325-27, 341-43. Despite the fact that his iPhone 6 had been seized more than three months prior, Doe entered all three levels of passcodes from memory and unlocked the iPhone 6. App. 326-27, 341-43. Investigators found the video of Doe's 4-year-old niece and approximately 24 pictures of his 6-year-old niece on the encrypted portion of the phone. App. 128, 327. The children were photographed in their underwear, and the focus of the video and photographs were on each child's genitals. *Id*.

Doe was then directed back to the external hard drives. *Id*. Doe failed to decrypt either hard drive. App. 328. The government then filed a motion with Magistrate Judge Rueter for an order to show cause why Doe should not be held in contempt. App. 79. A hearing was held on the motion on September 10, 2015. App. 86. The defendant did not testify at the hearing

and did not offer any other evidence or testimony in support of his contention that memory failure prevented him from complying with the court's order. On September 14, 2015, the court issued an order granting the government's motion, App. 6-10, finding that Doe was engaged in a "deliberate ruse" in claiming memory failure as to the external hard drives and that he intentionally disobeyed the court's orders directing him to decrypt the devices. App. 9. Further, the magistrate judge found that Doe engaged in a "wily subterfuge by choosing to decrypt his Apple iPhone 6 Plus which contains the images of his clothed nieces, but refusing to decrypt the devices containing the hard core child pornography." App. 10. The magistrate judge directed that Doe appear before the district court to show cause why he should not be held in contempt. App. 6.

On September 30, 2015, the district court held a trial de novo on the government's contempt motion. App. 227-388. The government called four witnesses at this hearing, and John Doe again failed to testify or to offer any evidence concerning his lack of compliance with the court's order. *Id.* At the conclusion of the hearing, then-District Court Judge L. Felipe Restrepo found John Doe to be in contempt of the court's order to decrypt his devices. App. 384. The district court advised Doe that he would be taken into custody, and advised Doe that he could purge himself of civil contempt

by simply providing the government with his computer equipment in unencrypted form, as was ordered by the court. *Id*. Before taking Doe into custody, the district court afforded Doe an additional ten minutes to consult with his attorney and to agree to comply with the court's directive. *Id*. Doe refused to do so and was transferred to the custody of the United States Marshal. App. 385. His verbal request for a stay was denied. *Id*.

STATEMENT OF RELATED CASES

The government is not aware of any other related case or proceeding that is completed, pending, or about to be presented before this Court or any other court or agency, state or federal.

SUMMARY OF ARGUMENT

First, because Doe never argued to the magistrate judge or the district court that the government's investigation must proceed by grand jury subpoena rather than a search warrant and All Writs Act order, Doe's challenge to the issuance of the All Writs Act order is subject only to plain error review except as to subject matter jurisdiction. The magistrate judge had subject matter jurisdiction to issue the All Writs Act order because the judge had jurisdiction to issue a search warrant for Doe's hard drives pursuant to Rule 41 of the Federal Rules of Criminal Procedure, and because the All Writs Act order was issued to facilitate execution of that warrant.

The remainder of Doe's challenge to the All Writs Act order, in which he argues that the magistrate judge should not have issued an All Writs Act order in support of the search warrant when the government might have been able to proceed by a grand jury subpoena, was not raised below and is subject to plain error review. But the magistrate judge did not err, much less plainly err, in issuing the All Writs Act order. The All Writs Act order was appropriately issued in support of the search warrant for Doe's hard drives, and both this Court and the Supreme Court have rejected arguments that an investigation must proceed via subpoena rather than warrant.

Second, this Court reviews Doe's claim of Fifth Amendment privilege for plain error, as Doe failed to object to the magistrate judge's order holding that under the foregone conclusion doctrine, requiring Doe to assist in decrypting his hard drives would not violate his Fifth Amendment privilege against self-incrimination. Nor did he raise the Fifth Amendment privilege as a defense at either contempt hearing. Even if Doe had preserved his Fifth Amendment claim, whether an act of production involves testimonial self-incrimination would be a question of fact reviewed for clear error.

Doe's claim under the Fifth Amendment fails because the All Writs Act order requires no testimony from him. Instead, under the foregone conclusion doctrine, it requires only a nontestimonial act of production. Under that doctrine, an act of production does not implicate the Fifth Amendment where any potentially testimonial component of the act of production is already known to the government. Here, based on Doe's own statements, the testimony of his sister, and forensic analysis of the hard drives seized from Doe via a search warrant, the government already knows that Doe possessed and owned the hard drives, that he can decrypt them, and that they contain child pornography. Under these circumstances, the magistrate judge did not clearly or plainly err in concluding that the

foregone conclusion doctrine applies in this case, and thus that requiring Doe to assist in decrypting the drives does not violate his privilege against self-incrimination.

ARGUMENT

I. THE MAGISTRATE JUDGE HAD SUBJECT MATTER JURISDICTION AND PROPERLY ISSUED AN ORDER UNDER THE ALL WRITS ACT REQUIRING DOE TO ASSIST WITH THE EXECUTION OF A SEARCH WARRANT

Standard of Review

Doe never argued to the magistrate judge or the district court that the government's investigation must proceed by grand jury subpoena rather than a search warrant and All Writs Act order. Doe concedes that he did not preserve this challenge. *See* Br. 3. Thus, except as to subject matter jurisdiction, Doe's challenge to the issuance of the All Writs Act order is subject only to plain error review. *See* Fed. R. Crim. P. 52(b); *United States v. Benjamin*, 711 F.3d 371, 377 (3d Cir. 2013); *United States v. Olano*, 507 U.S. 725, 731-35 (1993).

Doe argues that his challenge to the issuance of the All Writs Act order should be subject to plenary review because it is based on subject matter jurisdiction. *See* Br. 19. It is true that challenges to subject matter jurisdiction cannot be waived or forfeited and that this Court exercises plenary review regarding the existence of subject matter jurisdiction. *See United States v. Cotton*, 535 U.S. 625, 630 (2002); *Tellado v. IndyMac Mortg. Servs.*, 707 F.3d 275, 279 (3d Cir. 2013). These principles do not save Doe's grand jury subpoena argument from review for plain error,

however, because Doe's argument is fundamentally an argument on the merits that the magistrate judge should not have issued the All Writs Act order.

Moreover, even if Doe had challenged the issuance of the All Writs Act order before the magistrate judge, his challenge here would be subject to plain error review, as Doe failed to object to the magistrate judge's order before the district court. The magistrate judge's August 27, 2015, order required Doe to comply with the All Writs Act order and informed him: "Any party may file objections to this Order. See Loc.R.Crim.P. 50.2(IV). Failure to file timely objections may constitute a waiver of any appellate rights. United States v. Polishan, 336 F.3d 234, 240 (3d Cir. 2003)." App. 5 (emphasis removed). Despite this admonition, Doe did not file objections to the August 27 order, nor did he seek review of that order by way of appeal, writ of mandamus, as a defense to the contempt action, or otherwise. Where a party fails to object to a magistrate judge's ruling on a dispositive motion, this Court reviews only for plain error. *See Brightwell v. Lehman*,

637 F.3d 187, 193 (3d Cir. 2011); *Nara v. Frank*, 488 F.3d 187, 195 (3d Cir. 2007).[3]

Discussion

A. The Magistrate Judge Had Subject Matter Jurisdiction Over Issuance of the All Writs Act Order.

The magistrate judge had subject matter jurisdiction over issuance of the All Writs Act order pursuant to Rule 41 of the Federal Rules of Criminal Procedure and the All Writs Act. The All Writs Act provides in relevant part that "all courts established by Act of Congress may 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). Under this statute, a federal court has the power "to issue such commands" as "may be necessary or appropriate to effectuate and prevent the frustration of orders that it has previously issued in its exercise of jurisdiction otherwise obtained." *United States v. New York Telephone Co.*, 434 U.S. 159, 172 (1977).

Subject matter jurisdiction "refers to a tribunal's power to hear a case." *Morrison v. National Australia Bank, Ltd.*, 561 U.S. 247, 254 (2010) (internal quotation marks omitted); *In re Caterbone*, 640 F.3d 108, 111 (3d

[3] "Normally, a party who fails to object before the district court to a magistrate judge's ruling on a non-dispositive pretrial matter waives that objection on appeal." *Tabron v. Grace*, 6 F.3d 147, 153 n.2 (3d Cir. 1993).

Cir. 2011). A court has subject matter jurisdiction over an application for an All Writs Act order where it has subject matter jurisdiction over the underlying order that the All Writs Act order is intended to effectuate. *See In re Arunachalum*, 812 F.3d 290, 292 (3d Cir. 2016) (stating that before entertaining an application for a writ of mandamus under the All Writs Act, the court "must identify a jurisdiction that the issuance of the writ might assist" (quoting *United States v. Christian*, 660 F.2d 892, 894 (3d Cir. 1981))); *United States v. Denedo*, 556 U.S. 904, 911 (2009) ("As the text of the All Writs Act recognizes, a court's power to issue any form of relief—extraordinary or otherwise—is contingent on that court's subject-matter jurisdiction over the case or controversy.").

In *New York Telephone Co.*, the Supreme Court held that courts have authority under the All Writs Act to issue supplemental orders to third parties to facilitate the execution of search warrants. *See New York Telephone Co.*, 434 U.S. at 171-76. In that case, the government had obtained a search warrant for a pen register, but it needed the phone company's assistance to successfully accomplish the authorized surveillance. *See id.* at 175. The Supreme Court held that a court's authority to issue an All Writs Act order in support of a search warrant could even extend "to persons who, though not parties to the original action or

engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice" and "encompasses even those who have not taken any affirmative action to hinder justice." *Id.* at 174. Following *New York Telephone Co.*, this Court upheld an order under the All Writs Act requiring phone companies to assist with search warrants for trap and trace devices. *See In re Application of the United States for an Order Authorizing the Installation of a Pen Register or Touch-Tone Decoder and a Terminating Trap*, 610 F.2d 1148, 1155 (3d Cir. 1979) (hereinafter "*Trap and Trace Opinion*").

Thus, here, as under *New York Telephone Co.* and the *Trap and Trace Opinion*, the magistrate judge had subject matter jurisdiction to issue the All Writs Act order: the magistrate judge had authority pursuant to Rule 41 of the Federal Rules of Criminal Procedure to issue the search warrant for Doe's computer equipment, App. 49-51, and the All Writs Act order was issued in furtherance of that warrant. *See, e.g., Trap and Trace Opinion*, 610 F.2d at 1155 ("The courts issued these assistance orders in aid of their authority under Rule 41 to issue tracing warrants."). Doe cites *Sygenta Crop Protection, Inc. v. Henson*, 537 U.S. 28, 31 (2002), for the basic proposition that the All Writs Act does not in itself confer subject matter jurisdiction. *See* Br. 20. That proposition does not negate subject

matter jurisdiction here, however, because the underlying subject matter jurisdiction for the All Writs Act order was created when the magistrate judge issued the Rule 41 warrant.

The remainder (and bulk) of Doe's All Writs Act argument does not concern subject matter jurisdiction and is therefore subject to plain error review. Doe argues that the magistrate judge should not have issued an All Writs Act order in support of the search warrant when the government might have been able to proceed by a grand jury subpoena, *see* Br. 21-30, but this argument concerns whether issuing the All Writs Act order was in fact "necessary or appropriate," not whether the magistrate judge had subject matter jurisdiction. This Court should reject Doe's attempt to transform a question about whether the All Writs Act order was appropriate into a question of subject matter jurisdiction.

B. The Magistrate Judge Properly Issued the All Writs Act Order.

The magistrate judge did not err—much less plainly err—in issuing the All Writs Act order in support of the search warrant. As explained above, in *New York Telephone Co.*, the Supreme Court held that courts have authority under the All Writs Act to issue supplemental orders to third parties to facilitate the execution of search warrants. The Court considered three factors in concluding that the issuance of the All Writs Act order to

the phone company was appropriate: that the phone company was not "so far removed from the underlying controversy that its assistance could not be permissibly compelled," that the order did not place an undue burden on the phone company, and that the assistance of the company was necessary or appropriate to achieve the purpose of the warrant. *Id.* at 174-75. These factors support issuance of the All Writs Act order in this case, and Doe makes no argument to the contrary.[4]

Doe asserts that the government should have relied on a grand jury subpoena to compel Doe's assistance, rather than a search warrant and an All Writs Act order. This is error, for as discussed below, the law does not require the government to rely on a subpoena when a warrant is available. Although it is true that "[w]here 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 v. United States*

[4] Doe attempts to distinguish *New York Telephone Co.* based on his status as a target of the investigation and his allegation that he is being required to be "a witness against himself." Br. 29. It is certainly true that an All Writs Act order cannot be used to infringe an individual's privilege against self-incrimination. But where, as here, the order does not violate an individual's Fifth Amendment rights, the individual's proximity to the investigation strengthens the basis for obtaining an All Writs Act order pursuant to *New York Telephone Co.*, as an individual in close proximity to the investigation is not "so far removed from the underlying controversy that [his] assistance [cannot] be permissibly compelled." *New York Telephone Co.*, 434 U.S. at 174.

Marshals Service, 474 U.S. 34, 43 (1985), no statute addresses the extent to which third parties may be required to assist with the execution of Rule 41 warrants. Thus, consistent with the reasoning of *New York Telephone Co.*, the magistrate judge appropriately required Doe's assistance. In the absence of the All Writs Act order, the execution of a valid search warrant issued by a magistrate judge pursuant to Rule 41 would have been frustrated.

Nothing in the Federal Rules of Criminal Procedure or elsewhere required the government to rely on a subpoena issued under Rule 17 here rather than a warrant issued under Rule 41. Moreover, both this Court and the Supreme Court have rejected arguments that an investigation must proceed via subpoena rather than by warrant. In *Zurcher v. Stanford Daily*, 436 U.S. 547 (1970), the Supreme Court reversed a district court order that held that the government could not obtain a search warrant for evidence held by an innocent third party unless reliance on a subpoena would be impractical. The Court determined that the "Fourth Amendment has itself struck the balance between privacy and public need, and there is no occasion or justification for a court to revise the Amendment and strike a new balance by denying the search warrant in the circumstances present here and by insisting that the investigation proceed by subpoena." *Id.* at

559. Similarly, in *United States v. Educational Development Network Co.*, 884 F.2d 737 (3d Cir. 1989), the government had begun to use grand jury subpoenas in an investigation, but it also used inspector general subpoenas and search warrants to gather evidence at the same time. Appellants objected, asserting that the government had to proceed by grand jury subpoena only. *See id.* at 740. This Court firmly rejected that argument and held that the government may use search warrants or other subpoenas to gather evidence, even after a grand jury proceeding has begun. *See id.* at 740-44.

Doe's argument that the government was required to proceed by subpoena rather than by warrant is inconsistent with *Zurcher* and *Educational Development Network*. Moreover, because execution of the search warrant for the computer equipment would have been frustrated without the All Writs Act order, the magistrate judge properly issued the All Writs Act order in support of the warrant.

Additionally, Doe's argument that the government was required to proceed via subpoena rather than warrant and All Writs Act order has no case law support. He cites various cases on the important role of grand juries and grand jury subpoenas, *see* Br. 23-25, but none of these cases preclude use of warrants and All Writs Act orders as investigative tools

before indictment. Grand juries play an important role in criminal investigations, to be sure, but their authorities are not the exclusive means of investigating crimes.

Doe cites cases in which the government has used subpoenas to compel production of encrypted devices in a decrypted state, *see* Br. 26, but the government has also relied on All Writs Act orders in support of warrants as well. *See, e.g.*, *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1238 (D. Colo. 2012). Doe claims that the government has never before used the All Writs Act to require assistance of an uncharged suspect, but again he is wrong. In *United States v. Feldman*, No. 13-449, Doc. #6 (E.D. Wisc. May 21, 2013), a magistrate judge issued an All Writs Act order requiring a child pornography suspect to produce his encrypted devices in a decrypted state.[5]

Doe complains that use of the All Writs Act order rather than a subpoena "stripped appellant of significant protections," Br. 27, but the procedures associated with an All Writs Act order fully protect a

[5] The magistrate judge's order was not ultimately enforced. It was stayed pending review in the district court. While review was pending, the government managed to decrypt two of Feldman's devices on its own. Having obtained more than sufficient evidence to prove its case, the government moved to dismiss its application for an All Writs Act order. *See Feldman*, No. 13-449, at Doc. #9, 26.

defendant's due process rights. Doe was entitled to raise his Fifth Amendment privilege before the magistrate judge, and he did so.[6] App. 73. In addition, had Doe objected to the magistrate judge's ruling on his Fifth Amendment claim, he would have been entitled to *de novo* review of that claim before the district court and this Court. Doe failed to do so. *See* App. 229. He also failed to raise the claim as a defense to the contempt motion thereby precluding *de novo* review of his Fifth Amendment claim here. The Supreme Court has held that conditioning appellate review on the filing of objections to a magistrate judge's decision is consistent with due process. *See Thomas v. Arn*, 474 U.S. 140, 155 (1985).

Doe further objects that his period of incarceration is not limited to 18 months, *see* Doe Br. at 28, but he cites no case suggesting the existence

[6] Doe complains that the magistrate judge construed his Fifth Amendment claim as a motion for reconsideration, see Br. 27, but the magistrate judge addressed Doe's Fifth Amendment argument for the first time in the August 27 order, and the reasoning of that order suggests *de novo* review of Doe's privilege claim. App. 4-5 n.1 (specifying facts that support application of foregone conclusion doctrine and concluding that requiring Doe to assist "does not violate his privilege against self-incrimination"). Doe further objects that the Fifth Amendment ruling was based on a sworn affidavit, rather than testimony. Br. 27. But Doe did not raise this objection before the district court, and in any event, factual assertions in the affidavit were later the subject of testimony in the contempt hearings. Nor does Doe challenge the accuracy of any specific facts in the affidavit. For these reasons, any error regarding reliance on the affidavit was not prejudicial, and thus Doe cannot demonstrate that the magistrate judge committed plain error. *See Olano*, 507 U.S. at 734.

of a due process right to an 18-month limitation on incarceration for civil contempt. The fact that procedural protections associated with All Writs Act orders are not identical to those associated with subpoenas does not imply that the procedural protections associated with All Writs Act orders are inadequate. Indeed, given that search warrants have a higher evidentiary threshold than subpoenas, it would be odd to hold that due process requires an investigation to proceed by subpoena rather than search warrant.

The magistrate judge therefore did not commit any error, much less plain error, in issuing the All Writs Act order directing Doe to assist with decrypting the computer drives.

II. THE ALL WRITS ACT ORDER REQUIRES ONLY A NONTESTIMONIAL ACT OF PRODUCTION AND DOES NOT IMPLICATE DOE'S PRIVILEGE AGAINST SELF-INCRIMINATION

Standard of Review

This Court reviews Doe's claim of Fifth Amendment privilege for plain error, as Doe failed to preserve this issue for review. On August 27, 2015, the magistrate judge held that under the foregone conclusion doctrine, requiring Doe to assist in decrypting his devices would not violate his Fifth Amendment privilege against self-incrimination. App. 4-5 n.1. The magistrate judge also warned Doe that failure to object to the August 27 order could constitute a waiver of his appellate rights. *Id.* Doe did not object to that order, nor did he seek review of the magistrate's order by way of appeal, writ of mandamus, or any other type of relief. Nor did he renew his self-incrimination claim at either the hearing before the magistrate judge or the hearing before the district court judge. App. 229. This Court has held that failure to object to a magistrate judge's ruling on a dispositive motion results in plain error review. *See Brightwell v. Lehman*, 637 F.3d 187, 193 (3d Cir. 2011); *Nara v. Frank*, 488 F.3d 187, 195 (3d Cir. 2007).

Even if Doe had preserved his Fifth Amendment claim, whether an act of production involves testimonial self-incrimination would be a question of fact reviewed for clear error. *See United States v. Doe*, 465 U.S.

605, 613-14 (1984) (stating that Supreme Court would not overturn district court's finding that act of production would involve testimonial self-incrimination "unless it has no support in the record"); *United States v. Norwood*, 420 F.3d 888, 895 (8th Cir. 2005) ("Whether the existence of documents is a foregone conclusion is a question of fact, subject to review for clear error."*); United States v. Sideman & Bancroft*, LLP, 704 F.3d 1197, 1201 (9th Cir. 2013) (same).

Discussion

A. The All Writs Act Order Does Not Implicate Doe's Fifth Amendment Privilege Against Self-Incrimination

The All Writs Act order required Doe to produce his Mac Pro computer, two attached external hard drives, and his iPhone 6 "in a fully unencrypted state." App. 3. Doe repeatedly asserts that the All Writs Act order requires him to divulge his passcodes, but he is incorrect: the order requires no testimony from Doe, and he may keep his passcodes to himself. Instead, the order requires only that Doe produce his computer and hard drives in an unencrypted state. Under the reasoning of *Fisher v. United States*, 425 U.S. 391, 408-11 (1976), this act of production will not implicate Doe's Fifth Amendment privilege against self-incrimination because any potentially testimonial components that might be implicit in his act of

production are already known to the government. Doe's compliance with the order is a matter "not of testimony but of surrender."[7] *Id.* at 411.

1. The Fifth Amendment.

The Fifth Amendment states that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." However, "the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence." *Fisher v. United States,* 425 U.S. 391, 408 (1976). Instead, "the privilege protects a person only against being incriminated by his own compelled testimonial communications." *Id.* at 409. Thus, to fall within the protection of the Fifth Amendment the defendant must demonstrate: (1) compulsion, (2) a testimonial communication or act, and (3) incrimination.

As an initial matter, the information currently stored on Doe's electronic devices is not privileged because it was created and stored voluntarily rather than as a result of compulsion. In *Fisher*, where the government subpoenaed certain tax-related documents, the documents

7 The Electronic Frontier Foundation ("EFF") and the American Civil Liberties Union ("ACLU") filed a brief of amici curiae echoing Doe's argument that requiring a target to decrypt his computer devices violates the Fifth Amendment. The EFF and ACLU did not have the full record to review before taking this position; they instead relied only upon the unsealed filing by appellant John Doe. The government addresses the Fifth Amendment argument at length in this Section of this brief.

were not protected by the Fifth Amendment because "the preparation of all of the papers sought in these cases was wholly voluntary, and they cannot be said to contain compelled testimonial evidence." *Id.* at 409-10. The Court concluded that the "taxpayer cannot avoid compliance with the subpoena merely by asserting that the item of evidence which he is required to produce contains incriminating writing, whether his own or that of someone else." *Id.* In this case, the government did not compel Doe to create, obtain, or store any information on his electronic devices, and the information stored on the devices is therefore not protected by the Fifth Amendment. *See also United States v. Doe*, 465 U.S. 605, 611-12 (holding that the contents of documents were not privileged where respondent "does not contend that he prepared the documents involuntarily or that the subpoena would force him to restate, repeat, or affirm the truth of their contents").

2. The foregone conclusion doctrine.

The All Writs Act order does not require Doe to reveal his password or otherwise give any testimony. Instead, it directs him to produce the Mac Pro computer and two attached external hard drives "in a fully unencrypted state." App. 3. In *Fisher*, the Supreme Court recognized that an act of production may have testimonial components, and thus may be protected

by the Fifth Amendment. But *Fisher* also held that the Fifth Amendment did not protect an act of production when any potentially testimonial component of the act of production was "a foregone conclusion" that "adds little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411. This analysis is now known as the "foregone conclusion" doctrine, and its application to this case demonstrates that an order requiring Doe to produce his electronic devices in an unencrypted state does not violate his Fifth Amendment privilege against self-incrimination.

In *Fisher*, the government subpoenaed several categories of documents related to taxpayers' tax returns. The Court determined that "the act of producing evidence in response to a subpoena . . . has communicative aspects of its own, wholly aside from the contents of the papers produced." *Id.* at 410. For a subpoena seeking categories of documents, compliance with the subpoena concedes "the existence of the papers demanded and their possession or control by the taxpayer." *Id.* It also indicates the subpoena recipient's "belief that the papers are those described in the subpoena." *Id.* Nonetheless, the Supreme Court held that producing the documents sought in *Fisher* did not implicate the Fifth Amendment:

> It is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testimony within the protection of the

> Fifth Amendment . . . The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers.

Id. at 411. The Court concluded that "no constitutional rights are touched. The question is not of testimony but of surrender." *Id.*, quoting *In re Harris*, 221 U.S. 274, 279 (1911).

The act of producing an electronic device in an unencrypted state has potentially testimonial components similar, but not identical, to the potentially testimonial components involved in the act of responding to a subpoena for particular categories of documents. First, producing documents in response to a category-based subpoena demonstrates the document's existence; producing an unencrypted device will similarly demonstrate the device's existence. Second, compliance with a category-based subpoena demonstrates possession and control over the documents; producing an unencrypted device will similarly demonstrate possession and control over the device.

Regarding the knowledge implicitly demonstrated by the act of production, however, producing specified unencrypted devices may be less revealing than producing specified categories of documents in response to a subpoena. Producing papers in response to a category-based subpoena implicitly demonstrates knowledge of the contents of the papers produced:

it demonstrates the "belief that the papers are those described in the subpoena." *Fisher*, 425 U.S. at 410. In contrast, producing a device in an unencrypted state does not necessarily imply knowledge of the contents. The production implicitly demonstrates knowledge of the encryption password for the device. But the individual does not necessarily have knowledge of the contents stored on the device, as knowledge of the contents of a specified device is not needed to produce it in an unencrypted state.[8] At the same time, however, the government recognizes that where, as here, a search warrant has been issued for an individual's device based on probable cause to believe that it contains child pornography and that individual is then able to decrypt it, the individual's ability to produce the device in an unencrypted state will generally provide strong evidence of the individual's knowledge of the contents of the device. Accordingly, the government proceeds on the assumption that the production in this case has the potentially testimonial aspects of the act of production described in *Fisher*.

[8] For example, if Ann gives Bob an encrypted computer and reveals to him the password, Bob would be fully capable of producing the computer in an unencrypted state, even though he may have no idea what is stored on it. But if Bob were to receive a subpoena for child pornography files stored on the computer, he could not produce responsive files without knowing the contents of the computer.

3. The foregone conclusion doctrine applies here.

In this case, requiring Doe to produce his electronic devices in an unencrypted state is a matter of surrender, not testimony. The government's knowledge in this investigation includes any potentially testimonial or communicative component implicit in Doe's act of decrypting his electronic devices. In particular, the government has knowledge that the targeted devices exist, that they belonged to Doe, and that Doe knows the passwords necessary to decrypt them. In addition, to the extent that the government must have prior knowledge of the drives' contents, the government also knows that child pornography is stored on the drives. The magistrate judge's determination that the foregone conclusion doctrine applies in this case was not plain error, clear error, or any error at all.

To begin, the fact that the devices actually exist is known to the government in this case: they are in the government's possession, seized from Doe as a result of a search warrant issued for his home. App. 38. This is not a fishing expedition on the part of the government, nor is it a guessing game as to whether the evidence exists. The existence of the devices at issue is a fact in this case. *Cf. United States v. Hubbell*, 530 U.S. 27, 45 (2000) (holding that foregone conclusion did not apply to subpoena

where government did not demonstrate prior knowledge of the existence or location of the subpoenaed documents). The magistrate judge's finding that "the Government has custody of the electronic devices" is not clearly erroneous. App. 5.

Secondly, Doe's ownership and prior control of the devices are also known facts. The equipment was seized from Doe's Lansdowne apartment by Delaware County detectives pursuant to the search warrant. App. 38. Doe acknowledged his control over the Mac Pro and attached drives when he told detectives that he had FileVault encryption and Freenet on his computer. App. 38, 354. Doe rented the Lansdowne apartment since at least 2013, and he lived there alone, until he allowed his sister to move in approximately one month prior to the search warrant, in February 2015. App. 40, 94, 97. Doe's sister also identified as belonging to Doe the computers seized by Delaware County detectives from Doe's apartment. App. 97, 241-44.

Doe further demonstrated his ownership and control over the devices seized from his apartment by providing passwords to some of the equipment to police on the day of the search warrant, App. 38, 118, 294, 332-33, and by refusing to provide other passwords or encryption codes to his computer or hard drives to police, despite advising that he knew what

those passcodes were. App. 38, 118-19, 354-55. Doe provided the password to his iPhone 5S, and hidden in that phone was the recovery key to access his Mac Pro computer, to which his hard drives were connected. App. 38-39, 118, 121-23, 300-01. In addition, Doe once again acknowledged his ownership of all of the seized equipment, including the external hard drives still at issue, in the presence of his then-attorney, Perry DeMarco, Jr., when he appeared at Delaware County CID on the magistrate judge's order to unencrypt his devices and immediately advised that he "forgot" the passwords to the hard drives. App. 136, 319-20. All of the evidence adduced at the hearings established Doe's exclusive ownership and control of all of the devices. The magistrate judge's finding that Doe "possessed" and "owned" the devices is not clearly erroneous. App. 5.

Third, Doe's knowledge of the passwords was amply proven by the government and unrefuted by Doe. He gave over his passcodes for his iPhone 5S and Apple iPad to police on the day of the search warrant, and he also told them that his computer and hard drives were password protected and encrypted, and that he knew the codes but would not turn them over to police. App. 38-39, 118-19, 354-55. Other evidence also showed that Doe knew the passwords to his computers. App. 97-99. His sister observed him enter his passwords over a period of years, and he always entered the

password from memory, regardless of their length. App. 98-100. In fact, Doe had multiple layers of password protection on his devices, and he always entered his passcodes for all of his devices from memory. App. 100, 246-49. Doe never had any trouble remembering his passcodes (other than when compelled to do so by the federal court), never hesitated when entering the passcodes, and never failed to gain entry on his first attempt. App. 100, 246-47. Doe's ability to remember his passwords is further confirmed by his ability to decrypt his iPhone 6. On his iPhone 6, there were three levels of passwords and encryption codes that were installed by Doe, including a more complicated alphanumeric code, which he was able to recall from memory alone. App. 326-27, 341-43. This Doe was able to accomplish on a phone that he owned for less than two months, and which police possessed for a period longer than Doe had owned it – more than three months – before Doe decrypted it.[9] App. 251.

[9] After Delaware County detectives seized his iPhone 5S and computer equipment pursuant to the search warrant on March 30, 2015, Doe immediately obtained a new cell phone, the iPhone 6 later seized by Philadelphia Police on May 26, 2015. App. 251. It was this phone that Doe used to take the photographs and video of his nieces. Doe's iPhone 6 remained in police custody, and on September 4, 2015, Doe appeared at Delaware County CID and unencrypted his iPhone 6 by entering three levels of passcodes completely from memory. App. 326-27.

There was more than ample evidence that Doe knew the passwords to his computer. Most significantly, the evidence demonstrated that Doe had so clearly committed these passwords and encryption codes to memory that there was no need to document them anywhere, because there was no danger to Doe that he would ever fail to recall them. The magistrate judge's finding that Doe "accessed" the devices is not clearly erroneous. App. 5.

Lastly, the evidence demonstrated that child pornography is stored on the devices. Doe's own sister viewed his collection of child pornography from the computer equipment that is now in the possession of Delaware County.[10] App. 40, 101, 240, 247-48, 280-81. Her testimony was corroborated by the forensic expert testimony which established that Doe had requested known child pornography files from the message boards on

[10] Doe attempts to disparage his sister by arguing that she had questionable credibility and attenuated testimony. Br. 46. He incorrectly asserts that "as Mr. Doe was ceasing to provide her with financial support, she contacted a detective." *Id*. In fact, though counsel *attempted* to establish a financial motive at both hearings, App. 263, Doe's sister testified that she went to detectives because Doe had promised his family that he would get help for his problem with child pornography and had not only failed to do so, but had continued his involvement in child pornography by moving on to his own 4- and 6-year-old nieces. App. 252, 271. Doe's sister actually described their relationship as close, closer than with any other sibling before Doe's continued involvement in child pornography. App. 92-93, 104-05, 234. Doe's challenges here to his sister's credibility do not demonstrate clear error in the magistrate judge's determination that the foregone conclusion doctrine applies in this case.

the Internet and through Freenet, App. 311-13, 339-40, 345-47, and, more importantly, that Doe successfully downloaded those files. App. 308-10, 336-37, 339-40, 349. Doe had requested approximately 20,000 files, App. 307, and a sample of just three of those files demonstrated the hard core nature of the child pornography that Doe possessed on his devices. App. 306-07, 391. The examiner also found on the Mac Pro references to these child pornography files from Freenet being stored on the external hard drives. App. 303-05, 308-10, 337, 339-40. This forensic testimony provided the court with independent proof, unrefuted by Doe, that child pornography is contained on the very devices Doe refuses to decrypt – his two external hard drives. The magistrate judge's finding that "there are images on the electronic devices that constitute child pornography" is not clearly erroneous. App. 5.

Thus in this case, where Doe's ownership and ability to decrypt his devices is established, and where the existence of child pornography on those devices is known, the magistrate judge's determination that the foregone conclusion doctrine applies was not clearly erroneous. Doe's Fifth Amendment argument must fail.

4. The All Writs Act order is consistent with other caselaw regarding compelled production of devices in an unencrypted state.

At least three other courts have relied on the foregone conclusion doctrine to require production of an electronic device in a decrypted state. The facts of *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009), are most similar to this case. At a border crossing, Boucher revealed child pornography images on his computer to a federal agent. The agent seized his computer and obtained a search warrant, but the agent was later unable to decrypt the computer. Applying the foregone conclusion doctrine, the court required Boucher to produce his computer in a decrypted state. *See id*. at *3-4. Here, as in *Boucher*, the government knows that the hard drives belong to Doe, that Doe can decrypt them, and that child pornography is stored on the drives.

In *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 614 (Mass. 2014), and *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1235 (D. Colo. 2012), the courts applied the foregone conclusion doctrine to compel production of unencrypted devices without a showing that the government knew specifically what was stored on the devices. In *Gelfgatt*, the defendant had engaged in fraud, and he told the police on the day of his arrest that he was able to decrypt his computers. *Gelfgatt*, 11 N.E.3d at 610. In *Fricosu*, the

government had recorded jailhouse phone calls demonstrating that the defendant knew her computer was encrypted and accessible only with a password that she believed she could not be compelled to disclose. *Fricosu*, 841 F. Supp. 2d at 1235. The government did not in either case demonstrate knowledge of the specific information stored on the devices. Nevertheless, both courts required production of the devices in an unencrypted state pursuant to the foregone conclusion doctrine. *Gelfgatt*, 11 N.E.3d at 615 ("the factual statements that would be conveyed by the defendant's act of entering an encryption key in the computers are 'foregone conclusions'"); *Fricosu*, 841 F. Supp. 2d at 1237. Here, it is not necessary for this Court to determine whether the foregone conclusion doctrine would apply if the government had only established that Doe could decrypt his drives, as the government also established that he stores child pornography on them.

Doe relies heavily on *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012), but that decision is easily distinguishable. In that case, law enforcement officers conducting a child pornography investigation seized several items of encrypted electronic storage media from the defendant's hotel room. *Id*. at 1338-39. However, officers lacked evidence either that the defendant knew the password for any of the devices or that there were any child pornography files stored on

them. *Id*. at 1346. Under these circumstances, the court concluded that the foregone conclusion doctrine did not apply because the government had failed to show "that encrypted files exist on the drives, that [the defendant] has access to those files, or that he is capable of decrypting the files." *Id*. at 1349. Here, by contrast, the government knows that Doe has access to and is capable of decrypting his hard drives, and it has evidence from both a witness and forensic examination regarding the information stored on the drives. Thus, the government here can satisfy even the exacting standards set by the Eleventh Circuit for the application of the foregone conclusion doctrine.

Doe cites several cases in which the government attempted to compel a defendant to disclose a password, rather than compelling production of a device in an unencrypted state, but here Doe is not asked to make such a disclosure. See *SEC v. Huang*, 2015 WL 5611644, at *1-2 (E.D. Pa. Sept. 23, 2015); *Commonwealth v. Baust*, 89 Va. Cir. 267 (2014); *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010). Cases involving compelled disclosure of passwords simply do not involve the foregone conclusion doctrine, which applies only to an act of production, not to testimony. Under the foregone conclusion doctrine, an act of production is not testimonial when the facts implicit in the production are already known

to the government. See *Fisher*, 425 U.S. at 411. In contrast, revealing a password from memory is testimonial. For example, in *Boucher*, the court required the defendant to produce his laptop in an unencrypted state only after the government abandoned its attempt to compel the defendant to disclose his password. See *Boucher*, 2009 WL 424718, at *2, *4.

Doe's assertion that the foregone conclusion doctrine is limited only to "specifically identified files" is mistaken. Doe cites *United States v. Hubbell*, 530 U.S. 27 (2000), but in that case the government subpoenaed broad categories of documents. As the government had no "prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent," the Supreme Court held that the foregone conclusion doctrine did not apply. *Id*. at 44-45. In this case, however, the All Writs Act order is not directed to broad categories of documents or files about which the government lacks prior knowledge; it directs Doe to assist with decryption of two specific hard drives. Nothing in *Hubbell* or *Fisher* suggests that the foregone conclusion doctrine cannot apply to a single storage medium, any more than those cases suggest that the foregone conclusion doctrine must be applied on a paragraph-by-paragraph or sentence-by-sentence basis to a document. The All Writs Act order in this case directs Doe to assist with execution of a search warrant by

producing two hard drives in an unencrypted state, and the foregone conclusion doctrine applies because the potentially testimonial components of that act of production are already known to the government.[11]

As Doe notes, the Supreme Court has distinguished compelled disclosure of the combination of a strongbox, which is testimonial, from surrender of a key, which is not. See *Doe v. United States*, 487 U.S. 201, 210 n.9 (1988); *Hubbell*, 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."). Here, however, the government has not compelled disclosure of either a combination or a key; the All Writs Act order is more analogous to an order to surrender the contents of a safe. Such an act, however, remains an act of surrender, not testimony. Otherwise, a defendant could avoid disclosure of a document otherwise subject to the foregone conclusion doctrine by storing it in a combination-protected strongbox. Similarly, Doe's attempt to equate

[11] Doe also complains that there was no evidence admitted as to how the Freenet investigation led to Doe. Br. 45. However, Doe fails to recognize that the hearings in this case were based on the motion for contempt, and basis for the Freenet investigation was not relevant to the contempt hearing. Indeed, the Fifth Amendment issue Doe raises now was not addressed in either contempt hearing, as Doe did not object to the magistrate judge's August 27 order. Regardless, the record in this case set forth sufficient evidence to support the magistrate court's finding of a foregone conclusion.

disclosure of a password with disclosure of a device in an unencrypted state should be rejected because it would effectively nullify the foregone conclusion doctrine. If the foregone conclusion doctrine does not apply to encrypted information, the recipient of a subpoena could avoid application of the foregone conclusion doctrine in every case simply by using encryption.

Doe argues that producing a device in an unencrypted state is protected by the Fifth Amendment because it requires him to use his mind, Br. 33-37, but employing the contents of the mind is materially different from testifying to the contents of the mind. An individual producing documents that are the subject of the foregone conclusion doctrine under *Fisher* must use the contents of his mind, including his knowledge of the location of the documents. However, the act of producing documents is not testimonial regarding where they might have been located. The foregone conclusion doctrine applies where the potentially testimonial components of the act of production are known to the government; it does not require that the act of production be mindless.

B. Doe's Remaining Objections Are Without Merit.

Doe's remaining arguments are unavailing. Doe cites *Riley v. California*, 134 S. Ct. 2473 (2014), and notes his strong privacy interests in

his computer, Br. 36, but these interests are protected by the Fourth Amendment, not the Fifth Amendment. Here, Doe's Fourth Amendment interests are not violated because the government obtained a warrant to search his computer (in contrast to the warrantless cell phone search at issue in *Riley*).

Doe suggests that if he were directed to produce a particular thumbnail image from his drives (which would be impossible if Doe did not know the password), the government should grant him immunity or use a taint team. *See* Br. 48-49. Doe is not entitled to a grant of immunity because where the foregone conclusion doctrine applies, an act of production is not testimonial and thus not protected by the Fifth Amendment. *See Fisher*, 425 U.S. at 411. In addition, no taint team is needed here: once Doe complies with the All Writs Act order and produces the drives in an unencrypted state, the government will be able to complete review of the devices consistent with the search warrant.

CONCLUSION

For the reasons stated above, the government respectfully requests that the judgment of the district court be affirmed.

Respectfully submitted,

LESLIE R. CALDWELL
Assistant Attorney General
Criminal Division

/s Nathan Judish
NATHAN JUDISH
Attorney, Computer Crime and Intellectual Property Section, Criminal Division

ZANE DAVID MEMEGER
United States Attorney

/s Bernadette McKeon
BERNADETTE MCKEON
Assistant United States Attorney
Acting Chief of Appeals

/s Michelle Rotella
MICHELLE ROTELLA
Assistant United States Attorney
Pa. Bar No. 67265
United States Attorney's Office
615 Chestnut Street, Suite 1250
Philadelphia, PA 19106
(215) 861-8471

CERTIFICATION

1. The undersigned certifies that this brief contains 11,788 words, exclusive of the table of contents, table of authorities, and certifications, and therefore complies with the limitation on length of a brief stated in Federal Rule of Appellate Procedure 32(a)(7)(B).

2. I hereby certify that the electronic version of this brief filed with the Court was automatically scanned by OfficeScan Real-Time Scan Monitor, version 10.5, by Trend Micro, 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 Michelle Rotella
MICHELLE ROTELLA
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that this brief has been served on the Filing User identified below through the Electronic Case Filing (ECF) system:

Keith Donoghue, Esquire
Assistant Federal Defender
Federal Community Defender Office
601 Walnut Street, Suite 540 West
Philadelphia, PA 19106

Kit Walsh, Esquire
Counsel for Amici Curiae
Electronic Frontier Foundation and
American Civil Liberties Union
815 Eddy Street
San Francisco, CA 94109

/s Michelle Rotella
MICHELLE ROTELLA
Assistant United States Attorney

DATED: May 16, 2016.