

No. 00-0000

IN THE SUPREME COURT OF
THE UNITED STATES

COMMONWEALTH OF PENNSYLVANIA
Petitioner

v.

JOSEPH J. DAVIS
Respondent

ON PETITION FOR WRIT OF *CERTIORARI* TO THE
SUPREME COURT OF PENNSYLVANIA

APPENDICES TO PETITION FOR
WRIT OF *CERTIORARI*

JOSH SHAPIRO
Attorney General
Commonwealth of Pennsylvania

JENNIFER C. SELBER
Executive Deputy Attorney General
Director, Criminal Law Division

JAMES P. BARKER
Chief Deputy Attorney General
Appeals & Legal Services Section

WILLIAM R. STOYCOS *
Senior Deputy Attorney General
Counsel of Record

Office of Attorney General
16th Floor, Strawberry Square
Harrisburg, PA 17120
(717) 787-6348

**JOSEPH J. DAVIS PETITION FOR WRIT OF
CERTIORARI APPENDICES**

<u>Appendix</u>	<u>Document</u>
A	Supreme Court of Pennsylvania Majority Opinion
B	Supreme Court of Pennsylvania Minority Opinion
C	Superior Court of Pennsylvania Panel Opinion
D	Luzerne County Court of Common Pleas Opinion and Order

[J-42-2019]
IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

SAYLOR, C.J., BAER, TODD, DONAHUE,
DOUGHERTY, WECHT, MUNDY, JJ.

COMMONWEALTH OF PENNSYLVANIA,
Appellant

v.

JOSEPH J. DAVIS,
Appellee

No. 56 MAP 2018

Appeal From The Order Of The
Superior Court Dated November 30,
2017 At No. 1243 MDA 2016, Affirming
The Order Of The Court Of Common
Pleas Of Luzerne County, Criminal
Division, Dated June 30, 2016 Nos.
CP-40-CR-291-2016 and CP-40-MD-11-
2016.

ARGUED: May 14, 2019

OPINION

JUSTICE TODD DECIDED: November 20, 2019

In this appeal by allowance, we consider an issue of first impression: Whether a defendant may be compelled to disclose a password to allow the Commonwealth access to the defendant's lawfully-seized, but encrypted, computer. For the reasons that follow, we find that such compulsion is violative of the Fifth Amendment to the United

States Constitution's prohibition against self-incrimination. Thus, we reverse the order of the Superior Court.

On July 14, 2014, agents of the Office of Attorney General ("OAG"), as part of their investigation of the electronic dissemination of child pornography, discovered that a computer at an identified Internet Protocol (IP) address¹ registered with Comcast Cable Communications ("Comcast"), repeatedly utilized a peer-to-peer file-sharing network, eMule, to share child pornography. N.T. Hearing, 1/14/16, at 6-8. Specifically, agents used a computer with software designed to make a one-to-one connection with the computer at the aforementioned IP address and downloaded a file, later confirmed to contain child pornography, which was saved to the OAG computer. *Id.* at 5-6. Based upon its transference and review of the file, the OAG obtained a court order to compel Comcast to provide subscriber information associated with the IP address. The information provided by Comcast disclosed the subscriber as Appellant Joseph Davis, as well as his address. *Id.* at 8-9.

On September 9, 2014, the OAG applied for, received, and executed a search warrant at Appellant's apartment. OAG Special Agent Justin Leri informed Appellant that he was not under arrest, but that the search involved an investigation of child pornography. *Id.* at 11. Appellant was then read his *Miranda* warnings and

¹ IP addresses identify computers on the Internet, enabling data transmitted from other computers to reach them. *National Cable & Telecomm. Ass'n v. Brand X Internet Services*, 545 U.S. 967, 987 n.1 (2005).

waived his *Miranda* rights. *Id.* Appellant acknowledged that he was the sole user of a Dell computer.² He admitted to having prior pornography convictions, but denied the computer contained any illegal pornographic images. Appellant then declined to answer additional questions without a lawyer. *Id.* Later examination of the computer revealed that the hard drive had been “wiped,” removing data entirely or rendering it unreadable. *Id.* at 43-44.

On October 4, 2015, OAG Agent Daniel Block identified a different child pornography video that was shared with a different IP address utilizing the eMule server. An administrative subpoena to Comcast regarding this IP address again produced Appellant’s name and contact information. A direct connection was made from OAG computers to this IP address, and one electronic file containing child pornography was transferred to the OAG computer. *Id.* at 19.

On October 20, 2015, the OAG executed another search warrant at Appellant’s apartment based upon this video. At Appellant’s apartment, the agents discovered a single computer, an HP Envy 700 desktop. After being *Mirandized*, Appellant informed the agents that he lived alone, that he was the sole user of the computer, and that he used hardwired Internet services which are password protected, and, thus, not accessible by the public, such as through Wifi. *Id.* at 26. Appellant offered that only he knew the password to his

² The Dell computer seized in this search is not the subject of the Commonwealth’s motion to compel a password at issue in this matter.

computer. *Id.* Appellant also informed the agents, *inter alia*, that he watched pornography on the computer which he believed was legal; that he had previously been arrested for child pornography; and that child pornography was legal in other countries so he did not understand why it was illegal in the United States. *Id.* at 27-28. The agents arrested Appellant for the eMule distributions and seized his computer. Agent Block asked Appellant for the password to this computer and Appellant refused. *Id.* at 28. Subsequently, when in transit to his arraignment, Appellant spoke openly about watching various pornographic movies, indicating that he particularly liked watching 10, 11, 12, and 13-year olds. *Id.* at 30. Agent Block again requested that Appellant provide him with the password to the computer. Appellant responded: "It's 64 characters and why would I give that to you? We both know what's on there. It's only going to hurt me. No f*cking way I'm going to give it to you." *Id.*

Later, in a holding cell, Agent Leri conversed with Appellant who, *inter alia*, offered that he believes the "government continuously spies on individuals," and questioned "why it's illegal to . . . view movies in the privacy of [his] own home." *Id.* at 35. In a later conversation, Agent Leri asked Appellant if he could remember the password. Appellant replied that he could not remember it, and that, even if he could, it would be like "putting a gun to his head and pulling the trigger." *Id.* at 35-36. In a subsequent visit, when asked again about the password, Appellant offered that "he would die in jail before he could ever remember the password." *Id.* at 37.

A supervisory agent in computer forensics, Special Agent Braden Cook, testified that a portion

of Appellant's HP 700 Envy computer's hard drive was encrypted with a program called TrueCrypt Version 7.1. *Id.* at 42. The entire hard drive of the computer was encrypted and "there was no data that could be read without opening the TrueCrypt volume." *Id.* at 46. Agent Cook could only confirm that there was "Windows on the computer and the TrueCrypt," and he had no knowledge of any specific files other than the operating system files. *Id.* at 50-51.

Appellant was charged with two counts of disseminating child pornography in violation of 18 Pa.C.S. § 6312(c), and two counts of criminal use of a communication facility in violation of 18 Pa.C.S. § 7512(a), which arose from the July 2014 and October 2015 detections.

On December 17, 2015, the Commonwealth filed with the Luzerne County Court of Common Pleas a pre-trial motion to compel Appellant to divulge the password to his HP 700 computer. Appellant responded by invoking his right against self-incrimination. On January 14, 2016, the trial court conducted an evidentiary hearing at which several OAG agents testified, as set forth above, about the investigation supporting the seizure of the computer.

The trial court focused on the question of whether the encryption was testimonial in nature, and, thus, protected by the Fifth Amendment. The trial court opined that "[t]he touchstone of whether an act of production is testimonial is whether the government compels the individual to use 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact." Trial Court Opinion, 6/30/2016, at 8-9 (citation omitted). As part of its analysis, the trial court looked to the

“foregone conclusion” exception to the Fifth Amendment privilege against self-incrimination as articulated by the United States Supreme Court in *Fisher v. United States*, 425 U.S. 391, 409 (1976). The court noted the rationale underlying this doctrine is that an act of production does not involve testimonial communication if the facts conveyed are already known to the government, such that the individual “adds little or nothing to the sum total of the government’s information.” Trial Court Opinion, 6/30/2016, at 9 (quoting *Fisher*, 425 U.S. at 409). The trial court offered that for this exception to apply, the government must establish its knowledge of (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence. *Id.* at 9.

Applying the foregone conclusion exception, the trial court found that, in the case at bar, the computer located in Appellant’s residence had hard-wired Internet access only; Appellant admitted it was TrueCrypt encrypted; that he was the only user, and he was the only one who knew the password; Appellant indicated to the agents that “we both know what is on there,” and stated that he would “die in prison before giving up the password;” and that the Commonwealth knew with a reasonable degree of certainty that child pornography was on the computer. *Id.* at 11. Based upon these facts, the trial court determined that the information the Commonwealth sought from Appellant was a foregone conclusion, in that the facts to be conveyed by Appellant’s act of production of his password already were known to the government. As, according to the trial court, Appellant’s revealing his password would not provide the Commonwealth

with any new evidence, and would simply be an act that permitted the Commonwealth to retrieve what was already known to them, the foregone conclusion exception was satisfied. Thus, on June 30, 2016, the trial court granted the Commonwealth's motion and directed Appellant to supply the Commonwealth with any passwords used to access the computer within 30 days. Appellant filed an interlocutory appeal.

A three-judge panel of the Superior Court affirmed. *Commonwealth v. Davis*, 176 A.3d 869 (Pa. Super. 2017).³ Like the trial court, the Superior Court found that, to qualify for the Fifth Amendment privilege, a communication must be testimonial. The Superior Court observed that the question of whether compelling an individual to provide a digital password was testimonial in nature was an issue of first impression for the court. Building upon the trial court's analysis, the Superior Court explained that the Fifth Amendment right against self-incrimination is not violated when the information communicated to the government by way of a compelled act of production is a foregone conclusion. The court reasoned that the foregone conclusion exception provides that an act of production does not involve testimonial

³ The Superior Court initially considered whether it had jurisdiction to entertain the trial court's interlocutory order on appeal. In sum, the court determined that the order satisfied each of the requirements of the collateral order doctrine as set forth in Pa.R.A.P. 313(b). The parties do not question this determination on appeal. While the matter is jurisdictional in nature, and, thus, non-waivable and subject to *sua sponte* consideration by this Court, *Commonwealth v. Shearer*, 882 A.2d 462, 465 n.4 (Pa. 2005), we do not disagree with the Superior Court's analysis.

communication where the facts conveyed already are known to the government and set forth the applicable three-prong test. *Id.* at 874-75 (citing *Fisher*, 425 U.S. at 410-13).

Applying the foregone conclusion exception, the Superior Court, contrary to the trial court, focused on the password itself, and reasoned that the Commonwealth established the computer could not be opened without the password, that the computer belonged to Appellant and the password was in his possession, and that this information was "self-authenticating" — *i.e.*, if the computer was accessible upon entry of the password, the password was authentic. *Id.* at 876. Further, the court noted that multiple jurisdictions have held that the government's knowledge of the encrypted documents or evidence that it sought to compel did not need to be exact, and determined that, based on the agents' forensic investigation, as well as Appellant's own statements to the agents while in custody, there was a high probability that child pornography existed on his computer. Thus, the Superior Court concluded that the trial court did not err in holding that the act of providing the password in question was not testimonial in nature and that Appellant's Fifth Amendment right against self-incrimination would not be violated by compelling him to disclose the password.

Our Court granted allocatur to consider the following issue, as framed by Appellant:

May [Appellant] be compelled to disclose orally the memorized password to a computer over his invocation of privilege under the Fifth Amendment to the Constitution of the United States, and Article I, [S]ection 9 of the Pennsylvania

Constitution?

Commonwealth v. Davis, 195 A.3d 557 (Pa. 2018) (order). The parameters of our review of an issue involving a constitutional right is well settled. Our standard of review is *de novo*, and our scope of review is plenary. *Commonwealth v. Baldwin*, 58 A.3d 754, 762 (Pa. 2012).

Appellant argues the Fifth Amendment prohibits government compulsion to disclose a computer password against one's will, reasoning that requiring an individual to recall and disclose the memorized password is quintessentially testimonial, *i.e.*, revealing the contents of one's own mind. Indeed, according to Appellant, the privilege is not just about information, but is "about a core of individual autonomy into which the state may not encroach." Appellant's Brief at 16. Appellant maintains that, as his password exists in his mind, he cannot be compelled to remember the password or reveal it, as a person's thoughts and knowledge are at the core of the Fifth Amendment.

According to Appellant, the Fifth Amendment protects against not only compelled written and oral testimony, but nonverbal acts as well. Appellant continues that, while not at issue in this appeal, even if the Commonwealth had obtained an order compelling Appellant to physically enter his password into his computer — rather than forcing him to speak or write down his password — this would still constitute a form of written testimony and, in any event, such a demand for action still requires using the contents of his mind to enter his password. Appellant contrasts such compulsion with one requiring merely physical acts, such as being required to wear a particular shirt, provide a blood sample, or provide a handwriting exemplar,

which are not testimonial in nature, as they do not rely on the contents of one's mind. See *Holt v. United States*, 218 U.S. 245, 252-53 (1910); *Schmerber v. California*, 384 U.S. 757, 761 (1966); *Gilbert v. California*, 388 U.S. 263, 266-67 (1967). Appellant offers that providing a password that will unlock data on a computer is no different from providing a combination that unlocks a briefcase or a safe, which has been held to be testimonial in nature.

Appellant further asserts that the Supreme Court's "foregone conclusion' rationale," as set forth in *Fisher*, does not apply to computer passwords. Appellant's Brief at 24. Appellant suggests that the holding in *Fisher* was limited to its facts and merely involved the question of whether the disclosure of certain tax documents known to be in the possession of the defendants' attorneys, as agents of the defendants, could be compelled by the government. In distinguishing *Fisher*, Appellant not only emphasizes that in that case the request did not compel oral testimony, or require restating, repeating, or affirming the truth of the contents of the documents, but explains that, because accountants prepared the papers which were ultimately possessed by defendants' attorneys, and could independently authenticate them, the Government was not relying upon the "truth-telling" of the defendants. *Fisher*, 425 U.S. at 411.

Appellant submits that, regardless of the scope of the foregone conclusion rationale, it is limited to the act of producing documents and that, as discussed below, the United States Supreme Court has applied the foregone conclusion exception only once since *Fisher*, rejecting its usage in the context of the compelled production of business

records. *United States v. Hubbell*, 530 U.S. 27 (2000) (dismissing government's reliance on foregone conclusion exception, finding that compulsion to produce papers that would require defendant to make use of his own mind to identify hundreds of documents responsive to the request did not fall within the exception).

Appellant asserts that, even if the foregone conclusion rationale could apply to the compelled decryption of a computer, it cannot be satisfied in this matter. Specifically, as to the password itself, Appellant contends that it is not a foregone conclusion that he even knows the password at this time. Likewise, if the rationale goes to the presence of contraband on Appellant's computer, which Appellant maintains that it does, here, the OAG agents noted that they could not tell what might be on the confiscated computer, and, as the computer was not connected to the Internet when it was seized, there is no proof that it was the one used to share pornography on eMule.⁴ Finally, Appellant

⁴ Appellant also argues an independent basis for protection against disclosure of the password under Article I, Section 9 of the Pennsylvania Constitution. Appellant engages in a detailed analysis, offering that the text of the Pennsylvania charter as well as the history of the provision suggests broader protections thereunder. The Commonwealth strongly asserts throughout its brief that Appellant has waived his state constitutional law claim, and maintains that, in any event, such claim has no merit, stressing the numerous decisions in which our Court has indicated the rights under the sister sections are coterminous. As we resolve this matter on federal Constitutional grounds, we need not address the Commonwealth's waiver contention or Appellant's underlying assertion of the recognition of greater rights under the Pennsylvania Constitution.

adds that the relatively few states that have considered the decryption password issue have reached divergent conclusions, and stresses that the national trend is toward greater protections.

The Commonwealth explains that the Fifth Amendment, by its terms, provides that no person shall be compelled in any criminal case to be a witness against himself; thus, according to the Commonwealth, this Amendment covers only communications that are testimonial, and the compulsion to produce physical evidence is not protected. The Commonwealth relies almost exclusively on what it describes as the foregone conclusion “doctrine,” as articulated in *Fisher* and other decisional law. The Commonwealth surveys various decisions and submits that the majority of cases find it logical and sound to extend the foregone conclusion exception to providing the password to an encrypted device. Here, according to the Commonwealth, the compelled act is the surrendering of the password, and the “testimony” inherent in Appellant’s production of the password — the existence, location, and authenticity, *of the password* — is a foregone conclusion. In short, the Commonwealth contends that revealing the password will add nothing communicative to the government’s information as it does not disclose information about the computer or its contents. Thus, the Commonwealth asserts it has met its burden in this regard.⁵

⁵ *Amicus* for Appellant, the Electronic Frontier Foundation, stresses that compulsion to disclose a computer password subjects an individual to a “cruel trilemma” — to choose between providing the allegedly incriminating information; lying about the purported inability to do so; or refusing to

Our analysis begins with the United States Constitution. The Self-Incrimination Clause of the Fifth Amendment provides “[n]o person . . . shall be compelled in any criminal case to be a witness against himself.” U.S. Const. amend. V. This privilege not only applies to a defendant in a criminal trial, but “in any other proceeding, civil or criminal, formal or informal, where the answers might incriminate [the speaker] in future criminal proceedings.” *Minnesota v. Murphy*, 465 U.S. 420, 426 (1984) (citation omitted). “Although the text does not delineate the ways in which a person might be made a ‘witness against himself,’ we have long held that the privilege does not protect a suspect from being compelled by the State to produce ‘real or physical evidence.’ Rather, the privilege ‘protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature.’” *Pennsylvania v. Muniz*, 496 U.S. 582, 588-89 (1990) (citations omitted). As offered by Justice Oliver Wendell Holmes, “the prohibition of compelling a man in criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his

cooperate and be held in contempt. According to *Amicus*, the privilege was designed to prevent this trilemma. In a joint *amicus* brief in support of the Commonwealth, various states provide an interesting history of modern encryption, press the troubling consequences of Appellant’s position — including the altering of the balance of power, rendering law enforcement incapable of accessing large amounts of relevant evidence — and warn that adopting Appellant’s position could result in less privacy, not more, in the form of draconian anti-privacy legislation.

body as evidence when it may be material." *Holt*, 218 U.S. at 252-53. Indeed, "in order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself." *Doe v. United States*, 487 U.S. 201, 210 (1988) ("*Doe II*") (footnote omitted).

However, in the realm of the non-physical disclosure of information, the privilege is broad, as "compelled testimony that communicates information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory." *Id.* 487 U.S. at 208 n.6. Thus, it is a "protection against the prosecutor's use of incriminating information derived directly or indirectly from the compelled testimony." *Hubbell*, 530 U.S. at 38.

The primary policy undergirding the Fifth Amendment privilege against self-incrimination is our country's "fierce 'unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt' that defined the operation of the Star Chamber, wherein suspects were forced to choose between revealing incriminating private thoughts and forsaking their oath by committing perjury." *Muniz*, 496 U.S. at 596 (quoting *Doe II*, 487 U.S. at 212). This being the case, "the definition of 'testimonial' evidence articulated in *Doe* must encompass all responses to questions that, if asked of a sworn suspect during a criminal trial, could place the suspect in the 'cruel trilemma.'" *Id.* at 597. As the Supreme Court reasoned, "[t]his conclusion is consistent with our recognition in *Doe* that '[t]he vast majority of verbal statements thus will be testimonial' because

'[t]here are very few instances in which a verbal statement, either oral or written, will not convey information or assert facts.'" *Id.* Thus, "[w]henever a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief, the suspect confronts the 'trilemma' of truth, falsity, or silence, and hence the response (whether based on truth or falsity) contains a testimonial component." *Id.* (footnote omitted).

To invoke the Fifth Amendment privilege against the forced provision of information, a defendant must show (1) the evidence is self-incriminating; (2) the evidence is compelled; and (3) the evidence is testimonial in nature. *Hubbell*, 530 U.S. at 34. Thus, the government may not force someone to provide an incriminating communication that is "testimonial" in nature. It is only this last requirement — whether the evidence sought to be compelled is testimonial — that is at issue in this appeal.

The United States Supreme Court has not rendered a decision directly addressing whether compelling a person to disclose a computer password is testimonial. In a series of foundational, but somewhat complex, cases, however, the high Court has discussed whether the act of production of documents may be testimonial for purposes of the Fifth Amendment.

In *Fisher*, the high Court examined the question of what acts of production were testimonial in nature. *Fisher* involved consolidated cases in which the Internal Revenue Service ("IRS") sought to obtain voluntarily-prepared documents the defendant taxpayers had given to their attorneys. The IRS issued summonses on the defendant taxpayers' attorneys to produce the documents

which included accountants' work papers, copies of the defendant taxpayers' returns, and copies of other reports and correspondence. The attorneys responded that producing the documents would violate their clients' rights against self-incrimination, after which the IRS brought an enforcement action.

Ultimately, the Supreme Court, after rejecting the attorneys' argument that the Fifth Amendment protected them from being compelled to produce the documents, determined that the Fifth Amendment privilege was applicable where defendant taxpayers were required to produce incriminating evidence, and that the act of producing even unprivileged evidence could have communicative aspects rendering it testimonial and entitled to Fifth Amendment protection. *Fisher*, 425 U.S. at 409-10. Under the facts in *Fisher*, the Court found that the government was not relying on the "truth-telling" of the defendant taxpayers to establish the existence of the documents, their access to them, or their authentication of them, as they had been produced by accountants, and not the defendant taxpayers themselves. *Id.* at 411. Thus, the Court concluded that the act of producing the subpoenaed documents did not involve self-incriminating testimony.

This analysis served as the basis of the foregone conclusion exception to the Fifth Amendment, discussed below. The Court offered that, because the existence, location, and authenticity of the documents sought was known to the government, the Fifth Amendment privilege was rendered inapplicable. The Court explained that "[t]he 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.* Thus, the Court reasoned that the defendant taxpayers' production of the documents was non-testimonial because the government knew of the existence of the documents, that the defendant taxpayers possessed the documents, and that the government could show their authenticity — not through the use of the defendant taxpayers' minds, but through the testimony of others. Thus, the Fifth Amendment privilege did not apply to the third-party production of documents requested. *Id.* at 414.

Almost a decade later, in *United States v. Doe*, 465 U.S. 605 (1984) ("*Doe I*"), the Court considered a Fifth Amendment challenge to a subpoena that did not seek specific, known files, but broad categories of general business records of a sole proprietorship. The Court found that, while the contents of the documents were not privileged, the act of producing the business documents could have testimonial aspects and an incriminating effect. The Court opined that the enforcement of the subpoena would compel the defendant to admit that the records existed, that they were in his possession, and that they were authentic, which was sufficient to establish a valid claim of privilege against self-incrimination. While concluding that, by producing the documents, the defendant would relieve the government of the need for authentication, the Court mentioned (although did not apply) the foregone conclusion analysis: "This is not to say that the Government was foreclosed from rebutting respondent's claim by producing evidence that possession, existence, and authentication were a 'foregone conclusion.' . . . In

this case, however, the Government failed to make such a showing." *Id.* at 614 n.13 (citation omitted).

In a subsequent, unrelated, decision in *Doe II*, the high Court considered the legality of an order compelling the target of a grand jury investigation to authorize foreign banks to disclose records of his accounts. 487 U.S. at 202. The defendant contended that compelling him to sign the bank consent form would provide the government with incriminating records that would otherwise be unavailable, as the court had no power to order foreign banks to produce records. *Id.* at 204. In rejecting this contention, the high Court indicated that "an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information." *Id.* at 210. The Court reasoned that the written authorization did not have testimonial significance, as it did not communicate any factual assertion, implicit or explicit, or convey any information to the government.

Importantly, for purposes of the issue before us, in response to a dissent by Justice John Paul Stevens, wherein he would have found the Fifth Amendment gave the defendant the right to refuse to sign the consent authorizing access to his bank accounts on the basis that he was compelled to use his mind as a witness against himself, the majority first agreed with the dissent by acknowledging that "[t]he expression of the contents of an individual's mind" is testimonial communication for purposes of the Fifth Amendment. *Id.* at 210 n.9. Thus, the Court was unanimous in its holding on this issue. The majority continued, however, that "[w]e simply disagree with the dissent's conclusion that the execution of the consent directive at issue

here forced petitioner to express the contents of his mind. *In our view, such compulsion is more like 'be[ing] forced to surrender a key to a strongbox containing incriminating documents' than it is like 'be[ing] compelled to reveal the combination to [petitioner's] wall safe.'*" *Id.* (quoting Stevens, J. dissenting, 487 U.S. at 219) (emphasis added). Thus, the Court emphasized a clear physical/mental distinction in the context of a foregone conclusion analysis.

Another decade later, the Court in *Hubbell* again spoke to testimonial evidence in the business record context. In that case, Webster Hubbell, as part of the "Whitewater" investigation by Independent Counsel Kenneth Starr during the presidency of Bill Clinton, had pleaded guilty to charges of mail fraud and tax evasion arising out of his billing practices. In the plea agreement, Hubbell promised to provide the Independent Counsel with "full, complete, accurate, and truthful information" about matters relating to the Whitewater investigation. *Hubbell*, 530 U.S. at 30. Later, while Hubbell was in prison, a grand jury investigating the activities of the Whitewater Development Corporation, issued a *subpoena* demanding from Hubbell the production of eleven categories of documents. *Id.* at 31. Hubbell invoked his Fifth Amendment privilege. The Independent Counsel then obtained an order from the federal district court directing Hubbell to comply with the subpoena and granting him immunity against the government's use and derivative use of the compelled testimony. Hubbell then delivered 13,120 pages of the specified documents, after which the grand jury returned an indictment against Hubbell for various wire fraud, mail fraud, and tax

crimes. In response, Hubbell asserted his right against self-incrimination and a violation of the immunity previously granted. The district court dismissed this new indictment, but the United States Court of Appeals for the District of Columbia Circuit reversed, and the Supreme Court granted *certiorari*.

Citing *Fisher*, the Supreme Court reiterated that "a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the privilege." *Id.* at 35-36. Accordingly, the simple fact that the documents contained incriminating evidence did not mean that Hubbell could avoid complying with the subpoena.

Importantly, however, the Court reaffirmed that the very act of producing documents in response to a subpoena may have a compelled testimonial aspect in and of itself: "The 'compelled testimony' that is relevant . . . is not to be found in the *contents* of the documents produced in response to the subpoena. It is, rather, the testimony inherent in the act of producing those documents." *Id.* at 40. (emphasis added.) Noting that in *Fisher*, the government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants, the *Hubbell* Court nevertheless found that the government had not shown it had prior knowledge of the existence or whereabouts of the documents produced by Hubbell. Moreover, in rejecting the government's assertion that its possession of the documents was the result of the physical act of producing the documents, the Court explained that it was

Hubbell's responses that had provided the government with this information, and that it was "unquestionably necessary for [Hubbell] to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena." *Id.* at 43. Indeed, in discussing the government's subpoena, which had required Hubbell to provide numerous responses to very broad requests, the Court, harkening back to the *Doe II* distinction, made clear that "[t]he assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." *Id.* at 43 (citation omitted).

The Court then considered whether the act of producing the records was sufficiently testimonial because the existence and possession of such records was a foregone conclusion. The Court held that "[w]hatever the scope of this 'foregone conclusion' rationale," it did not apply to overcome the testimonial aspects of Hubbell's production of documents because the government did not have prior knowledge of the existence or location of the documents. *Id.* at 44-45. Thus, the Court concluded that the Fifth Amendment privilege applied, and that Hubbell's act of production of the documents had testimonial aspects, at least regarding the existence and location of the documents, which was not overcome by being a foregone conclusion. *Id.* at 45.

Finally, the Supreme Court's decision in *Muniz* informs our analysis. *Muniz*, after failing field sobriety tests, was arrested for driving while intoxicated, and asked various questions when he was being booked. 496 U.S. at 585-86. Specifically, the defendant was asked, *inter alia*, for identifying

information such as his name, address, and date of birth, along with the date of his sixth birthday. The high Court considered the issue of whether the defendant's statements during the booking process were testimonial, and, thus, subject to the Fifth Amendment privilege against self-incrimination, which was implicated because the defendant had not been provided with *Miranda* warnings. *Id.* at 589-90. The Court held that descriptions by police of the defendant's speech as "slurred," although incriminating, were not testimonial, but akin to other physical characteristics that do not enjoy Fifth Amendment protection. *Id.* at 590-91. However, the substance of the defendant's answers, specifically involving his birthday, were held to be testimonial. The *Muniz* Court emphasized that the Fifth Amendment spares an accused from "having to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share this thoughts and beliefs with the Government." *Id.* at 595 (citation omitted). Moreover, the Court reasoned that when the defendant was asked about his birthday, he had to admit that he did not know, or answer untruthfully, raising the specter of the "cruel trilemma." *Id.* at 596. This, according to the Court, was entirely consistent with the Court's prior admonition that "[t]he vast majority of verbal statements thus will be testimonial" because they likely "convey information or assert facts." *Id.*, 496 U.S. at 597 (quoting *Doe II*, 487 U.S. at 213). Thus, the testimonial statements revealing the contents of the defendant's own mind disclosed consciousness of fact subject to the privilege.

From this foundational law noted above, we can distill certain guiding principles. First, the Supreme Court has made, and continues to make,

a distinction between physical production and testimonial production. As made clear by the Court, where the government compels a physical act, such production is not testimonial, and the privilege is not recognized. *See Holt; Doe II*. Second, an act of production, however, may be testimonial when the act expresses some explicit or implicit statement of fact that certain materials exist, are in the defendant's custody or control, or are authentic. *See Fisher; Hubbell*. The crux of whether an act of production is testimonial is whether the government compels the defendant to use the "contents of his own mind" in explicitly or implicitly communicating a fact. *See Doe II; Hubbell*. Third, and broadly speaking, the high Court has recognized that the vast majority of compelled oral statements of facts will be considered testimonial, as they convey information or assert facts. *See Muniz; Doe II*. This is consistent with the Court's deep concern regarding placing a suspect in the "cruel trilemma" of telling the truth, lying and perjuring himself, or refusing to answer and facing contempt and jail. *Id.* Indeed, the Court has unanimously concluded that "[t]he expression of the contents of an individual's mind" is testimonial communication for purposes of the Fifth Amendment. *Doe II*, 487 U.S. at 210 n.9.

Finally, and consistent with this historical repulsion of the prospect of compelling a defendant to reveal his or her mental impressions, we find it particularly revealing that, when addressing Justice Stevens's dissent in *Doe II*, the majority of the Court noted that compelling the defendant to sign the bank disclosure forms was more akin to "be[ing] forced to surrender a key to a strongbox containing incriminating documents" than it was to "be[ing] compelled to reveal the combination to [petitioner's]

wall safe." *Id.*, at 210 n.9. This is a critical distinction. Consistent with a physical/mental production dichotomy, in conveying the combination to a wall safe, versus surrendering a key to a strongbox, a person must use the "contents of [their] own mind." If one is protected from telling an inquisitor the combination to a wall safe, it is a short step to conclude that one is protected from telling an inquisitor the password to a computer.

Based upon these cases rendered by the United States Supreme Court regarding the scope of the Fifth Amendment, we conclude that compelling the disclosure of a password to a computer, that is, the act of production, is testimonial. Distilled to its essence, the revealing of a computer password is a verbal communication, not merely a physical act that would be nontestimonial in nature. There is no physical manifestation of a password, unlike a handwriting sample, blood draw, or a voice exemplar. As a passcode is necessarily memorized, one cannot reveal a passcode without revealing the contents of one's mind. Indeed, a password to a computer is, by its nature, intentionally personalized and so unique as to accomplish its intended purpose — keeping information contained therein confidential and insulated from discovery. Here, under United States Supreme Court precedent, we find that the Commonwealth is seeking the electronic equivalent to a combination to a wall safe — the passcode to unlock Appellant's computer. The Commonwealth is seeking the password, not as an end, but as a pathway to the files being withheld. As such, the compelled production of the computer's password demands the recall of the contents of Appellant's mind, and the act of production carries with it the

implied factual assertions that will be used to incriminate him. Thus, we hold that compelling Appellant to reveal a password to a computer is testimonial in nature.

Numerous other courts have come to similar conclusions. *See, e.g., In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) (holding “the decryption and production of the hard drives would require the use of the contents of Doe’s mind and could not be fairly characterized as a physical act that would be nontestimonial in nature,” thus Fifth Amendment protections were triggered); *United States v. Kirschner*, 823 F.Supp.2d 665 (E.D. Mich. 2010) (finding the government could not compel the defendant to reveal his password because this amounted to “testimony” from him which would “requir[e] him to divulge through his mental processes his password”).⁶

This, however, does not end our analysis. As noted above, the United States Supreme Court has found information, otherwise testimonial in nature, to be unprotected where the production of such information is a foregone conclusion. In essence, this judicial toleration of certain compelled testimony renders otherwise privileged testimonial communication non-testimonial. Specifically, under a foregone conclusion analysis, the Supreme Court

⁶ In this regard, we reject the Commonwealth’s seemingly newly-raised contention that there might be a slip of paper containing the password which would be covered by the trial court’s order, Commonwealth’s Brief at 1. There has been no suggestion in the proceedings in this matter that such a paper exists, and this case has proceeded under the assumption of an oral or written compulsion of Appellant to provide the password.

has reasoned that an act of production does not render communication testimonial where the facts conveyed already are known to the government such that the evidence sought "adds little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411. Thus, what is otherwise testimonial in nature is rendered non-testimonial, as the facts sought to be compelled are a foregone conclusion. As described above, for the exception to apply, the government must establish its knowledge of: (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence.

Based upon the United States Supreme Court's jurisprudence surveyed above, it becomes evident that the foregone conclusion gloss on a Fifth Amendment analysis constitutes an extremely limited exception to the Fifth Amendment privilege against self-incrimination. The Supreme Court has spoken to this exception on few occasions over the 40 years since its recognition in *Fisher*, and its application has been considered only in the compulsion of specific existing business or financial records. *See Doe I; Doe II; Hubbell*. Its circumscribed application is for good reason. First, the Fifth Amendment privilege is foundational. Any exception thereto must be necessarily limited in scope and nature. Moreover, business and financial records are a unique category of material that has been subject to compelled production and inspection by the government for over a century. *See, e.g., Shapiro v. United States*, 335 U.S. 1, 33 (1948). The high Court has never applied or considered the foregone conclusion exception beyond these types of documents. Indeed, it would be a significant expansion of the foregone conclusion rationale to

apply it to a defendant's compelled oral or written testimony. As stated by the Supreme Court, "[t]he essence of this basic constitutional principle is 'the requirement that the [s]tate which proposes to convict *and punish* an individual produce the evidence against him by the independent labor of its officers, not by the simple cruel expedient of forcing it from his own lips.'" *Estelle v. Smith*, 451 U.S. 454, 462 (1981) (emphasis original). Broadly circumventing this principle would undercut this foundational right.

The Court's decisions have been ambiguous concerning the breadth of the rationale as well as its value. See *Hubbell*, 530 U.S. at 44 ("Whatever the scope of this 'foregone conclusion' rationale. . ."); *Fisher*, 425 U.S. at 411 (finding that to succeed, the government must show that the sought after information is a "foregone conclusion" in that it "adds little or nothing to the sum total of the Government's information.") Thus, generally speaking, the exception to a large degree appears to be intentionally superfluous; hence, the accommodation to the government is of limited value. Accordingly, by definition, application of the foregone conclusion analysis in any given case will not be fatal to the government's prosecution.

Finally, the prohibition of application of the foregone conclusion rationale to areas of compulsion of one's mental processes would be entirely consistent with the Supreme Court decisions, surveyed above, which uniformly protect information arrived at as a result of using one's mind. To broadly read the foregone conclusion rationale otherwise would be to undercut these pronouncements by the high Court. See *Doe II*; *Hubbell*; *Muniz*. When comparing the modest value

of this exception to one's significant Fifth Amendment privilege against self-incrimination, we believe circumscribed application of the privilege is in order.

We acknowledge that, at times, constitutional privileges are an impediment to the Commonwealth. Requiring the Commonwealth to do the heavy lifting, indeed, to shoulder the entire load, in building and bringing a criminal case without a defendant's assistance may be inconvenient and even difficult; yet, to apply the foregone conclusion rationale in these circumstances would allow the exception to swallow the constitutional privilege. Nevertheless, this constitutional right is firmly grounded in the "realization that the privilege, while sometimes 'a shelter to the guilty,' is often 'a protection to the innocent.'" *Doe II*, 487 U.S. at 213. Moreover, there are serious questions about applying the foregone conclusion exception to information that manifests through the usage of one's mind. As expressed by the California Court of Appeals in a matter involving an order compelling the production of a weapon allegedly used in a crime: Implicit in the prosecution's position, and the court's order, is the argument that independent evidence establishes defendant's possession of the gun at the time of the offense and after. . . . The Commonwealth does not simply assert that the evidence to be gained by production is here inconsequential or non-incriminating; rather it says that the evidence is unworthy of Fifth Amendment protection because it merely enhances other persuasive evidence obtained without the defendant's help. *The Commonwealth's argument is indeed curious. It is as if we were asked to rule that a confession could be coerced from an accused as soon as the*

government announced (or was able to show) that [in] a future trial it could produce enough independent evidence to get past a motion for a directed verdict of acquittal.

Goldsmith v. Superior Court, 152 Cal. App. 3d 76, 87 n.12 (1984) (quotations and citations omitted) (emphasis added).

We appreciate the significant and ever-increasing difficulties faced by law enforcement in light of rapidly changing technology, including encryption, to obtain evidence. However, unlike the documentary requests under the foregone conclusion rationale, or demands for physical evidence such as blood, or handwriting or voice exemplars, information in one's mind to "unlock the safe" to potentially incriminating information does not easily fall within this exception.⁷

⁷ Because we are dealing with a motion to require an individual to recall and disclose a memorized password to a computer, in essence, revealing the contents of one's own mind, we need not address the related, but distinct, area involving biometric features like fingerprints, thumbprints, iris scanning, and facial recognition, or whether the foregone conclusion rationale would be appropriate in these circumstances. The dissent, however, makes much of the potential for inconsistent results in "future cases" involving these types of biometric passwords. Dissenting Opinion at 8-9. Yet, not only are these communications not before our Court, it is the United States Supreme Court that long ago has created the dichotomy between physical and mental communication. *See Holt*, 218 U.S. at 252-53 ("the prohibition of compelling a man in criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material."); *Doe II*, 487 U.S. at 210 n.9. (finding the expression "more like 'be[ing] forced to surrender a key to a strong box containing incriminating documents' than it is like be[ing] compelled to

Indeed, we conclude the compulsion of a password to a computer cannot fit within this exception.

Thus, we hold that the compelled recollection of Appellant's password is testimonial in nature, and, consequently, privileged under the Fifth Amendment to the United States Constitution. Furthermore, until the United States Supreme Court holds otherwise, we construe the foregone conclusion rationale to be one of limited application, and, consistent with its teachings in other decisions, believe the exception to be inapplicable to compel the disclosure of a defendant's password to assist the Commonwealth in gaining

reveal the combination to [petitioner's] wall safe.").

access to a computer.^{8 9 10}

⁸ After oral argument, we granted Appellant's Motion for Leave to File Post-Argument Submission and now grant the Commonwealth's Motion for Leave to File Response to Post-Argument Submission with respect to this issue. However, as we resolve this matter in favor of Appellant exclusively under the Fifth Amendment to the United States Constitution, we need not address his additional contention that the Pennsylvania Constitution provides greater protections than the federal charter.

⁹ Even if we were to find that the foregone conclusion exception could apply to the compulsion to reveal a computer password, we nevertheless would conclude that the Commonwealth has not satisfied the requirements of the exception in this matter. As noted above, for the compelled evidence to fall within the exception, the Commonwealth must establish: (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence.

As the Superior Court recounted below, there is a high probability that child pornography exists on Appellant's computer, as evidenced by: Appellant's IP address utilizing a peer-to-peer file sharing network to share videos depicting child pornography; the fact that the sole computer seized had hardwire Internet; and the fact that Appellant "implied as to the nefarious contents of the computer on numerous occasions." *Davis*, 176 A.3d at 876. However, for the exception to apply, the facts sought to be compelled must be already known to the Commonwealth. It is not merely access to the computer that the Commonwealth seeks to obtain through compelling Appellant to divulge his computer password, but all of the files on Appellant's computer. The password is merely a means to get to the computer's contents. While it is conceivable, and indeed, likely, that a single video containing child pornography (as previously viewed by the OAG agents) may be on the computer, the compelled revelation of the password could lead to a trove of a presently unknown number of files. Indeed, the record establishes that the entire hard drive of the computer was encrypted and "there was no data that could be read without opening the TrueCrypt

volume." N.T. Hearing, 1/14/16, at 46. Agent Cook could only confirm that there was "Windows on the computer and the TrueCrypt," and he had no knowledge of any specific files other than the operating system files. *Id.* at 50-51.

In sum, because the Commonwealth has failed to establish that its search is limited to the single previously identified file, and has not asserted that it is a foregone conclusion as to the existence of additional files that may be on the computer, which would be accessible to the Commonwealth upon Appellant's compelled disclosure of the password, we find the Commonwealth has not satisfied the foregone conclusion exception.

¹⁰ The dissent agrees that the information the Commonwealth seeks to compel is testimonial in nature. Dissenting Opinion at 2. The dissent, however, contends that, in these circumstances, governmentally forced testimony involving a computer password falls within the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination. Respectfully, the dissent's position is unpersuasive.

Initially, the dissent broadly dilutes the historic and contextual underpinnings of the application of the foregone conclusion exception, which, as noted above, constitutes an extremely narrow exception. Indeed, the high Court has found the exception to have been satisfied only one time in the over 40 years since it was created; moreover, the exception's provenance is exclusively in cases involving subpoenaed paper documents - never in the context of oral testimony. Thus, application of the foregone conclusion exception outside of this narrow context is dubious at best. For that reason, we will not apply the foregone conclusion exclusion in the absence express guidance from the high Court.

Furthermore, the dissent adopts a minority interpretation of that exception which focuses on the password itself, rather than on the underlying files. Yet, even employing this password-centric approach, the circumstances, *sub judice*, do not satisfy the foregone conclusion doctrine. As set forth above, and noted by the dissent, to satisfy the foregone

conclusion doctrine, the government must establish, *inter alia*, the authenticity of the evidence, *i.e.*, the password, with reasonable particularity. Of course, here, the Commonwealth cannot establish with reasonable particularity the authenticity of the password. Rather, authenticity may only be established after the information — the password — is turned over to the Commonwealth. The dissent is turning the authenticity requirement on its head, allowing the Commonwealth to satisfy its burden by, in essence, saying, “Turn over the facts we want, and we will tell you if it is authentic or not.” Of course, this is not how the exception works. Rather, the burden is on the Commonwealth to establish its independent knowledge of, *inter alia*, the authenticity of the documents or evidence sought, *before* that information is properly compelled over a defendant’s Fifth Amendment assertion of his or her right against self-incrimination. *Fisher*. Indeed, the dissent’s password-centric logic was recently rejected by the Third District Court of Appeal of Florida in *Pollard v. State*, 2019 WL 2528776 (Fla. Dist. Ct. App. June 20, 2019), where the court forcefully explained the logical shortcomings of this approach:

[The foregone conclusion exception’s] three-part test is tautological when applied to passwords because all password-protected cellphones have an “authentic” password, making the [*State v. Stahl*, 206 So.3d 124 (Fla. Dist. Ct. App. 2016)] test somewhat circular. In this regard, the court in *Stahl* said that “[i]f the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic. 206 So.3d at 136, which begs the question of whether sufficient evidence established that the passcode is authentic *before* it had been compelled and used successfully. The state must have sufficient proof of authenticity *before* it can compel the password’s production; simply because a compelled password unlocks a cellphone after the fact doesn’t make it authentic *ex ante*. To do otherwise is “like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox.” [citing *Hubbell*].

Pollard, 2019 WL 2528776 at *4.

Related thereto, and as noted above, the United States Supreme Court has limited the application of this narrow

For the above-stated reasons, we reverse the order of the Superior Court and remand the matter

exception to Fifth Amendment protections to contexts where the facts sought “add little or nothing to the sum total of the Government’s information.” *Fisher*, 425 U.S. at 411. Nothing could be farther from the case here, as the password which the Commonwealth seeks to compel could disclose a vast swath of files of which the Commonwealth, it appears, currently has no knowledge.

Finally, and directly related thereto, the dissent gives scant attention or significance to the Supreme Court’s consistent approach that revealing the contents of one’s mind is protected by the Fifth Amendment. This unmistakable overarching jurisprudential theme has been consistently applied in all of the high Court’s decisions in this area. *Doe II*, *Hubbell*, *Muniz*. Indeed, the dissent speaks volumes by reducing to a footnote, without analysis, its mention of the United States Supreme Court’s distinction between the production of documents and the forced compulsion of mental processes such as the combination to a safe, which, in the high Court’s view, plainly violates the Fifth Amendment. *Doe II*, *Hubbell*. Simply stated, there is no meaningful distinction between the government compelling a suspect to provide the combination to access a safe, and the government forcing one to disclose a password to access a computer. Here, it is unquestionably necessary for Appellant to make use of “the contents of his own mind” in providing the password. In essence, the dissent’s approach is effectively the same as compelling Appellant to affirm that, “I know the password, this is my computer, I have knowledge of the existence and location of incriminating files, and I have the capability to decrypt the files.” To accept the dissent’s position is to embrace a stance contrary to the foundational privilege against the probing of an individual’s mind to compel communication that is incriminating.

to the Superior Court, for remand to the trial court,
for proceedings consistent with our Opinion.
Jurisdiction relinquished.

Chief Justice Saylor and Justices Donohue and
Wecht join the opinion.
Justice Baer files a dissenting opinion in which
Justice Dougherty and Mundy join.

[J-42-2019]
[MO: Todd, J.]
IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

COMMONWEALTH OF PENNSYLVANIA,
Appellant

v.

JOSEPH J. DAVIS,
Appellee

No. 56 MAP 2018

Appeal From The Order Of The Superior Court Dated November 30, 2017 At No. 1243 MDA 2016, Affirming The Order Of The Court Of Common Pleas Of Luzerne County, Criminal Division, Dated June 30, 2016 Nos. CP-40-CR-291-2016 and CP-40-MD-11-2016.

ARGUED: May 14, 2019

DISSENTING OPINION

JUSTICE BAER DECIDED: November 20, 2019

I respectfully dissent from the majority's decision, which holds that the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination does not apply to the compelled disclosure of a computer password because the password manifests from one's mind. I further disagree with the majority's alternative

holding that if the foregone conclusion exception would apply under the circumstances presented, the Commonwealth failed to satisfy the requisites thereof because it did not establish that it had knowledge of the various files stored on Appellant's computer hard drive in addition to the single previously identified file that contained child pornography.

Preliminarily, I acknowledge that the issue presented in this appeal is one of first impression, with which courts across the nation have struggled. *See generally* Marjorie A. Shields, *Fifth Amendment Privilege Against Self-Incrimination as Applied to Compelled Disclosure of Password or Production of Otherwise Encrypted Electronically Stored Data*, 84 A.L.R. 6th 251 (2019)(compiling Fifth Amendment cases involving "compelled disclosure of an individual's password, means of decryption, or unencrypted copy of electronically stored data"). Upon review of the High Court's seminal decision in *Fisher v. United States*, 425 U.S. 391 (1976), which first recognized the foregone conclusion exception, and its progeny, I would hold that the foregone conclusion analysis applies to the compelled disclosure of a password to an electronic device, which the Commonwealth has seized pursuant to a warrant.

My analysis focuses on the compulsion order, which directed Appellant to "supply the Commonwealth with any and all passwords used to access" a specific desktop computer and hard drive seized from his residence. Trial Court Order, 6/30/2016. In my view, this order compels an act of production that has testimonial aspects

in that it conveys, as a factual matter, that Appellant has access to the particular computer seized by the Commonwealth pursuant to a warrant, and that he has possession and control over the password that will decrypt the encrypted files stored on that computer. As discussed in detail *infra*, because the Commonwealth was already aware of these facts based upon its own investigation and Appellant's candid discussion with government agents, the password falls within the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination, and may be constitutionally compelled. Notably, critical to my position is the recognition that this case does not involve a Fourth Amendment challenge based upon Appellant's privacy rights in his encrypted computer files but, rather, solely a challenge to the compelled disclosure of his password based upon his Fifth Amendment privilege against self-incrimination.

I. The Fifth Amendment As Applied To Acts of Production

As noted by the majority, the Fifth Amendment provides, in relevant part, that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend V. Courts have interpreted the privilege as protecting a citizen "from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature." *Pennsylvania v. Muniz*, 496 U.S. 582, 588-89 (1990) (citations omitted). The Fifth Amendment "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*, 425 U.S. at 408. 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).

In *Fisher*, the High Court explained that in addition to traditional testimony, acts of production may implicate the Fifth Amendment because the "act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced." 425 U.S. at 410. The Court explained that compliance with a request for evidence "tacitly concedes" the existence of the evidence, possession or control of the evidence by the individual, and the belief that the evidence is, in fact, the item requested by the government. *Id.* Whether the act of production has a testimonial aspect sufficient to warrant Fifth Amendment protection "depends on the facts and circumstances of particular cases or classes thereof." *Id.*

It is well established that some compelled acts have no testimonial aspects and, thus, no Fifth Amendment protection, as the acts do not require an accused to relate a factual assertion, disclose knowledge, or "speak his guilt." *Doe v. United States*, 487 U.S. 201, at 210-11 (1988). These include, for example, furnishing a blood sample, providing a voice or handwriting exemplar, or standing in a line-up. *Id.* (collecting cases). Other compelled acts, such as the production of certain subpoenaed documents, may

have a compelled testimonial aspect warranting Fifth Amendment protection where the government's demand is akin to a "detailed written interrogatory or a series of questions at a discovery deposition," characterized as a "fishing expedition." *United States v. Hubbell*, 530 U.S. 27, 36, 41-42 (2000).¹

Finding that an act of production has testimonial aspects, however, does not necessarily mean that the Fifth Amendment privilege precludes compulsion of the evidence sought. As the majority cogently observes, the United States Supreme Court has found that information, otherwise testimonial in nature, is unprotected where the production of such information is a foregone conclusion. Majority Opinion at 20. The foregone conclusion exception applies where the existence and location of the compelled evidence "adds little or nothing to the sum total of the government's information." *Fisher*, 425 U.S. at 410. The High Court in *Fisher* explained that a foregone conclusion exists where "[t]he question is not of testimony but of surrender." *Id.* at 411 (quoting *In re Harris*, 221 U.S. 274, 279 (1911)). Thus, as the majority recognizes, "what is otherwise testimonial in nature is rendered non-testimonial, as the facts

¹ In *Hubbell*, the Supreme Court held that the act of producing thousands of subpoenaed documents had testimonial aspects in that the act of production communicated information about the documents' existence, custody, and authenticity. The High Court concluded that, unlike in *Fisher*, the government had shown no prior knowledge of either the existence or whereabouts of the documents, thus, the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination did not apply.

sought to be compelled are a foregone conclusion.” Majority Opinion at 21.

In my opinion, the compulsion of Appellant’s password is an act of production, requiring him to produce a piece of evidence similar to the act of production requiring one to produce a business or financial document, as occurred in *Fisher*.² See Trial Court Order, 6/20/2016 (directing Appellant to “supply the Commonwealth with any and all passwords used to access the HP Envy 700 desktop computer with serial # MXX410000042C containing Seagate 2 TB hard drive with serial # Z4Z1AAAEFM”). An order compelling disclosure of the password, here a 64-character password, has testimonial attributes, not in the characters themselves, but in the conveyance of information establishing that the password exists, that Appellant has possession and control of the password, and that the password is authentic, as it will decrypt the encrypted computer files. The Commonwealth is not seeking the 64-character password as an investigative tool, as occurred in *Hubbell*, where the government compelled the disclosure of thousands of documents to engage in a fishing expedition to discover evidence of the defendant’s guilt. To the contrary, the Commonwealth already possesses evidence of Appellant’s guilt, which it set forth in an affidavit

² The summonses in *Fisher* directed the defendants’ attorneys to produce documents relating to the defendants’ tax returns in connection with an investigation into possible civil or criminal liability under federal income tax laws.

of probable cause to obtain a warrant to search Appellant's computer. Stated differently, the Commonwealth is not asking Appellant to "speak his guilt," but merely to allow the government to execute a warrant that it lawfully obtained.

Because I view the compulsion order as requiring the "surrender" of Appellant's password to decrypt his computer files, I would apply *Fisher's* act-of-production test. The majority declines to apply the foregone conclusion rationale to the compelled disclosure of Appellant's computer password, finding that to do so would constitute a "compulsion of one's mental processes" in violation of the Fifth Amendment. Majority Opinion at 22. There is appeal to this conclusion, as requiring Appellant to supply his password involves some mental effort in recalling the 64 characters used to encrypt the computer files.³ However, one would expend similar mental effort when engaging in virtually any other act of production, such as the disclosure of business or

³ I recognize that the majority's conclusion in this regard finds support in commentary found in federal cases, suggesting a constitutional distinction between the compelled surrender of a key and the compelled disclosure of a combination to a wall safe. For the reasons set forth herein, however, I do not find any such distinction dispositive in a case involving current day technology relating to the compelled disclosure of a password to encrypted digital information, where the Commonwealth has a warrant to search the digital container. Only the High Court can make the final determination in this regard for purposes of the Fifth Amendment, and the present case offers an attractive vehicle by which the Court could do so.

financial records, as the individual must retrieve the contents of his mind to recall the documents' location before disclosing them to the government. Under the majority's reasoning, the compelled production of documents would be tantamount to placing the defendant on the stand and requiring him to testify as to the location of the documents sought. The mere fact that Appellant is required to think in order to complete the act of production, in my view, does not immunize that act of production from the foregone conclusion rationale.

II. Application of the Foregone Conclusion Test

Having determined that the foregone conclusion rationale may potentially apply to cases involving the compelled disclosure of a computer password, significant questions arise regarding how to administer the three-part test. As observed by the majority, to satisfy the foregone conclusion exception to the Fifth Amendment privilege, "the government must establish its knowledge of: (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence." Majority Opinion at 21.

As an alternative holding, the majority opines that if the Court were to find that the foregone conclusion exception could apply to the compelled disclosure of a password, it would apply *Fisher's* act-of-production test to the computer files stored on Appellant's computer. *See* Majority Opinion at 25 n.9 (holding that "because the Commonwealth has failed to establish that its search is limited to the single previously identified file [containing child pornography], and has not

asserted that it is a foregone conclusion as to the existence of additional files that may be on the computer, which would be accessible to the Commonwealth upon Appellant's compelled disclosure of the password, we find the Commonwealth has not satisfied the foregone conclusion exception").

Respectfully, it is my position that the foregone conclusion exception as applied to the facts presented relates not to the computer files, but to the password itself. Appellant's computer files were not the subject of the compulsion order, which instead involved only the password that would act to decrypt those files. This change of focus is subtle, but its effect is significant. While the government's knowledge of the specific files contained on Appellant's computer hard drive would be central to any claim asserted pursuant to the Fourth Amendment, the same is not dispositive of the instant claim based upon the Fifth Amendment right against self-incrimination, which focuses upon whether the evidence compelled, here, the password, requires the defendant to provide incriminating, testimonial evidence. *See Doe v. United States (In re Grand Jury Subpoena)*, 383 F.3d 905, 910 (9th Cir. 2004) (providing that "it is the government's knowledge of the existence and possession of the actual documents [subpoenaed by the government], not the information contained therein, that is central to the foregone conclusion inquiry"). This Court should not alleviate concerns over the potential overbreadth of a digital search in violation of Fourth Amendment privacy concerns by invoking the Fifth

Amendment privilege against self-incrimination, which offers no privacy protection. The High Court in *Fisher* made this point clear by stating, “We cannot cut the Fifth Amendment loose from the moorings of its language, and make it serve as a general protector of privacy – a word not mentioned in its text and a concept directly addressed in the *Fourth Amendment*.” 425 U.S. at 401 (quoting *United States v. Nobles*, 422 U.S. 225, 233 n.7 (1975) (emphasis in original)).

Accordingly, I would align myself with those jurisdictions that examine the requisites of the foregone conclusion exception by focusing only on the compelled evidence itself, *i.e.*, the computer password, and not the decrypted files that the password would ultimately reveal. *See, e.g., United States v. Apple MacPro Computer*, 851 F.3d 238, 248 n.7 (3rd Cir. 2017) (“[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 device is ‘I, John Doe, know the password for these devices.’”); *State v. Johnson*, 576 S.W.3d 205, 277 (Mo. Ct. App. 2019) (holding that the focus of the foregone conclusion exception as applied to the compelled entering of one’s cell phone passcode is the extent of the government’s knowledge about the existence of the passcode, his possession and control of the phone’s passcode, and the passcode’s authenticity); *Commonwealth v. Gelfatt*, 11 N.E.3d 605, 615 (Mass. 2014) (holding that the compelled decryption of computer

files satisfied the elements of the foregone conclusion exception because the government already knew the implicit facts conveyed through the act of entering the encryption key, such as the defendant's ownership and control of the computers, knowledge of the encryption, and knowledge of the encryption key); *State v. Andrews*, 197 A.3d 200, 205 (N.J. Super. 2018) (holding that whether the government was aware of the possible contents of the defendant's cell phones was immaterial "because the order requires defendant to disclose the passcodes, not the contents of the phones unlocked by those passcodes").

III. Application to Future Cases

Finally, it is my belief that the majority's approach could render inconsistent results as the determination of whether there was a Fifth Amendment violation in compelled decryption cases could depend upon the type of password that the individual employed to protect his encrypted files. For example, according to the majority, if the accused used a multi-character password to encrypt computer files, as occurred here, and the government compelled the individual to supply the password, a Fifth Amendment violation would result because the password manifests through the use of one's mind. Majority Opinion at 23. However, if the individual employed a biometric password, such as facial recognition or a fingerprint, the majority's analysis would arguably lose its force. Under those circumstances, the individual is not using the contents of his mind but, rather, is performing a

compelled act of placing his finger or face in the appropriate position to decrypt the files. Additional questions arise when the act of compulsion is not the disclosure of the password itself, but the entry of the password into the computer. It is my position that all these examples constitute acts of production that would be subject to the foregone conclusion rationale in the appropriate case. The same legal analysis should apply to the underlying act of compelled decryption of digital information when the government has obtained a warrant to search the digital container. To hold to the contrary would create an entire class of evidence, encrypted computer files, that is impervious to governmental search. This could potentially alter the balance of power between governmental authorities and criminals, and render law enforcement incapable of accessing relevant evidence.

VI. Conclusion

Accordingly, I would hold that the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination applies to render non-testimonial Appellant's compelled act of producing the password to his encrypted, lawfully seized computer. As the majority observes, when government agents attempted to execute the search warrant, Appellant voluntarily informed them that he was the sole user of the computer, that he used hardwired Internet services that were password protected, that only he knew the password to decrypt his computer files, and that he would never disclose the password, as it would incriminate him.

In addition to Appellant's voluntary disclosure to government agents that he knew the password that would decrypt the files stored on the computer that the Commonwealth lawfully seized, there is ample circumstantial evidence demonstrating Appellant's knowledge of the password. Before seizing the computer, government agents conducted an investigation of the "eMule" peer-to-peer network to identify internet users sharing child pornography. Agents made a direct connection with a device that used a particular IP address over the eMule network, which agents subsequently linked to Appellant. Using this direct connection, agents downloaded one child pornography video file from Appellant's IP address. Affidavit of Probable Cause, 10/20/2015, at 7. Based on this download, the agents obtained the search warrant for Appellant's residence. *Id.* at 9.

Upon executing the search warrant, agents seized a single desktop computer, as that was the only device connected to Appellant's IP address. N.T., 1/14/2016, at 33. Forensic analysis revealed that Appellant's IP address had used the eMule file-sharing program on 23 dates from July 4, 2015, through October 19, 2015, to share files indicative of child pornography. Affidavit of Probable Cause, 10/20/2015, at 10-11; N.T., 1/14/2016, at 29. Agent Daniel Block explained that the government reached this conclusion based upon the "SHA value," which is essentially a "digital fingerprint" that corresponds with known SHA values of child pornography files. N.T., 1/14/2016, at 20. This evidence demonstrates that Appellant possessed the password to decrypt files on the computer

seized by the Commonwealth, as his own words established that he was the sole user of the computer and forensic analysis demonstrated that he was accessing the encrypted files on the days leading up to his arrest.

Under these circumstances, it was a foregone conclusion that the government knew that the password to decrypt the files existed, that Appellant had exclusive control over the password, and that the password was authentic.⁴ Accordingly, the testimonial aspects of the password disclosure "adds little or nothing to the sum total of the government's information." *Fisher*, 425 U.S. at 410. Thus, I would find that the compelled disclosure of Appellant's password does not violate his Fifth Amendment privilege against self-incrimination.

Justices Dougherty and Mundy join this dissenting opinion.

⁴ I would hold that the authenticity prong of the foregone conclusion exception requires the government to establish that the compelled information is what it purports to be, *i.e.*, a password that will decrypt the computer files on Appellant's hard drive. The Commonwealth may prove the authenticity of the password by Appellant's own voluntary statements. *See* Pa.R.E. 901(b) (providing that the requirement of authenticating an item of evidence may be satisfied by testimony of a witness with knowledge that an item is what it is claimed to be). Here, Appellant's voluntary statements establish that the password would decrypt the files on his hard drive; thus, I would conclude that the authenticity requirement has been satisfied.

[J-A20044/17]
[2017 PA Super 376]
IN THE SUPERIOR COURT OF PENNSYLVANIA
MIDDLE DISTRICT

COMMONWEALTH OF PENNSYLVANIA,
Appellee

v.

JOSEPH J. DAVIS,
Appellant

No. 1243 MDA 2016

Appeal From The Order Entered June
30, 2016, In The Court of Common
Pleas of Luzerne County Criminal
Division at Nos. CP-40-CR-291-2016
and CP-40-MD-11-2016.

Before: Gantman, P.J., Panella, J., and Ford
Elliott, P.J.E.

OPINION BY FORD ELLIOTT, P.J.E.

FILED NOVEMBER 30, 2017

Joseph J. Davis appeals from the
June 30, 2016 order granting the
Commonwealth's pre-trial motion to compel
appellant to provide the password that will
allow access to his lawfully-seized
encrypted computer. After careful review,
we affirm.

The relevant facts and procedural history of this case are as follows. On October 10, 2015, law enforcement officials executed a search warrant at appellant's residence after it was determined that a computer with an IP address subscribed to appellant utilized peer-to-peer file sharing network, eMule, to share videos depicting child pornography. During the course of the search, law enforcement officials seized a password-encrypted HP Envy 700 desktop computer. The Forensic Unit of the Pennsylvania Office of Attorney General ("POAG") was unable to examine the contents of this computer due to the "TrueCrypt" encryption program installed on it and appellant has refused to provide the password to investigating agents.

On December 17, 2015, the Commonwealth filed a pre-trial "Motion to Compel Defendant to Provide Password for Encryption Enabled Device." On January 14, 2016, the trial court conducted an evidentiary hearing on the Commonwealth's motion. The testimony adduced at this hearing was summarized by the trial court as follows:

TESTIMONY OF SPECIAL AGENT

[JUSTIN] LERI

On July 14, 2014, [POAG] Agent Leri was conducting an online investigation on the eDonkey2000¹ network for offenders sharing

¹ We note that the terms "eDonkey2000" and "eMule"

child pornography. On that date a computer was located that was sharing files believed to be sharing other files of child pornography. When the computer is located that is suspected of sharing these files, the IP address of that computer is recorded and one-to-one connection is made.

Agent Leri testified that the focus of the investigation was a device at IP address 98.235.69.242. This device had a 1-to-1 connection to the [POAG] as a suspect file, depicting child pornography. The agent was undercover in a peer to peer connection. Later that same day, the file from the suspect device was made available and downloaded through the direct connection to the law enforcement computer.

Special Agent Leri personally viewed the file identified as [boy+man][MB]NEW!! Man+Boy13Yo.mpg. He described it as a video, approximately twenty[-]six (26) minutes and fifty[-]four (54) seconds in length, depicting a young prepubescent boy. [Agent Leri's description of the contents of the video clearly established its extensive pornographic nature.] Officer Leri is certain that the video he watched came from [appellant's] computer. He attested that the law enforcement software is retrofitted for law enforcement and the

are used interchangeably throughout the transcript of the January 14, 2016 hearing to describe the peer-to-peer file sharing network. (See notes of testimony, 1/14/16 at 5.)

software logs in the activity. The retrofit allows for one-to-one connection only. According to Agent Leri, what this means is that law enforcement is directly connected to the subject's computer and only the suspect's computer.

The IP address was registered to Comcast Communication. After obtaining a court order directing Comcast Cable to release the subscriber information, [appellant] was identified as the subscriber. The [POAG] then obtained a search warrant for the listed address. The warrant was executed on September 9, 2014. The agent testified that [appellant] waived his *Miranda*² rights and admitted that he did his time for prior pornography arrests. He then refused to answer any questions.

SPECIAL AGENT [DANIEL] BLOCK

Agent Block testified that he is a special agent assigned to the Child Predator Section of the [POAG]. On October 4, 2015, an online investigation on the eMule network for offenders sharing child pornography was being conducted. The internet provider was determined to be Comcast and an administrative subpoena was issued which revealed the billing information belonged to the billing address. The focus of the investigation was IP address 174.59.168.185, port 6350. The file was downloaded and viewed.

² *Miranda v. Arizona*, 384 U.S. 436 (1966).

[Agent Block's testimony indicated that the video in question depicted a prepubescent boy between the ages of nine and eleven years old and clearly described the extensive pornographic content of the video.]

Special Agent Block indicated that the Log File provides the date and time of the download and the client user's hashtag which is unique to [appellant]. Again Comcast Cable identified, through a Court Order, the subscriber was [appellant]. A search warrant was prepared and executed at [appellant's] home. Agent Block executed a search warrant on [appellant] at his residence and gave [appellant] his *Miranda* warnings. While he was at [appellant's] home, [appellant] spoke to Agent Block telling him he resided alone at the apartment since 2006 and that he was hardwired internet services which are password protected. According to Agent Block, [appellant] stated he uses this service so no one else can steal his Wi-Fi. There was only one computer in the house and that [no]one else uses it.

[Appellant] told Agent Block that he was previously arrested for child pornography related crimes. His reasoning was that it is legal in other countries like Japan and [the] Czech Republic, and he does not know why it is illegal here. He stated "what people do in the privacy of their own homes is their own business. It's all over the Internet. I don't know why you guys care so much about stuff when people are getting killed and those videos are being posted."

Agent Block testified that [appellant's] IP address was used during downloads on the following dates: July 4, 2015; July 5, 2015; July 6, 2015; July 19, 2015; July 20, 2015, August 2, 2015; August 9, 2015; August 16, 2015; September 5, 2015; September 12, 2015; September 13, 2015; September 14, 2015; September 19, 2015; September 20, 2015; September 23, 2015; September 26, 2015; September 27, 2015; October 4, 2015; October 5, 2015; October 10, 2015; October 17, 2015; October 18, 2015 and October 19, 2015.

While transporting [appellant] to his arraignment, [appellant] spoke about gay, X-rated movies that he enjoyed watching. He stated that he liked 10, 11, 12 & 13 year olds, referring to them as, "[a] perfectly ripe apple." Agent Block requested that [appellant] give him his password. [Appellant] replied that it is sixty-four (64) characters and "Why would I give that to you?" "We both know what's on there. It's only going to hurt me. No f[***]ing way I'm going to give it to you."

TESTIMONY OF AGENT BRADEN COOK

After [appellant] was arrested and the various devices were confiscated, Agent Cook previewed the computer. The hard drive was found to contain a "TrueCrypt" encrypted protected password setup with TrueCrypt 7.1 aBootloader. The user must input the password for the TrueCrypt encrypted volume in order to boot the system into the Operating System.

Agent Cook stated that [appellant] told him that he could not remember the password. Moreover [appellant] stated that although the hard drive is encrypted, Agent Cook knows what is on the hard drive. Trial court opinion, 6/30/16 at 3-7 (citations to notes of testimony omitted).

On February 11, 2016, appellant was charged with two counts of distribution of child pornography and two counts of criminal use of a communication facility.³ Thereafter, on June 30, 2016, the trial court granted the Commonwealth's motion to compel and directed appellant to supply the Commonwealth with the password used to access his computer within 30 days. (Trial court order, 6/30/16; certified record at no. 4.) In reaching this decision, the trial court reasoned that appellant's argument under the Fifth Amendment right against self-incrimination is meritless because "[his] act of [providing the password in question] loses its testimonial character because the information is a for[e]gone conclusion." (See trial court opinion, 6/30/16 at 13 (internal quotation marks omitted).)

On July 15, 2016, appellant filed a motion to immediately appeal the trial court's June 30, 2016 order. On July 19, 2016, the trial court granted appellant's motion by amending its June 30, 2016 order to include the 42 Pa.C.S.A. § 702(b)

³ 18 Pa.C.S.A. §§ 6312(c) and 7512(a), respectively.

language.⁴ On July 21, 2016, appellant filed a timely notice of appeal, pursuant to Pa.R.A.P. 313(b).⁵ The trial court ordered appellant to file a concise statement of errors complained of on appeal, in accordance with Pa.R.A.P. 1925(b), on July 29, 2016. Thereafter, on August 8, 2016, this court entered an order directing appellant to show cause why the appeal should not be quashed. On August 17, 2016, appellant filed a timely Rule 1925(b) statement. Appellant then filed a response to our show-cause order on August 22, 2016. On September 27, 2016, the trial court filed a one-page Rule 1925(a) opinion

⁴ 42 Pa.C.S.A. 702(b) provides as follows: **(b) Interlocutory appeals by permission.** -- When a court or other government unit, in making an interlocutory order in a matter in which its final order would be within the jurisdiction of an appellate court, shall be of the opinion that such order involves a controlling question of law as to which there is substantial ground for difference of opinion and that an immediate appeal from the order may materially advance the ultimate termination of the matter, it shall so state in such order. The appellate court may thereupon, in its discretion, permit an appeal to be taken from such interlocutory order. 42 Pa.C.S.A. § 702(b).

⁵ We note that appellant should have filed a petition for permission to appeal, since the trial court granted his petition to amend the underlying June 30, 2016 order. See Pa.R.A.P. 1311(b) (stating, “[p]ermission to appeal from an interlocutory order containing the statement prescribed by 42 Pa.C.S. § 702(b) may be sought by filing a petition for permission to appeal with the prothonotary of the appellate court within 30 days after entry of such order in the lower court”).

that incorporated by reference its prior June 30, 2016 opinion. On October 5, 2016, this court entered an order denying appellant's July 15, 2016 motion, which we treated as a petition for permission to appeal, discharging the show-cause order, and referring the issue of appealability to the merits panel.

Appellant raises the following issue for our review:

Whether [a]ppellant should be compelled to provide his encrypted digital password despite the rights and protection provided by the Fifth Amendment to the United States Constitution and Article 1, Section 9 of the Pennsylvania Constitution?

Appellant's brief at 4.

Before we may entertain the merits of appellant's underlying claim, we must first determine whether this court has jurisdiction to consider the appeal under Pa.R.A.P.313. Although the Commonwealth has not raised a question regarding our jurisdiction over the trial court's interlocutory order, we may nevertheless raise the issue of jurisdiction *sua sponte*. *Commonwealth v. Shearer*, 882 A.2d 462, 465 n.4 (Pa. 2005).

It is well settled that, generally, appeals may be taken

only from final orders; however, the collateral order doctrine permits an appeal as of right from a non-final order which meets the criteria established in Pa.R.A.P. 313(b). Pa.R.A.P. 313 is jurisdictional in nature and provides that "[a] collateral order is an order [1] separable from and collateral to the main cause of action where [2] the right involved is too important to be denied review and [3] the question presented is such that if review is postponed until final judgment in the case, the claim will be irreparably lost." Pa.R.A.P. 313(b). Thus, if a non-final order satisfies each of the requirements articulated in Pa.R.A.P. 313(b), it is immediately appealable.

Commonwealth v. Blystone, 119 A.3d 306, 312 (Pa. 2015) (case citations omitted; quotation marks in original).

Upon review, we conclude that the order in question satisfies each of the three requirements articulated in Rule 313(b). Specifically, the trial court's June 30, 2016 order is clearly "separable from and collateral to the main cause of action" because the issue of whether the act of compelling appellant to provide his computer's password violates his Fifth Amendment right against self-

incrimination can be addressed without consideration of appellant's underlying guilt. See Pa.R.A.P. 313(b). Second, courts in this Commonwealth have continually recognized that the Fifth Amendment right against self-incrimination is the type of privilege that is deeply rooted in public policy and "too important to be denied review." *Id.*; see, e.g., *Veloric v. Doe*, 123 A.3d 781, 786 (Pa.Super. 2015) (stating that, "the privilege against self-incrimination is protected under both the United States and Pennsylvania Constitutions ... and is so engrained in our nation that it constitutes a right deeply rooted in public policy[]"(citations and internal quotation marks omitted)); *Ben v. Schwartz*, 729 A.2d 547, 552 (Pa. 1999) (holding that orders overruling claims of privilege and requiring disclosures were immediately appealable under Rule 313(b)). Lastly, we agree with appellant that if review of this issue is postponed and appellant is compelled to provide a password granting the Commonwealth access to potentially incriminating files on his computer, his claim will be irreparably lost. See *Commonwealth v. Harris*, 32 A.3d 243, 249 (Pa. 2011) (concluding that appeal after final judgment is not an adequate vehicle for vindicating a claim of privilege and reaffirming the court's position in *Ben* "that once material has been disclosed, any privilege is effectively destroyed[]"). Accordingly, we deem the order in question immediately appealable

and proceed to address the merits of appellant's claim.

The question of whether compelling an individual to provide a digital password is testimonial in nature, thereby triggering the protections afforded by the Fifth Amendment right against self-incrimination, and is an issue of first impression for this court. As this issue involves a pure question of law, "our standard of review is *de novo* and our scope of review is plenary." *Commonwealth v. 1997 Chevrolet & Contents Seized from Young*, 160 A.3d 153, 171 (Pa. 2017) (citation omitted).

The Fifth Amendment provides "no person shall be compelled in any criminal case to be a witness against himself[.]" U.S. Const. amend. V. This prohibition not only permits an individual to refuse to testify against himself when he is a defendant but also privileges him not to answer official questions put to him in any other proceeding, civil or criminal, formal or informal, where the answers might incriminate him in future criminal proceedings.

Commonwealth v. Cooley, 118 A.3d 370, 375 (Pa. 2015) (case citations and some internal quotation marks omitted). "To qualify for the Fifth Amendment privilege,

a communication must be testimonial, incriminating and compelled." *Commonwealth v. Reed*, 19 A.3d 1163, 1167 (Pa.Super. 2011) (citation omitted), *appeal denied*, 30 A.3d 1193 (Pa. 2011).⁶

Although not binding on this court, the Supreme Judicial Court of Massachusetts examined the Fifth Amendment implications of compelling an individual to produce a password key for an encrypted computer and its relation to the "forgone conclusion" doctrine in *Commonwealth v. Gelfatt*, 11 N.E.3d 605 (2014). The *Gelfatt* court explained that,

[t]he "foregone conclusion" exception to the Fifth Amendment privilege against self-incrimination provides that an act of production does not involve testimonial communication where the facts conveyed already are known to the government, such that the individual "adds little or nothing to the sum total of the Government's information." For the exception to apply, the government must establish its knowledge of (1) the existence of the evidence

⁶ We note that our supreme court has recognized that Article I, § 9 of the Pennsylvania Constitution "affords no greater protections against self-incrimination than the Fifth Amendment to the United States Constitution." *Commonwealth v. Knoble*, 42 A.3d 976, 979 n.2 (Pa. 2012) (citation omitted).

demanded; (2) the possession or control of that evidence by the defendant; and (3) the authenticity of the evidence.

Id. at 614, citing *Fisher v. United States*, 425 U.S. 391, 410-413 (1976) (quotation marks in original; remaining citations omitted).

More recently, in *United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017), the Third Circuit Court of Appeals explained that in order for the foregone conclusion exception to apply, the Commonwealth "must be able to describe with reasonable particularity the documents or evidence it seeks to compel." *Id.* at 247, citing *United States v. Bright*, 596 F.3d 683, 692 (9th Cir. 2010).

Additionally, in *State v. Stahl*, 206 So.3d 124 (Fla. Dist. Ct. App. 2016), the Second District Court of Appeals of Florida addressed a similar issue in the context of a motion to compel a defendant charged with video voyeurism to produce the passcode for his iPhone. The *Stahl* court held that requiring a defendant to produce his passcode did not compel him to communicate information that had testimonial significance. *Id.* at 135. The *Stahl* court reasoned as follows:

To know whether providing the passcode implies testimony that is a foregone conclusion, the

relevant question is whether the State has established that it knows with reasonable particularity that the passcode exists, is within the accused's possession or control, and is authentic.

The State established that the phone could not be searched without entry of a passcode. A passcode therefore must exist. It also established, with reasonable particularity based upon cellphone carrier records and Stahl's identification of the phone and the corresponding phone number, that the phone was Stahl's and therefore the passcode would be in Stahl's possession. That leaves only authenticity. And as has been seen, the act of production and foregone conclusion doctrines cannot be seamlessly applied to passcodes and decryption keys. If the doctrines are to continue to be applied to passcodes, decryption keys, and the like, we must recognize that the technology is self-authenticating no other means of authentication may exist. If the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic.

Id. at 136 (citations omitted). With these principles in mind, we turn to the issue presented.

Appellant contends that the act of compelling him to disclose the password in question is tantamount to his testifying to the existence and location of potentially incriminating computer files, and that contrary to the trial court's reasoning, it is not a "foregone conclusion" that the computer in question contains child pornography because the Commonwealth conceded it does not actually know what exact files are on the computer. (Appellant's brief at 7-8.) We disagree.

As noted, the United States Supreme Court has long recognized that the Fifth Amendment right against self-incrimination is not violated when the information communicated to the government by way of a compelled act of production is a foregone conclusion. See *Fisher*, 425 U.S. at 409. Instantly, the record reflects that appellant's act of disclosing the password at issue would not communicate facts of a testimonial nature to the Commonwealth beyond that which he has already acknowledged to investigating agents.

Specifically, the testimony at the January 14, 2016 hearing established that the Commonwealth "knows with reasonable particularity that the passcode exists, is

within the accused's possession or control, and is authentic." See *Stahl*, 206 So.3d at 136 (emphasis added). First, the Commonwealth clearly established that the computer in question could not be searched without entry of a password. The computer seized from appellant's residence was encrypted with "TrueCrypt" software that required a 64-character password to bypass. (Notes of testimony, 1/14/16 at 26, 30, 42.) Second, the Commonwealth clearly established that the computer belonged to appellant and the password was in his possession. Appellant acknowledged to both Agent Leri and Agent Block that he is the sole user of the computer and the only individual who knows the password in question. (*Id.* at 11, 26-28.) As noted, appellant repeatedly refused to disclose said password, admitting to Agent Block that "we both know what is on [the computer]" and stating "[i]t's only going to hurt me." (*Id.* at 30.) Additionally, appellant informed Agent Leri that giving him the password "would be like ... putting a gun to his head and pulling the trigger" and that "he would die in jail before he could ever remember the password." (*Id.* at 36, 37.) Third, we agree with the court in *Stahl* that "technology is self-authenticating." *Stahl*, 206 So.3d at 136. Namely, if appellant's encrypted computer is accessible once its password has been entered, it is clearly authentic.

Moreover, we recognize that multiple jurisdictions have recognized that the

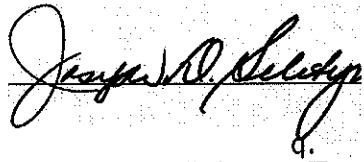
government's knowledge of the encrypted documents or evidence that it seeks to compel need not be exact. *See Securities and Exchange Commission v. Huang*, 2015 WL 5611644, at *3 (E.D. Pa. 2015) (stating, "the Government need not identify exactly the underlying documents it seeks[.]" (citation and internal quotation marks omitted)); *Stahl*, 206 So.3d at 135 (stating, "the State need not have perfect knowledge of the requested evidence[.]" (citation and internal quotation marks omitted)).

Herein, the record reflects that there is a high probability that child pornography exists on said computer, given the fact that the POAG's investigation determined that a computer with an IP address subscribed to appellant utilized a peer-to-peer file sharing network, eMule, approximately 25 times in 2015 to share videos depicting child pornography (notes of testimony, 1/14/16 at 5-8, 19-24, 28-29); the sole computer seized from appellant's residence had hard-wired internet that was inaccessible via a WiFi connection and contained a Windows-based version of the eMule software (see *id.* at 7, 12, 26); and as noted, appellant implied as to the nefarious contents of the computer on numerous occasions (see *id.* at 30, 36-37).

Based on the forgoing, we agree with the trial court that appellant's act of providing the password in question is not testimonial in nature and his Fifth Amendment right against self-incrimination

would not be violated. Accordingly, we discern no error on the part of the trial court in granting the Commonwealth's pre-trial motion to compel appellant to provide the password that will allow access to his lawfully seized encrypted computer.

Order affirmed.
Judgement Entered.

A handwritten signature in black ink, appearing to read "Joseph D. Seletyn". The signature is written in a cursive style with a large initial "J".

Joseph D. Seletyn, Esq.
Prothonotary
Date: 11/30/2017

**IN THE COURT OF COMMON PLEAS
OF LUZERNE COUNTY**

COMMONWEALTH OF : CRIMINAL DIVISION
PENNSYLVANIA, :
 :
 V. :
JOSEPH J. DAVIS : NO: 11 MD 2016
 : NO: 291 OF 2016

OPINION

This matter comes before the Court on the Commonwealth's Motion to Compel Defendant to Provide Password for Encryption Enabled Device. After a hearing, and consideration of the briefs filed by the respective parties, the matter is now ripe for determination.

FACTUAL AND PROCEDURAL HISTORY

On February 11, 2016, the Commonwealth filed an Information alleging that the Defendant, Joseph J. Davis (hereinafter the "Defendant" or Mr. Davis), committed the following offenses:

Count 1
Sexual Abuse of Children
(Distribution of Child Pornography)
(Video Depicting Indecent Contact)
18 Pa.C.S. Section 6312(c)
Second Degree Felony

Count2
Sexual Abuse of Children
(Distribution of Child Pornography)
(Video Depicting Indecent Contact)
18 Pa.C.S. Section 6312(c)

Second Degree Felony

Count 3

Criminal Use of A

Communication Facility

18 Pa.C.S. Section 7512 (a)

Third Degree Felony

Count 4

Criminal Use of A

Communication Facility

18 Pa.C.S. Section 7512(a)

Third Degree Felony

Specifically, the Commonwealth alleges that on October 4, 2015, a computer utilizing peer-to-peer file sharing was identified as sharing videos that depicted child pornography. According to the Commonwealth, the computer that was sharing the child pornography files utilized IP address 174.59.168.185, which was determined to be subscribed to Mr. Davis, located at 2 Bertram Court, Apartment 12, Edwardsville, Pennsylvania 18704-2548.

Subsequently, investigating law enforcement made a direct connection to the IP address 174.59.168.185. As a result, one video file depicting child pornography was downloaded from that IP address. Thereafter, Defendant was arrested on October 10, 2015, and a search warrant was executed at his residence. After the execution of the search warrant, law enforcement located an HP Envy 700 desktop computer, plugged directly with a "hard wired" internet access.

Members of the Pennsylvania Office of Attorney General Forensic Unit are unable to analyze the computer because it is "TrueCrypt" encrypted, which was acknowledged by the Defendant. Indeed, the Defendant stated that TrueCrypt is on his computer, that he is the sole user of the computer, and that he is the only one who knows the password. To date, Mr. Davis refuses to provide the password to the investigating agents. As a result, the Commonwealth has filed the Motion before the Court.

At the hearing on the Motion to Compel, the Commonwealth presented three witnesses: Special Agent Justin Leri, Pennsylvania Office of Attorney General Child Predator Section; Special Agent Daniel Block, Pennsylvania Office of Attorney General Child Predator Section; and Agent Braden Cook, Pennsylvania Office of Attorney Computer Forensic Section. The Court will address their individual testimony.

TESTIMONY OF SPECIAL AGENT LERI

On July 14, 2014, Agent Leri was conducting an online investigation on the *eDonkey 2000* network for offenders sharing child pornography. On that date a computer was located that was sharing files believed to be sharing other files of child pornography. When the computer is located that is suspected of sharing these files, the IP address of that computer is recorded and one-to-one connection is made.

Agent Leri testified that the focus of the investigation was a device at IP address 98.235.69.242. This device had a 1-to-1 connection to

the Attorney General as a suspect file, depicting child pornography. The agent was undercover in a peer to peer connection. Later that same day, the file from the suspect device was made available and downloaded through the direct connection to the Jaw enforcement computer.

Special Agent Leri personally viewed the file identified as [boy+man] [MB]NEWIIMan & Boy 13Yo.mpg. He described it as a video, approximately twenty six (26) minutes and fifty four (54) seconds in length, depicting a young prepubescent boy. In the video, the boy is laying on what appears to be a couch when an adult male removes his clothes and begins masturbating the boy who is then naked. The adult male then removes his own clothes and the boy begins masturbating the adult male. The next scene shows the young boy lying nude on his side with the adult male lubricating his own penis. The adult male then performs anal sex on the boy. Officer Leri is certain that the video he watched came from Mr. Davis' computer. He attested that the law enforcement software is retrofitted for law enforcement and the software logs in the activity. The retrofit allows for one-to-one connection only. According to Agent Leri, what this means is that law enforcement is directly connected to the subject's computer and only the suspect's computer.

The IP address was registered to Comcast Communication. After obtaining a court order directing Comcast Cable to release the subscriber information, Joseph Davis was identified as the subscriber. The Attorney General's Office then obtained a search warrant for the listed address. The warrant was executed on September 9, 2014.

The agent testified that the Defendant waived his Miranda rights and admitted that he did his time for prior pornography arrests. He then refused to answer any questions.

SPECIAL AGENT BLOCK

Agent Block testified that he is a special agent assigned to the Child Predator Section of the Attorney General's Office. On October 4, 2015, an online investigation on the eMule network for offenders sharing child pornography was being conducted. The internet provider was determined to be Comcast and an administrative subpoena was issued which revealed the billing information belonged to the billing address. The focus of the investigation was IP address 174.59.168.185, port 6350. The file was downloaded and viewed.

Special Agent Block viewed the video named "Peto Boy Love" and described the video as follows. After a numeric countdown, it begins with a prepubescent Chinese boy who is between nine (9) and eleven (11) years old walking into a bedroom, who then proceeds to strip. The child, who is naked, then walks into the bathroom and into the tub. He gets out of the tub, dries off, and the video transitions to the child lying naked in the bed with a naked adult male.

The video then transitions to showing the child in a seated position on top of the adult male with the adult male's penis in the child's anus. The child changes his position and is straddling the adult with his back to the camera. The adult male again penetrates the boy in his anus with the adult male's penis. The video then shows the boy lying on his

back with his legs pushed back and the adult male penetrating the boy with his penis. The child is crying and seems to be in pain. The child rolls over and is given a plastic object to bite on with a tear visible on the child's face. The child is next on his stomach with the adult male penetrating his anus with his penis. The video ends with the adult male's penis in the child's mouth. The child appears to be between nine (9) and eleven (11) years old.

Special Agent Block indicated that the Log File provides the date and time of the download and the client users hashtag which is unique to the Defendant. Again Comcast Cable identified, through a Court Order, the subscriber was Joseph Davis. A search warrant was prepared and executed at the Defendant's home. Agent Block executed a search warrant on the defendant at his residence and gave the defendant his Miranda warnings. While he was at the Defendant's home Mr. Davis spoke to Agent Block telling him he resided alone at the apartment since 2006 and that he was hardwired internet services which are password protected. According to Agent Block, the Defendant stated he uses this service so no one else can steal his Wi-Fi. There was only one computer in the house and that one else uses it.

Mr. Davis told Agent Block that he was previously arrested for child pornography related crimes. His reasoning was that it is legal in other countries like Japan and Czech Republic, and he does not know why it is illegal here. He stated "what people do in the privacy of their own homes is their own business. It's all over the internet. I don't know why you guys care so much about stuff when people

are getting killed and those videos are being posted." (N.T. January 14, 2016, p.28, Ins. 9-11).

Agent Block testified that the Defendant's IP address was used during downloads on the following dates: July 4, 2015; July 5, 2015; July 6, 2015; July 19, 2015; July 20, 2015, August 2, 2015; August 9, 2015; August 16, 2015; September 5, 2015; September 12, 2015; September 13, 2015; September 14, 2015; September 19, 2015; September 20, 2015; September 23, 2015; September 26, 2015; September 27, 2015; October 4, 2015; October 5, 2015; October 10, 2015; October 17, 2015; October 18, 2015 and October 19, 2015.

While transporting the Defendant to his arraignment, Mr. Davis spoke about gay, X-rated movies that he enjoyed watching. He stated that he liked 10, 11, 12 & 13 year olds, referring to them as, "[a] perfectly ripe apple." (N.T. pg. 30, Ins. 1-3).

Agent Block requested that Defendant give him his password. Mr. Davis replied that it is sixty-four (64) characters and "Why would I give that to you?" "We both know what's on there. It's only going to hurt me. No fucking way I'm going to give it to you." (N.T. pg. 30, Ins. 16-18).

TESTIMONY OF AGENT BRADEN COOK

After the Defendant was arrested and the various devices were confiscated, Agent Cook previewed the computer. The hard drive was found to contain a "True Crypt" encrypted protected password setup with TrueCrypt 7.1aBootloader. The user must input the password for the TrueCrypt

encrypted volume in order to boot the system into the Operating System.

Agent Cook stated that the Defendant told him that he could not remember the password. Moreover the Defendant state that although the hard drive is encrypted, Agent Cook knows what is on the hard drive.

QUESTION AT ISSUE

Whether the Defendant can be compelled to provide his encrypted digital password despite the rights and protections provided by the Fifth Amendment to the United States Constitution and Article 1 Section 9 of the Pennsylvania Constitution?

LAW

The pivotal question is whether the encryption is testimonial in nature which then triggers protection of the Fifth Amendment.

The Fifth Amendment of the United States Constitution, a cornerstone of fundamental liberties, provides that "[n]o persons ...shall be compelled in any criminal case to be a witness against himself". See *Couch v. United States*, 409 U.S. 322, 328, 9 S.Ct. 611, 3 L.Ed.2d 548 (1973). The availability of the Fifth Amendment privilege does not turn upon the type of proceeding in which its protection is invoked, but upon the nature of the statement or admission and the exposure which it invites. *Commonwealth v. Brown*, 26 A.3d 485, 493-94 (Pa. Super. 2016). The focus of any Fifth Amendment claim must be based on the nature of the compelled statement in relation to an existing or potential future criminal proceeding. "The privilege

extends not only to the disclosure of facts which would in themselves establish guilty, but also to any fact which might constitute an essential link in a chain of evidence by which guilty can be established." *Commonwealth v. Saranchak*, 866 A.2d 292, 303 (Pa. 2005).

It is clear that the decryption and production are compelled and incriminatory. The issue is not whether the drivers are testimonial but rather whether the act of production may have some testimonial quality sufficient to trigger the Fifth Amendment Protection when the production explicitly or implicitly conveys some statement of fact. *Fisher v. United States*, 425 U.S. 391, 6 S.Ct. 1569, 48 L.Ed. 39 (1976).

Fisher concerned an individual who refused to produce subpoenaed documents based on their Fifth Amendment privileges. In *Fisher*, a taxpayer forwarded tax records prepared by his accountants to his attorneys. The Internal Revenue Services subpoenaed the attorneys to produce the documents. The Court held that the Fifth Amendment protects an individual from giving compelled and self-incriminating testimony, not from disclosing private papers. In reaching this result, the Court examined whether the contents of the records were "compelled" and whether producing those records amounted to incriminating testimony. The *Fisher* Court found that the preparation of the records was voluntary and had not been compelled. Thus it held that the Fifth Amendment did not protect the documents' contents from disclosure. However, the *Fisher* court made a further inquiry and examined the act of producing the records. In doing so, the

court found that act of production was compelled, yet the production was not testimony. "The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing of significance to the sum total of the Government's information by conceding that he has the papers." *Id.* at 409.

The touchstone of whether an act of production is testimonial is whether the government compels the individual to us "the contents of his own mind" too explicitly or implicitly communicate some statement of fact. *Curcio v. United States*, 354 U.S. 118 (1957).

The Commonwealth makes two arguments: (1) that the Defendant's act of decryption would not communicate facts of a testimonial nature to the government beyond what the Defendant already has admitted to investigators; or, in the alternative, (2) that the decryption falls under the "foregone conclusion" exception to the Fifth Amendment privilege against self-incrimination. The "foregone conclusion" exception provides that an act of production does not involve testimonial communication where the facts conveyed already are known to the government, such that the individual "adds little or nothing to the sum total of the government's information". *Fisher, supra*.

In *Fisher*, the court found that the production was not testimonial because the government had knowledge of each fact that had the potential of being testimonial. In order to successfully establish the foregoing conclusion exception, the Commonwealth must establish its knowledge of (1)

the existence of the evidence, (2) the possession or control of that evidence by the defendant, and (3) the authenticity of evidence. *Id.*, at 410-413; *United States v. Bright*, 596 F.3d 683, 692 (9th Cir. 2010).

Technology has out run the law and there are no Pennsylvania cases on point as to this particular issue. The laws, however, must be applied as they exist. Therefore, we turn to our sister-states and to federal courts that have addressed a similar issue for guidance.

In *Commonwealth v. Gelfatt*, 468 Mass. 512 (Mass. 2014), the Supreme Court of Massachusetts reversed the trial court's decision denying the government's motion to compel defendant to privately enter an encryption key into computers seized from the defendant. The facts in *Gelfatt*, are as follows.

Beginning in 2009, the defendant orchestrated a scheme to acquire for himself funds that were intended to be used to pay off home mortgage loans. He had numerous computers, laptops, and a tablets. The Commonwealth maintained that the encryption software on the computers is virtually impossible to circumvent. The defendant also informed investigators that "everything is encrypted and no one is going to get to it." *Id.* In order to decrypt the information, he would have to "start the program." The Commonwealth argued that the information was essential to the discovery of "materials" or "significant" evidence relating to the defendant's purported criminal conduct. The trial court refused to compel the Defendant to enter an encryption key.

On appeal, the Supreme Court of Massachusetts determined that the defendant's act of entering an encryption key in the computers seized by the Commonwealth would appear, at first blush, to be testimonial communication that triggers Fifth Amendment protection. However, that court ultimately concluded that the defendant's act of production loses its testimonial character because the information is a "foregone conclusion."

In Re Subpoena Duces Tecum, 670 F.3d 1335 (11th Cir. 2012), the Court of appeals held that a subpoenaed individual's acts of decrypting and producing for the grand jury the contents of hard drives seized during the course of a child pornography investigation was sufficiently testimonial to trigger Fifth Amendment protection; since the act was not merely physical but would require the use of the individual's mind and would be tantamount to testimony by an individual of his knowledge of the existence and location of potentially incriminating files, of his possession, control, and access to the encrypted portions of the trial, and his capacity to decrypt the files, and the purported testimony was not a "foregone conclusion", as nothing in the record revealed that the government knew whether any files actually existed in the location of the files on the hard drives or that the government knew with reasonable particularity that the individual was even capable of accessing the encrypted portion of the drives.

Such is not in the case at bar. In the case herein, the testimony established that (1) the HP Envy 700 desktop computer located in Defendant's

residence was hard-wired internet access only; (2) the Defendant admitted to the agents that the computer has TrueCrypt encryption, which he is the sole user of that computer and he is the only individual who knows the password; (3) that Defendant admitted to Agent that "we both know what's on there" and that he stated he "will die in prison before giving up the password;" and, (4) that the Commonwealth knows with a reasonable degree of certainty that there is child pornography files on the computer seized from the Defendant's residence and that the Defendant utilized a Windows based version of eMule on this computer.

Again in *United States v. Hubbell*, 530 U.S. 27 (2000), the government did not satisfy the "foregone conclusion" exception where no showing of prior knowledge of the existence or whereabouts of documents ultimately produced by respondent to subpoena. In *Hubbell*, the defendant was prosecuted for mail fraud and tax evasion *Hubbell* from *Fisher, supra*, holding that defendant did not have to produce the subpoenaed documents. In doing so, the court reasoned that the government had no preexisting knowledge of the documents produced in response to the subpoena. Rather, the Court reasoned that to require production of the documents would also require the defendant "to make extensive use of the contents of his own mind in identifying the hundreds of documents responsive to the requests in the subpoenas. In the court's view, compliance with the subpoena was testimonial because the subpoena was vague to an extent that compliance required the Defendant to take "mental steps." Those mental steps, rather than the content of the documents themselves, triggered the

privilege. *Hubbell, supra.*, at 40. In *Fisher*, unlike *Hubbell*, the government knew exactly what documents it sought to be produced, knew that they were in the possession of the attorney, and knew that they were prepared by an accountant. Ultimately, the cases do not demand that the government identify exactly the documents the government seeks, but does require some specificity in the request—categorical requests for document the government anticipates are likely to exist simply will not suffice. *Hubbell, supra.* That is precisely what the Commonwealth has shown in the case at bar.

Defendant argues that revealing the password is testimonial in nature and could be incriminating. All that law enforcement has are two (2) videos and they do not know what is on the computer. Therefore, the “foregone conclusion” argument fails.

Whereas, the Commonwealth argues that the act of revealing the password is not giving the Commonwealth anything new, it is simply an act that allows the Commonwealth to retrieve what is already know to them.

In the case at bar it is clear that the Commonwealth has prior knowledge of the existence as well as the whereabouts of the documents. Therefore, the Defendant’s act of production loses its testimonial character because the information is a “foregone conclusion.” Therefore, the Commonwealth’s Motion to Compel Defendant to Provide Password for Encryption Enabled Device is **GRANTED.**

IN THE COURT OF COMMON PLEAS
OF LUZERNE COUNTY

COMMONWEALTH OF :
PENNSYLVANIA : CRIMINAL DIVISION
:
v. : NO: .11 MD 2016
: NO. 291 of 2016
JOSEPH J. DAVIS :

ORDER

AND NOW, this 30th day of June, 2016, upon consideration of the Commonwealth's Motion to Compel Defendant to Provide Password for Encryption Enabled Device, and supporting documents filed by the parties and after a hearing held on January 14, 2016, wherein all parties were present, IT IS HEREBY ORDERED AND DECREED, that the Defendant supply the Commonwealth with any and all passwords used to access the HP Envy 700 desktop computer with serial #MXX410000042C containing Seagate 2 TB hard Drive with serial # ZAZ1AAAEFM or within thirty (30) days of this Order.

The Clerk of Court is directed to enter this Order of Record and to mail a copy of this Order to all counsel of record or, if unrepresented, to each party pursuant to PaR.Crim.P. 114.

BY THE COURT:

/S/
POLACHECK GARTLEY, J.

Copies:

Rebecca Elo, Esquire

Office of Attorney General

1000 Madison Avenue, Suite 310

Norristown, PA 19403

Mark A Singer, Esquire/Luzerne County Public Defender's Office

Court Administration