

**IN THE SUPREME COURT OF PENNSYLVANIA
EASTERN DISTRICT**

NO. , M.D. Allocatur Docket 2018

COMMONWEALTH OF PENNSYLVANIA,

Respondent,

v.

JOSEPH J. DAVIS,

Petitioner

PETITION FOR ALLOWANCE OF APPEAL

Petition for Allowance of Appeal from Judgment of Superior Court
(Docket No. 1243 MDA 2016), Filed November 30, 2017 Affirming a
Judgment of Contempt Entered on June 30, 2016 at Nos. CP-40-0000291-2016,
CP-40-MD0000011-2016 in the Court of Common Pleas, Luzerne County

Witold J. Walczak
American Civil Liberties Union
Of Pennsylvania
247 Fort Pitt Boulevard
Pittsburgh, PA 15222
412-681-7864

Peter Goldberger (No. 22364)
Law Office of Peter Goldberger
50 Rittenhouse Place
Ardmore, PA 19003
610-649-8200

Robert E. Welsh (No. 28143)
Catherine M. Recker (No. 56813)
Welsh & Recker, P.C.
Suite 2903
2000 Market Street
Philadelphia, PA 19103
215-972-6430

Attorneys for Petitioner

TABLE OF CONTENTS

Table of Authorities..... ii

Statement of Jurisdiction.....1

Opinions Below and Order in Question.....2

Question Presented for Review.....3

Statement of the Case.....4

Reasons for Allowance of Appeal.....7

 A. The Holding of the Superior Court Conflicts with a Holding of the United States Supreme Court on the Same Legal Question.....7

 B. The Question is One of Such Substantial Importance as to Require Prompt and Definitive Resolution by the Pennsylvania Supreme Court.....8

Conclusion.....24

Appendices

 Appendix A—Docket Sheet of Superior Court re Denial of Petition for Reargument

 Appendix B—Order of the Trial Court

 Appendix C—Opinion of the Trial Court Pursuant to Pa.R.A.Pro 1925

 Appendix D—Opinion and Order of the Superior Court

Proof of Service.....25

TABLE OF AUTHORITIES

In re Boucher (Boucher II), No. 06-mj-91,
2009 WL 424718 (D. Vt.2009).....21

Commonwealth v. Edmunds, 586 A.2d 887 (1991).....16

Commonwealth v. Gelfgatt, 11N. E.3d 605, 615 (Mass. 2014).21

Commonwealth v. Knoble, 615 Pa. 285, 42 A.3d 976 (2012).15

Commonwealth v. Muniz, 377 Pa.Super. 382 (1988),
allocatur denied, 522 Pa. 575
(1989).....12

Commonwealth v. Swinehart, 541 Pa. 500, 664 A. 2d 957 (1995).....13, 16

Curcio v. United States, 354 U.S. 118 (1957).....11, 13

Doe v. United States, 487 U.S. 201(1988) (*Doe II*).....12, 13

Fisher v. United States, 425 U.S. 391 (1976).....7, 8,9

Pennsylvania v. Muniz, 496 U.S. 582 (1990).....11, 13

Riley v. California, __ U.S. __, 134 S.Ct. 2473 (2014).....19

<i>Securities and Exchange Commission v. Huang</i> , 2015 WL 561644 (E.D.Pa. 2015).....	22-23
<i>State v. Stahl</i> , 206 So.3d 124 (Fla. App.2016).....	21, 22
<i>State v. Trant</i> , No. 15-2389, 2015 WL Me. Super. LEXIS 272(2015).....	21
<i>United States v. Apple MacPro Computer</i> , 851 F.3d 238(3d Cir. 2017).....	21
<i>United States v. Doe</i> , 465 U.S. 605 (1984)(Doe I).....	9
<i>United States v. Friscosu</i> , 841 F.Supp.2d 1232 (D.Col. 2012).....	22
<i>United States v. Hubbell</i> , 530 U.S. 27 (2000).....	9
<i>United States v. Leon</i> , 468 U.S. 897(1984).....	16

STATEMENT OF JURISDICTION

This Court's jurisdiction is invoked under 42 Pa.C.S. § 724. The judgment of the Superior Court was entered on November 30, 2017. A timely application for reargument was filed on December 7, 2017. The Superior Court denied the application for reargument on February 5, 2018. App. A-5. This petition is filed within 30 days of the denial of the application for reargument. Pa.R.App.P. 1113.

The underlying order in this matter was entered on June 30, 2016, granting the Commonwealth's motion to compel the petitioner—the defendant in the underlying criminal case—to supply the Commonwealth with the password for his computer.¹ App. B. The petitioner/defendant filed a timely notice of appeal on July 15, 2016, invoking collateral order jurisdiction under Pa.R.App.P. 313. On September 7, 2016, the trial court entered its opinion under Pa.R.A.P. 1925. Appendix C. On October 5, 2016, the Superior Court referred the matter of appellate jurisdiction to the merits panel. The merits panel held that the underlying order was immediately appealable as a collateral order under Pa.R.App.P. 313. App. D-8.

¹ The petitioner/defendant initially pursued an appeal by permission under 42 Pa.C.S. § 702(b) by motion filed on July 15, 2016, which motion was granted by the Court of Common Pleas on July 19, 2016. His notice of appeal, filed July 15, 2015 was a change in theory, invoking collateral order jurisdiction under Rule 313.

OPINIONS BELOW AND ORDER IN QUESTION

The Opinion and Order of the Superior Court dated November 30, 2017 (Gantman, P.J., Panella, J. and Ford Elliot, P.J.E.) and designated J.A20044/17, are attached to this petition as Appendix D. The opinion is reported at *Commonwealth v. Davis*, 2017 Pa. Super. 376, 176 A.3d 869 (2017), 2017 WL 5896465.

The order and opinion of the Court of Common Plea are attached attached as Appendix B and C, respectively.

The final order of the Court of Common Pleas for Luzerne County (Tina Polacheck Gartley, J.) which is the subject of this petition is as follows:

The Order of the Superior Court that is the subject of this petition states as follows:

Order affirmed,
Judgment Entered.

Joseph D. Seletyn, Esq.,
Prothonotary
Date: 11/30/17

App. D-15.

QUESTION PRESENTED FOR REVIEW

May the defendant 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, section 9, of the Pennsylvania Constitution?

STATEMENT OF THE CASE

On October 10, 2015, law enforcement officials executed a search warrant at the petitioner's home, seizing a computer which had been identified as having been used to share child pornography through a certain peer-to-peer file sharing network. During the search, the authorities seized a password-encrypted HP Envy 700 desktop computer which is the subject of this proceeding.

On December 17, 2005, the Commonwealth filed a motion to compel the defendant to provide the password to the computer.

On February 11, 2016, Mr. Davis was charged with two counts of distribution of child pornography and two counts of criminal use of a communications facility.

An evidentiary hearing on Commonwealth's motion to compel disclosure of the password was convened on January 14, 2016, during which testimony enforcement officers was adduced.

The testimony may be summarized as follows. First, special agent Justin Leri testified that, based upon his investigation, he traced certain offending child pornography from a file sharing source to Mr. Davis's computer. Agent Leri further testified that Mr. Davis was the subscriber to the IP address assigned to the subject computer and that Mr. Davis, after waiving his rights, admitted that he had previously served time for an offense involving child pornography.

Second, Agent Daniel Block testified he was able to trace certain child pornography to appellant's computer. Agent Block also testified that Mr. Davis admitted that he was previously arrested for child pornography and that he defended the use of child pornography, pointing out that it is legal in other countries. Agent Block identified various dates on which Mr. Davis' computer was used to download child pornography. Agent Block testified that, while he transported Mr. Davis to his arraignment, Mr. Davis spoke about how much he enjoyed pornography involving prepubescent children and, referring to his password, said, "Why would I give that to you. We both know what's on there. It's only going to hurt me. No f*** way I'm going to give it to you."

Finally, Agent Braden Cook testified that he examined the computer and determined that it contained a "TrueCrypt" encryption-protected password installation that required the use of a password to access the computer. Agent Cook testified that Mr. Davis said he could not remember the password but that Agent Cook already knew what was on the computer.

On June 30, 2016, the trial court granted the prosecution's motion to compel the disclosure of the password to the computer within 30 days. The trial court reasoned that Mr. Davis could not invoke the Fifth Amendment to avoid disclosure of the password, because the act of providing the password was no longer

testimonial in character in light of the fact that “the information is a foregone conclusion.”

Mr. Davis filed a motion to immediately appeal the trial court’s order to disclose the password which was granted. See discussion of appellate jurisdiction above. The Superior Court affirmed. This petition follows.

REASONS FOR ALLOWING THE APPEAL

A. The Holding of the Superior Court Conflicts with Holdings of the United States Supreme Court and of the Pennsylvania Supreme Court on the Same Legal Question

1. Conflict with Holdings of the United States Supreme Court

Whatever the vitality of the “foregone conclusion” rule in its original context of document production, its expansion to computer passwords is unwarranted. Extension beyond its narrow origin conflicts in the context of computer passwords with authority of the United States Supreme Court that centers Fifth Amendment protections on compelled disclosures of the contents of one’s mind.

The “foregone conclusion” aspect of Fifth Amendment doctrine originates in *Fisher v. United States*, 425 U.S. 391, 410–11 (1976), where the Court considered whether the compelled disclosure of certain documents was sufficiently “testimonial” in nature to be protected under the Fifth Amendment.² Specifically, the Court addressed the government’s ability to compel attorneys for taxpayers to produce their clients’ accountants’ work papers then in the attorneys’ possession. The Court held that, because the work papers had been retrieved from the

² If a communication is not deemed “testimonial,” then under this analysis it does not compel the subject “to be a witness” against himself.

accountants and provided to counsel by their taxpayer clients, counsel could not be compelled to produce documents provided by their clients because of the attorney-client privilege. But, the Court reasoned, counsel had no greater rights to withhold production of the work papers than their clients possessed under the Fifth Amendment. Accordingly, for purposes of its analysis, the Court then considered the somewhat hypothetical question of whether the clients could invoke the privilege if they personally possessed the work papers.

The Court noted that the Fifth Amendment may be invoked in the face of compelled actions of a testimonial or communicative nature that carry a substantial risk of incrimination. The Court recognized that the production of documents involves at least an implicit representation that the documents exist and that taxpayer possesses them. But the “existence and location of the papers [were] a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government’s information by conceding that he in fact has the papers.” *Id.* at 411. No precedent was cited for the existence of a “foregone conclusion” notion in Fifth Amendment jurisprudence. There is nothing surprising about this “foregone conclusion” in the peculiar setting of the *Fisher* case, because the Court assumed that the taxpayer possessed the work papers for the hypothetical determination of whether he or she could invoke the Fifth Amendment. The Court expressed doubt that implicitly admitting to possession of the papers rises to the level of

“testimony” protected under the Fifth Amendment, because the work papers belonged to the accountant and were prepared by him, and were of the usual kind used by accountants rendering tax return preparation services. *Id.* at 411. Even if the production of records compiled by a third party had “some minimal testimonial significance,” seeking accounting assistance is not illegal and thus the production of the work papers did not carry “any realistic threat of incrimination to the taxpayer.” *Id.* at 414. While compulsion was clearly present, the taxpayer could not invoke the privilege because the act of production was insufficiently testimonial or communicative and carried insufficient threat of incrimination.

The Court has commented on the “foregone conclusion” rule on only two occasions in the four decades since *Fisher*. First, in *United States v. Doe*, 465 U.S. 605 (1984), the Court upheld the right of a sole proprietor of a large business operation to invoke the Fifth Amendment against the compelled production of business records, but noted that the government was not foreclosed from trying to defeat the invocation of the privilege if it could prove that the possession, existence and authentication of the records were “a foregone conclusion.” *Id.* at ___ n. 13. Later, in *United States v. Hubbell*, 530 U.S. 27 (2000), the Court rejected the government’s attempt to rely on the rule, noting that, “[w]hatever the scope of this ‘foregone conclusion’ rationale,” the facts of the case fell outside of it. *Id.* at 44. Thus, *Hubbell* does not overrule *Fisher* on the foregone conclusion “rationale,” but

it is far from a ringing endorsement of its expansion beyond its narrow – and to a great extent, assumed – facts.

Applying *Fisher* to computer passwords, as did the Superior Court in this case, stretches its holding far beyond its legal underpinnings, justification and rationale. In *Fisher*, the taxpayer would be compelled to implicitly acknowledge possession of routine documents prepared by a third-party professional, documents which could and normally would be legally possessed. Any testimonial or communicative features of the act of production were slight and merely implicit.

That the taxpayer may have taken possession of the documents at some point after their preparation is not remotely incriminating without a more sinister context and in any event, the work papers would, in a typical criminal prosecution, be addressed in testimony by the accountants and thus the act of production indeed has little or no realistic impact on the criminal proceeding.

Compelled production of a computer password in this case differs entirely, in all material respects. The underlying files on the computer in this case are *prima facie* contraband of the most serious nature and the accumulation of the images that reside on the computer were not prepared by a third-party but, on this record, appear to consist of files downloaded and presumably saved by the user of the computer (perhaps in folders or another organizational system designed and labeled by him). Moreover, the password here is not written down (much less

shared with a third party) or saved electronically, but rather memorized. The user's apparently exclusive knowledge of the password to a computer on which sexually explicit images of children reside is incriminating in the extreme.

The lower court's analysis of the testimonial element of the act of disclosing the password is utterly inconsistent with holdings of the United States Supreme Court, decisions that center the Fifth Amendment's protections, not on the contents of papers or other items, but on the "contents of one's mind." The United States Supreme Court has long held that, notwithstanding that certain acts may be compelled, a subject may not be compelled to disclose what is in his or her own mind. For example, in *Curcio v. United States*, 354 U.S. 118 (1957), the Court held that, while the records custodian of a labor union could be compelled to produce records of the union, he could not be compelled over the invocation of the Fifth Amendment to explain the whereabouts of records not produced pursuant to subpoena. "He cannot be compelled," the Court held, "to condemn himself by his own oral testimony." *Id.* at 124.

The Fifth Amendment's protection against compelled disclosure of one's mind finds fuller flower in the Supreme Court's more recent decision in *Pennsylvania v. Muniz*, 496 U.S. 582 (1990). There, the Court held that a defendant under investigation for drunk driving could be compelled to perform sobriety tests, such as counting from one to nine, but he could not be compelled to

answer the question, “Do you know what was the date of your sixth birthday?”

The difference was that the former was non-testimonial while the latter required

“testimonial response.” The distinction followed from the rule that the Fifth

Amendment privilege spares an accused from “having to share his thoughts and

beliefs with the Government.” *Id.* at 592. The Court further explained that the

Fifth Amendment protects both “verbal and nonverbal conduct.” *Id.* at 592 n. 9.³

Obviously, the police did not lack means of determining Muniz’s birthdate; the test

was of his ability to remember and recount. Yet because the substance of the

compelled disclosure was of the content of his mind, it fell within Fifth

Amendment protection. At its core, the Fifth Amendment protects against

compelled disclosure of “the actor’s communications of his thoughts to another.”

Id.

In *Doe v. United States*, 487 U.S. 201(1988) (*Doe II*), discussed in *Muniz*,

the Court also addressed the distinction between a non-testimonial act that may be

compelled and a related testimonial act that may not be compelled. In *Doe II*, the

issue before the Court was whether a person could be compelled to execute a

consent or authorization to disclose bank records otherwise subject to secrecy. The

³ Notably, the Superior Court of Pennsylvania’s decision in *Muniz* was consistent with the United States Supreme Court’s analysis, both courts reasoning that compelled disclosure of a memorized fact—a birthday—was a violation of the Fifth Amendment. See *Commonwealth v. Muniz*, 377 Pa.Super. 382 (1988), *allocatur denied*, 522 Pa. 575 (1989).

Court traced the development of Supreme Court decisions that distinguished non-testimonial acts such as the production of a blood sample, handwriting or voice exemplars and the like from acts that “disclose the contents of [one’s] mind”, to “disclose any knowledge [one] might have.” *Id.* at 211. Because the authorization in question made no representation of fact, “sparing the accused from having to reveal directly or indirectly, his knowledge of facts relating him the offense,” the act of executing the authorization had no testimonial component and could be compelled. *Id.*

Curcio, Muniz and *Doe II* stand for the proposition that, while a subject may be compelled to perform certain acts, such as the production of records of a collective entity, performance of a sobriety test that includes oral responses and even signing an authorization to disclose bank records, there is clear and bright line drawn to protect that which is in the subject’s mind. In *Muniz*, the defendant could not be compelled to disclose the date on which he turned six years old because the date of his birth was a fact held in his mind (and the fact that he could or could not, at that moment, recall and/or calculate it had incriminating implications). In *Doe II*, the subject was subject to compulsion to execute the authorization only because the language of the form was “carefully drafted not to make reference to a specific account but only to speak in the hypothetical” and did not include an

acknowledgement that the accounts even existed at the financial institution in question. 487 U.S. at 215.

These cases reduce to a simply stated and easily applied principle: a subject may not be compelled over the invocation of the privilege to disclose a fact held in his memory. This principle has been articulated and repeated over a period of more than fifty years in various contexts and forms the very basis determining what is “testimonial” and thus protected by the Fifth Amendment.

It is this principle that limits the application of the “foregone conclusion” notion to the narrow context of production of records prepared by a third-party from information voluntarily disclosed to that third-party by the defendant. The Supreme Court of the United States has never taken it farther, and this Court should not permit the lower courts of this Commonwealth to do so. Described in other words, the “foregone conclusion” rule (even if it may be called a “rule”) may permit the compelled implicit assertion that certain records exist but it may not be applied to compel a subject to reach into his mind and disclose a fact seemingly as innocuous as the dated he turned six years old, let alone a powerfully incriminating password.

2. Conflicts with Holdings of this Court

The lower court noted in footnote 6 that this Court has recognized that Article I, § 9 of the Pennsylvania Constitution “affords no greater protections

against self-incrimination that the Fifth Amendment to the United States Constitution.” 176 A.3d n.6, *quoting Commonwealth v. Knoble*, 615 Pa. 285, 42 A.3d 976, 979 n. 2(2012). Indeed, decisions of this Court have so spoken but have done so in connection with specific issues of constitutional interpretation.⁴ This Court has not addressed the “foregone conclusion” rule or whether our state constitution provides the same protection as the United States Constitution in this respect. It does a disservice to say that our state constitution should be construed in accordance with federal case law as to all provisions and issues. This Court has repeatedly stated that it has an independent responsibility to construe the Constitution of our Commonwealth which in some cases is broader in its protections than the United States Constitution.

This Court undertakes its own examination of provisions of the Pennsylvania Constitution that may be similar to provisions of the United States Constitution:

Here in Pennsylvania, we have stated with increasing frequency that it is both important and necessary that we undertake an independent

⁴ For example, in *Commonwealth of Pennsylvania Department of Environmental Protection v. Marra*, 527 Pa. 526, 594 A.2d 646 (1991), in a case dealing with the production of chemicals, this Court held that the protections under the state constitution are “conterminous” with those under the Fifth Amendment. Yet, in *Commonwealth v. Swinehart*, 541 Pa. 500, 664 A. 2d 957 (1995), a case concerning derivative use of immunized testimony, this Court considered but was not bound by federal interpretations of the Fifth Amendment in its interpretation state constitution’s protections against self-incrimination.

analysis of the Pennsylvania Constitution, each time a provision of that fundamental document implicated. Although we may accord weight to federal decisions where they “are found to be logically persuasive and well reasoned, paying due regard to precedent and the policies underlying specific constitutional guarantees,” we are free to reject conclusions of the United States Supreme Court so long as we remain faithful to the minimum guarantees established by the United States Constitution.

Commonwealth v. Swinehart, 541 Pa. 500, 664 A. 2d 957 (1995), quoting

Commonwealth v. Edmunds, 586 A.2d 887 (1991).⁵

In *Edmunds*, this Court “set forth certain factors to be briefed and analyzed by litigants in each case implicating a provision of the Pennsylvania Constitution

.... As a general rule [when addressing the meaning of a provision of the Pennsylvania Constitution related to a similar provision of the United States Constitution] it is important that the litigants brief and analyze at least the following four factors:

- 1) The text of the Pennsylvania constitutional provision;
- 2) History of the provision, including Pennsylvania case-law;
- 3) Related case-law from other states;
- 4) Policy considerations, including unique issues of state and local concern, and applicability within modern Pennsylvania jurisprudence.

Id. at 390.

⁵ In *Edmunds*, this Court considered but rejected the good faith exception to the warrant requirement established in federal law in *United States v. Leon*, 468 U.S. 897(1984), doing so on the basis of the Pennsylvania constitution.

But, the Court added, “an examination of related federal precedent may be useful as part of the state constitutional analysis not as binding authority.” Adding, “it is essential that courts in Pennsylvania undertake an independent analysis under the Pennsylvania Constitution.” *Id.* at 390–91.

The text of Article I, Section 9, which is not identical to the self-incrimination clause of the Fifth Amendment, states that a person “cannot be compelled to give evidence against himself.” The compelled disclosure of a password, which is surely “evidence,” is a violation of the plain language of the provision. Section 9 does not refer to “be[ing] a witness” and thus need not be interpreted with the same focus on what is “testimonial.” There is nothing in our history or in Pennsylvania case law that recognizes the “foregone conclusion” rule in any context and there is no apparent analogue in our laws. Finally, policy considerations strongly support protection against compelled disclosure in this case, because the idea of a “foregone conclusion” admits to no limit and is impermissibly based on the notion that a person’s rights are dependent on what the prosecution “knows.”

The Court should therefore grant the appeal in this case to explore whether Article I, section 9, of the Pennsylvania Constitution independently forbids compulsion of self-incriminating evidence, even if the federal courts might deem

the existence of the information a “foregone conclusion.” Upon such review, the Court should reject that doctrine as a matter of state constitutional law.

B. The Question Is One of Such Substantial Importance as to Require Prompt and Definitive Resolution by the Pennsylvania Supreme Court

1. This Petition Presents Critical Question Concerning the Resolution of Interests Protected by the Fifth Amendment and the Legitimate Law Enforcement Needs

It is difficult to overstate the gravity of the privacy interests implicated by our use of and reliance upon electronic devices and the importance of access to such devices to state, local and federal law enforcement agencies. This fact of modern life alone calls upon this Court to review the Superior Court’s judgment and opinion in this case.

Password protected computer devices are pervasive in our community. A large percentage of the population carries smart phones, and almost as many likely own, possess or use other computer devices including tablets, desktop or notebook computers, many of which are password protected. Moreover, access to second tier data such as individual files contained on those devices and access to websites often requires a password. Cloud computing is a commonplace, consisting of the storage of all manner of computer files from financial data, photographs and other files on remote computer systems hosted by service providers such as Apple,

Google, Amazon or one of many other providers. Access to data in cloud storage requires a password to overcome encryption.

The privacy implications of access to the universe of computer media that each person owns are deep. In, the *Riley v. California*, __U.S.__, 134 S.Ct. 2473 (2014) Supreme Court of the United States examined the application of the search incident to arrest exception to the warrant requirement and observed that computer media—in that case, cell phones—implicate privacy concerns far beyond those implicated by the search of mere physical items due to the former’s immense storage capacity, the many distinct types of information such devices collect and store such that a phone or other device contains the “sum of an individual’s private life.” *Id.* at 2489. Although *Riley* involved the Fourth Amendment, the thrust of the case—the pervasive nature of computer devices in our lives—is instructive.

At the same time, access to password-protected electronically stored information is critical to law enforcement in all manner of investigations and prosecutions. The underlying opinion of the Superior Court contains but a brief survey of cases from other jurisdictions involving securities enforcement, child pornography and other crimes. The pervasiveness of electronic devices is such that any category of criminal activity can be recorded, proven or documented in some manner by access to a password protected handheld smartphone, a tablet, a

notebook or desktop computer, a file on such device, or on a cloud-based platform accessed through such a device.

2. This Court Should Grant Review in Order to Clarify the Underlying Question and Standards for the Application of the “Foregone Conclusion” Rationale to Computer Searches

This Court should grant the petition for allowance of appeal to clarify exactly what conclusion or conclusions must be shown to be “foregone”—that the subject knows the password or the contents of the computer, or both—and whether the prosecution must show manifest need, that is, that the contents of the computer may not be accessed without disclosure of the password by the subject, and by what standard.

All three elements were found by the Superior Court but the court did not specify whether a finding on less than all of the elements is sufficient to overcome the invocation of the Fifth Amendment. Review of the lower court opinion is appropriate therefore in order to resolve what is required to overcome the invocation of the privilege, clearly of great important to the administration of justice in the Commonwealth, even if the “foregone conclusion” doctrine could somehow be applied to an oral assertion of the otherwise un-shared contents of a person’s own mind.

In *Fisher, supra*, the Supreme Court held that the “existence and location” (emphasis added) of the accountants’ work papers were a “foregone conclusion.”

However, the production of documents does not easily map to the compelled production of a computer password. Perhaps as a result, lower courts are split on what must be shown. One view suggests that the prosecution must show only that the suspect knows the password. *United States v. Apple MacPro Computer*, 851 F.3d 238, n. 7 (3d Cir. 2017) (“It is important to note that we are not concluding that the Government’s knowledge of the contents of the devices is necessarily the correct focus of the ‘foregone conclusion’ inquiry ...”); *State v. Stahl*, 206 So.3d 124, 136 (Fla. App. 2016); *Commonwealth v. Gelfgatt*, 11N. E.3d 605, 615 (Mass. 2014).

Other courts have held that it is sufficient if the prosecution can demonstrate that it knows the contents of the computer media “with reasonable particularity.” *In re Boucher (Boucher II)*, No. 06-mj-91, 2009 WL 424718 (D. Vt.2009); *State v. Trant*, No. 15-2389, 2015 WL Me. Super. LEXIS 272, *10 (2015).

In the case at hand, the Superior Court rejected the petitioner’s claim that compelled disclosure was testimonial and thus protected by the Fifth Amendment, addressing first, the petitioner’s knowledge of the passcode, holding as follows:

- 1) That the Commonwealth knew with “reasonable particularity” that the password was in the subject’s “possession or control, and is authentic”; 2) that the computer could not be accessed without entry of the password; and, 3) that “technology is self-authenticating,” such that “if the computer is accessible once the password has been entered, it is clearly authentic.”

The lower court then noted that it “recognize[s] that multiple jurisdictions have recognized that the government’s knowledge of ... the evidence it seeks to compel need not be exact” and noted that the record showed a high probability that the contained computer child pornography.

There are two layers of ambiguity in the lower court’s holding. First, is it necessary for the prosecution to demonstrate both that it knows that the subject possess or controls the password and to describe with some level of specificity the contents of the computer, or it is sufficient to demonstrate but one of those elements? This ambiguity flows from the lower court’s quotation of *State v. Stahl, supra*, that the question turns on whether the prosecution has shown that it knows that the subject controls the password.⁶

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 possession or control and it authentic.

Commonwealth v. Davis, supra, quoting State v. Stahl, supra at 136 (emphasis added).

Yet, the lower court treated the prosecution’s knowledge of the contents as a required element by quoting with approval *Securities and Exchange Commission v.*

⁶ There is apparent ambiguity in other jurisdictions on what the prosecution must show in order to invoke the foregone conclusion rule for passwords. See *Commonwealth v. Gelfgatt*, 11 N.E. 3d 605, 615 (Mass. 2014); *United States v. Friscosu*, 841 F.Supp.2d 1232, 1237 (D.Col. 2012).

Huang, 2015 WL 561644 (E.D.Pa. 2015), which held that the government's sole burden is to show that it knows the contents of the encrypted data with reasonable particularity without regard to the subjects' knowledge of the password. In short, the lower court quoted with approval cases on both sides of the split of authority on whether the government must show knowledge of the password or the contents of the computer, or both. A simple analogy shows the clear error in this analysis. It is equally a "foregone conclusion" that the arrested suspect in an ordinary robbery case knows whether he was or was not at the scene of the robbery at the time of the crime. The police even have (by hypothesis that the arrest was valid) probable cause to believe they know the answer. Yet the suspect's privilege against having to respond to that question is the core of the Fifth Amendment's protection. The password in this case is no different.

Thus, this Court should grant the petition in order to establish clear and definable standards to determine the application of the foregone conclusion rationale.

CONCLUSION

The petition for allowance of appeal should be granted.

Respectfully Submitted,



Peter Goldberger (No. 22364)
Law Office of Peter Goldberger
50 Rittenhouse Place
Ardmore, PA 19003
610-649-8200

Witold J. Walczak
American Civil Liberties Union
Of Pennsylvania
247 Fort Pitt Boulevard
Pittsburgh, PA 15222
412-681-7864

Robert E. Welsh (No. 28143)
Catherine M. Recker (No. 56813)
Welsh & Recker, P.C.
Suite 2903
2000 Market Street
Philadelphia, PA 19103
215-972-6430

Attorneys for Petitioner

Appeal Docket Sheet

Superior Court of Pennsylvania

Docket Number: 1243 MDA 2016

Page 1 of 5

March 7, 2018



CAPTION

Commonwealth of Pennsylvania

v.

Joseph J. Davis
Appellant

CASE INFORMATION

Initiating Document: Notice of Appeal IFP

Case Status: Decided/Active

Case Processing Status: February 5, 2018 Awaiting Remittal

Journal Number: J-A20044-17

Case Category: Criminal Case Type(s): Criminal

CONSOLIDATED CASES

RELATED CASES

SCHEDULED EVENT

Next Event Type: Record Remitted

Next Event Type: Record Remitted

Next Event Due Date: January 2, 2018

Next Event Due Date: March 7, 2018

COUNSEL INFORMATION

Appellant Davis, Joseph J.

Pro Se: No

IFP Status: Yes

Attorney: Singer, Mark Alan

Law Firm: Luzerne County Public Defenders Office

Address: Penn Place
20 N. Pennsylvania Avenue
Wilkes-Barre, PA 18711

Attorney: Kostelaba, Michael Charles

Address: Luzerne County Public Defender's Office
Penn Place Building
20 N Pennsylvania Ave - Suite 235
Wilkes-Barre, PA 18701

Phone No: (570) 825-1754 Fax No:

Attorney: Fannick, Demetrius Wm.

Law Firm: Luzerne County Public Defender's Office

Address: 20 N Pennsylvania Ave #235
Wilkes-Barre, PA 18701

Phone No: (570) 830-5116 Fax No:

A-1

Appeal Docket Sheet

Superior Court of Pennsylvania

Docket Number: 1243 MDA 2016

Page 2 of 5

March 7, 2018



COUNSEL INFORMATION

Appellant Davis, Joseph J.
 Pro Se: No
 IFP Status: Yes
 Attorney: Young, Amanda Marie
 Address: Luzerne County Public Defender's Office
 20 N Pennsylvania Ave Ste 231
 Wilkes-Barre, PA 18701
 Phone No: (570) 825-1754 Fax No:

Appellee Commonwealth of Pennsylvania
 Pro Se: No
 IFP Status: No
 Attorney: Stoycos, William Ross
 Law Firm: PA Office of Attorney General
 Address: 16th Floor, Strawberry Square
 Harrisburg, PA 17120-0001
 Phone No: (717) 787-6348 Fax No:

FEE INFORMATION

Fee Dt	Fee Name	Fee Amt	Receipt Dt	Receipt No	Receipt Amt
03/07/2017	2nd Motion for Extension of Time	10.00	03/16/2017	2017-SPR-M-000208	10.00
04/17/2017	3rd Motion for Extension of Time	25.00	04/17/2017	2017-SPR-M-000300	25.00

AGENCY/TRIAL COURT INFORMATION

Court Below: Luzerne County Court of Common Pleas
 County: Luzerne Division: Luzerne County Criminal Division
 Order Appealed From: June 30, 2016 Judicial District: 11
 Documents Received: July 29, 2016 Notice of Appeal Filed: July 21, 2016
 Order Type: Order Entered
 OTN(s): T7162724
 Lower Ct Docket No(s): CP-40-CR-0000291-2016 CP-40-MD-0000011-2016
 Lower Ct Judge(s): Polachek Gartley, Tina
 Judge

ORIGINAL RECORD CONTENT

Original Record Item	Filed Date	Content Description
Original Record	October 07, 2016	2 Parts
Transcript(s)	October 07, 2016	1
Trial Court Opinion	October 07, 2016	
Supplemental Record	September 18, 2017	1 part

Date of Remand of Record:

BRIEFING SCHEDULE

Appellant	Appellee
Davis, Joseph J.	Commonwealth of Pennsylvania
Brief	Brief
Due: January 17, 2017	Filed: January 13, 2017
	Due: May 15, 2017
	Filed: May 15, 2017
Reply Brief	

A-2

Appeal Docket Sheet

Superior Court of Pennsylvania

Docket Number: 1243 MDA 2016

Page 3 of 5

March 7, 2018



BRIEFING SCHEDULE

Appellant

Davis, Joseph J.

Reply Brief

Due: May 30, 2017

Filed: May 25, 2017

DOCKET ENTRY

Filed Date	Docket Entry / Representing	Participant Type	Filed By
July 29, 2016	Notice of Appeal IFP Docketed	Appellant	Davis, Joseph J.
August 1, 2016	Docketing Statement Exited (Criminal)		Superior Court of Pennsylvania
August 11, 2016	Docketing Statement Received (Criminal)	Appellant	Davis, Joseph J.
August 16, 2016	Entry of Appearance - Attorney General Commonwealth of Pennsylvania	Appellee	Stoycos, William Ross
August 17, 2016	Order - Rule to Show Cause		Per Curiam
	Comment: Appellant cited in his notice of appeal and docketing statement that the June 30, 2016 order from which he filed the instant appeal is appealable under Pa.R.A.P. 313. It is not apparent at this time whether the June 30, 2016 order satisfies all three prongs of Pa.R.A.P. 313. Therefore, Appellant is directed to show cause, within 10 days of the date of this Order, why the appeal should not be quashed as taken from an unappealable order and how this appeal satisfies the requirements of Pa.R.A.P. 313.		
August 22, 2016	Response to Rule to Show Cause	Appellant	Davis, Joseph J.
October 5, 2016	Order Discharging Rule to Show Cause		Per Curiam
	Comment: The petition for review, treated as a petition for permission to appeal, is hereby DENIED. The application to proceed in forma pauperis, filed at No. 43 MDM 2016, is hereby DENIED as moot. The show-cause order at the appeal No. 1243 MDA 2016 is DISCHARGED and the issue of appealability is referred to the merits panel.		
October 7, 2016	Trial Court Record Received		Luzerne County Court of Common Pleas
October 7, 2016	Trial Court Opinion Received		Luzerne County Court of Common Pleas
October 7, 2016	Briefing Schedule Issued		Superior Court of Pennsylvania

A-3

Appeal Docket Sheet

Superior Court of Pennsylvania

Docket Number: 1243 MDA 2016

Page 4 of 5

March 7, 2018



DOCKET ENTRY

Filed Date	Docket Entry / Representing	Participant Type	Filed By
November 1, 2016	Entry of Appearance - Private Davis, Joseph J.	Appellant	Singer, Mark Alan
November 1, 2016	Application for Extension of Time to File Brief - First Request	Appellant	Davis, Joseph J.
November 1, 2016	Order Granting Application for Extension of Time to File Appellant Brief		Per Curiam
	Comment: 60 days given, due 1/17/17		
January 13, 2017	Appellant's Brief Filed	Appellant	Davis, Joseph J.
January 13, 2017	Reply Letter(s) Printed		Superior Court of Pennsylvania
January 19, 2017	Reply Received (Argument)	Appellant	Davis, Joseph J.
February 10, 2017	Application for Extension of Time to File Brief - First Request	Appellee	Commonwealth of Pennsylvania
February 13, 2017	Order Granting Application for Extension of Time to File Appellee Brief		Per Curiam
	Comment: 30 days given, due 3/15/17		
March 7, 2017	Application for Extension of Time to File Brief - Second Request	Appellee	Commonwealth of Pennsylvania
March 8, 2017	Order Granting Application for Extension of Time to File Appellee Brief		Per Curiam
	Comment: Upon consideration of the Commonwealth's application for extension of time to file its brief, the following is hereby ORDERED: The Commonwealth shall file its brief on or before April 14, 2017.		
April 17, 2017	Application for Extension of Time to File Brief - Third Request	Appellee	Commonwealth of Pennsylvania
April 18, 2017	Order Granting Application for Extension of Time to File Appellee Brief		Per Curiam
	Comment: Upon consideration of the Commonwealth's application for extension of time to file its brief, the application is hereby GRANTED as follows: The Commonwealth shall file its brief on or before May 15, 2017. No further extensions will be granted.		
May 15, 2017	Appellee's Brief Filed	Appellee	Commonwealth of Pennsylvania
May 25, 2017	Appellant's Reply Brief	Appellant	Davis, Joseph J.
July 5, 2017	Argument Letter Sent		Middle District Filing Office

A-4

Appeal Docket Sheet

Superior Court of Pennsylvania

Docket Number: 1243 MDA 2016

Page 5 of 5

March 7, 2018



DOCKET ENTRY

Filed Date	Docket Entry / Representing	Participant Type	Filed By
July 18, 2017	Acknowledgement of Argument Notice Commonwealth of Pennsylvania	Appellee	Stoycos, William Ross
July 19, 2017	Acknowledgement of Argument Notice Davis, Joseph J.	Appellant	Singer, Mark Alan
August 16, 2017	Argued		Superior Court of Pennsylvania
September 18, 2017	Supplemental Record Filed		Luzerne County Court of Common Pleas
November 30, 2017	Affirmed		Ford Elliott, Kate
December 7, 2017	Application for Reargument	Appellant	Davis, Joseph J.
February 5, 2018	Order Denying Application for Reargument		Per Curiam

Comment: IT IS HEREBY ORDERED:

THAT the application filed December 7, 2017, requesting reargument of the decision dated November 30, 2017, is DENIED.

SESSION INFORMATION

Journal Number: J-A20044-17
 Consideration Type: Argument Panel
 Listed/Submitted Date: August 16, 2017

Panel Composition:

The Honorable Susan Peikes Gantman	President Judge
The Honorable Jack A. Panella	Judge
The Honorable Kate Ford Elliott	President Judge Emeritus

DISPOSITION INFORMATION

Final Disposition:	Yes	Judgment Date:	November 30, 2017
Related Journal No:	J-A20044-17	Disposition Author:	Ford Elliott, Kate
Category:	Decided	Disposition Date:	November 30, 2017
Disposition:	Affirmed	Filing Author:	Ford Elliott, Kate
Dispositional Filing:	Opinion		
Filed Date:	11/30/2017 12:00:00AM		

REARGUMENT / RECONSIDERATION / REMITTAL

Filed Date: December 7, 2017
 Disposition: Order Denying Application for Reargument
 Disposition Date: February 5, 2018
 Record Remittal:

AS

file

IN THE COURT OF COMMON PLEAS
OF LUZERNE COUNTY

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

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 # MXX41000000420 containing Seagate 2 TB hard Drive with serial # Z4Z1AAAEFM or within thirty (30) days from the date of this Order.

CLERK OF COURTS
2016 JUN 30 PM 3:55
CRIMINAL DIV
LUZERNE COUNTY

The Clerk of Courts 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 Pa.R.Crim.P. 114.

BY THE COURT:

POLACHEK 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

Δ(LCCF) - sent 7/13/16 © . B-1

Received
JUL 07 2016
Office of the 1
Luzerne County Public Defender

IN THE COURT OF COMMON PLEAS
OF LUZERNE COUNTY

COMMONWEALTH OF PENNSYLVANIA:

v.

CRIMINAL DIVISION

JOSEPH J. DAVIS

Defendant

: NO. 11 MD 2016; 291 ^{ck}MD 2016

ORDER

AND NOW, this 2th day of September, 2016, it is hereby DIRECTED that the attached Opinion, filed on June 30, 2016, is adopted and entered pursuant to Pa. R.A.P. 1925 (c) in response to Defendant's Concise Statement of Errors Complained of on Appeal.

The Clerk of Courts of Luzerne County is hereby **ORDERED** and **DIRECTED** to transmit the entire record in this case to the Superior Court of Pennsylvania, and shall serve a copy of this Order and Opinion on all counsel of record.

BY THE COURT:


POLACHEK GARTLEY, J.

CLERK OF COURTS
16 SEP 27 PM 3:17
CRIMINAL DIV.
LUZERNE COUNTY

Copies
Rebecca Elo, Esquire
Mark A. Singer, Esquire, Luzerne County Public Defender's Office
Court Administration

C-1

IN THE COURT OF COMMON PLEAS
OF LUZERNE COUNTY

COMMONWEALTH OF PENNSYLVANIA :
 : CRIMINAL DIVISION
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
Count 2	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 law enforcement computer.

Special Agent Leri personally viewed the file identified as [boy+man] [MB] NEW!!Man & 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 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 "TrueCrypt" 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 stated 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, 93 S.Ct. 611, 34 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).

C-8

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 use "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. Gelfgatt*, 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 *Gelfgatt*, 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.

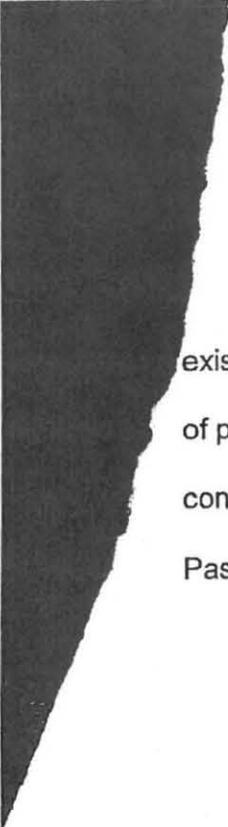
Such is not in the case at bar. In the case herein, the testimony established that (1) the HP Envy 700 desktop computer located in Defendant's residence was hard-wired internet access only; (2) the Defendant admitted to the agents that the computer has TrueCrypt encryption, which he is the sole user of that computer and he is the only individual who know the password; (3) that Defendant admitted to Agents that "we both knows what is 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 based on documents that had come to light because of his compliance with an earlier subpoena. *Hubbell* argued that the evidence derived from the documents should be privileged as fruits of a testimonial set of production. The court distinguished the

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 known 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**.

END OF OPINION

C-1a

COMMONWEALTH OF PENNSYLVANIA	:	IN THE SUPERIOR COURT OF
	:	PENNSYLVANIA
v.	:	
	:	
JOSEPH J. DAVIS,	:	No. 1243 MDA 2016
	:	
Appellant	:	

Appeal from the Order Entered June 30, 2016,
in the Court of Common Pleas of Luzerne County
Criminal Division at Nos. CP-40-CR-0000291-2016,
CP-40-MD-0000011-2016

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

D-1

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 eDonkey2000^[1] 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 [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.

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

Special Agent Leri personally viewed the file identified as [boy+man][MB]NEW!!Man&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. [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 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

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

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) language.⁴ On July 21, 2016, appellant filed a timely

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).

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 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.

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 . . .").

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

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).

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 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

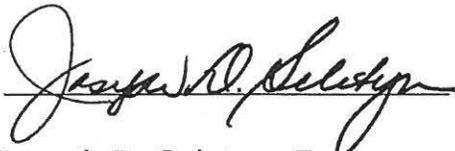
J. A20044/17

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.

Judgment Entered.



Joseph D. Seletyn, Esq.
Prothonotary

Date: 11/30/2017

PROOF OF SERVICE

I hereby certify that on this date I served a copy of the attached Petition for Allowance of Appeal on the following counsel of record in the Superior Court action below by placing it in the United States Mail, postage prepaid:

William Ross Stoycos, Esq.
Pennsylvania Office of Attorney General
16th Floor, Strawberry Square
Harrisburg, PA 17120-0001

Date: March 7, 2018



Robert E. Welsh Jr. (no. 28143)