

IN THE SUPREME COURT OF PENNSYLVANIA

No. 56 MAP 2018

COMMONWEALTH OF PENNSYLVANIA

Appellee,

v.

JOSEPH J. DAVIS

Appellant.

BRIEF FOR APPELLANT JOSEPH DAVIS

*Appeal from the Order of the Superior Court of Pennsylvania,
1243 MDA 2016, dated November 20, 2017.*

Brett Max Kaufman*
Jennifer S. Granick*
American Civil Liberties Union
125 Broad St., Floor 18
New York, NY 10004
(t) 212.549.2500

* *Pro hac vice* pending

Witold J. Walczak, Pa. I.D. 62976
Andrew Christy, Pa. I.D. 322053
ACLU of Pennsylvania
P.O. Box 60173
Philadelphia, PA 19102
(t) 215.592.1513 x138
(f) 267.225.0447
achristy@aclupa.org

Counsel for Appellant Joseph J. Davis

Peter Goldberger, Pa. I.D. 22364
50 Rittenhouse Place
Ardmore, PA 19003
(t) 610.649.8200
peter.goldberger@verizon.net

Robert E. Welsh, Pa. I.D. 28143
Catherine M. Recker, Pa. I.D. 56813
Welsh & Recker, P.C.
2000 Market Street, Suite 2903
Philadelphia, PA 19103
(t) 215.972.6430

Steven Greenwald, Pa. I.D. 42890
Luzerne County Public Defender
20 N. Pennsylvania Avenue
Wilkes-Barre, PA 18701
(t) 570-825-1754

TABLE OF CONTENTS

TABLE OF AUTHORITIES	iii
STATEMENT OF JURISDICTION.....	1
ORDERS IN QUESTION.....	1
STATEMENT OF THE SCOPE AND STANDARD OF REVIEW	2
QUESTION PRESENTED FOR REVIEW	2
STATEMENT OF THE CASE.....	2
A. Form of Action and Procedural History.....	2
B. Factual Background.....	5
SUMMARY OF ARGUMENT	8
ARGUMENT	11
I. The Fifth Amendment to the U.S. Constitution Protects Against Compelled Disclosure of a Computer Password.....	11
A. The Fifth Amendment Prohibits the Commonwealth from Compelling Appellant to Disclose his Computer Password, Either Orally or in Writing.....	14
B. Even an Order Compelling Appellant to Decrypt his Computer by Entering his Password Himself Would Violate the Fifth Amendment Because the Self-Incrimination Privilege Applies to Non-Verbal Acts that Require the Witness’s Mental Capacity to Perform.	17
C. The “Foregone Conclusion” Rationale Does Not Apply to the Compelled Disclosure or Entry of Computer Passwords to Decrypt Electronic Devices.....	24
D. Even if the “Foregone Conclusion” Rationale Could Apply to the Compelled Decryption of a Computer, the Commonwealth Cannot Satisfy It Here.....	29
II. The Self-Incrimination Privilege Enshrined in Article I, Section 9 of the Pennsylvania Constitution, Independently Protects Appellant Davis from Compulsion to Reveal the Password for his Encrypted Computer, Notwithstanding Any Conclusion this Court May Reach under the United States Constitution.....	33
A. Constitutional Text.....	39
B. History and Policy	46

C. Decisions in Other Jurisdictions.....51

D. Conclusion Under the Article I, Section 9 Privilege: The Judgment of the Superior Court Must Be Reversed.....55

CONCLUSION.....56

ADDENDUM OF STATE CONSTITUTIONAL PROVISIONS

APPENDIX A (SUPERIOR COURT OPINION)

APPENDIX B (TRIAL COURT OPINION)

CERTIFICATES

TABLE OF AUTHORITIES

Cases

<i>Albertson v. Albertson</i> , 73 Va. Cir. 94 (19th Jud.Cir. 2007)	53
<i>Boyd v. United States</i> , 116 U.S. 616 (1886)	13, 20
<i>Boyle v. Smithman</i> , 146 Pa. 255, 23 A. 397 (1892).....	44
<i>Braswell v. United States</i> , 487 U.S. 99 (1988).....	19
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	41
<i>Commonwealth v. Arroyo</i> , 555 Pa. 125, 723 A.2d 162 (1999).....	36, 40
<i>Commonwealth v. Baust</i> , 89 Va. Cir. 267 (4th Jud. Cir. 2014)	16, 53
<i>Commonwealth v. Cooley</i> , 632 Pa. 119, 118 A.3d 370 (2015)	36
<i>Commonwealth v. Dabbierio</i> , 290 Pa. 174, 138 A. 679 (1927)	42
<i>Commonwealth v. Davis</i> , 2017 Pa. Super. 376, 176 A.3d 869.....	passim
<i>Commonwealth v. Dravec</i> , 424 Pa. 582, 227 A.2d 904 (1967).....	45
<i>Commonwealth v. Edmunds</i> , 526 Pa. 374, 586 A.2d 887 (1991).....	38
<i>Commonwealth v. Fisher (Appeal of Snyder)</i> , 398 Pa. 237, 157 A.2d 207 (1960).....	39
<i>Commonwealth v. Gary</i> , 625 Pa. 183, 91 A.3d 102 (2014).....	13
<i>Commonwealth v. Gelfgatt</i> , 11 N.E.3d 605 (Mass. 2014).....	53
<i>Commonwealth v. Gibbs</i> , 4 U.S. (4 Dallas) 253 (1802)	43
<i>Commonwealth v. Johnson</i> , 115 Pa. 369, 9 A. 78 (1887).....	45
<i>Commonwealth v. Knoble</i> , 615 Pa. 285, 42 A.3d 976 (2012)	4, 36
<i>Commonwealth v. Molina</i> , 628 Pa. 465, 104 A.3d 430 (2014)	passim
<i>Commonwealth v. Muniz</i> , 640 Pa. 699, 164 A.3d 1189 (2017).....	34
<i>Commonwealth v. Swinehart</i> , 541 Pa. 500, 664 A.2d 957 (1995).....	37
<i>Commonwealth v. Triplett</i> , 462 Pa. 244, 341 A.2d 62 (1975).....	37, 39
<i>Commonwealth v. Turner</i> , 499 Pa. 579, 454 A.2d 537 (1982).....	37
<i>Commonwealth v. Valeroso</i> , 273 Pa. 213, 116 A. 828 (1922)	44

<i>Couch v. United States</i> , 409 U.S. 322 (1973).....	10
<i>Curcio v. United States</i> , 354 U.S. 118 (1957)	9, 14, 15
<i>D’Elia v. Pennsylvania Crime Commission</i> , 521 Pa. 225, 555 A.2d 864 (1989)....	37
<i>Doe v. United States</i> , 487 U.S. 201 (1988).....	passim
<i>Entick v. Carrington</i> , 19 How. St. Tr. 1029 (1813 ed.).....	44
<i>Firing v. Kephart</i> , 466 Pa. 560, 353 A.2d 833 (1976).....	40
<i>Fisher v. United States</i> , 425 U.S. 391 (1976).....	passim
<i>G.A.Q.L. v. State</i> , 2018 WL 5291918 (Fla. 4th Dist. Ct. App., Oct. 24, 2018) 16, 53	
<i>Galbreath’s Lessee v. Eichelberger</i> , 3 Yeates 515 (Pa. 1803).....	43, 48
<i>Gilbert v. California</i> , 388 U.S. 263 (1967).....	18
<i>Goldsmith v. Superior Court</i> , 152 Cal. App. 3d 76 (1984)	28
<i>Griffin v. California</i> , 380 U.S. 609 (1965)	37
<i>Hoffman v. United States</i> , 341 U.S. 479 (1951)	12, 30
<i>Holt v. United States</i> , 218 U.S. 245 (1910)	18
<i>Horstman v. Kaufman</i> , 97 Pa. 147 (1881)	44
<i>In re Boucher</i> , 2007 WL 4246473 (D. Vt. Nov. 29, 2007)	17
<i>In re Eckstein</i> , 148 Pa. 509, 24 A. 63 (1892).....	49
<i>In re Grand Jury Subpoena Dated April 18, 2003</i> , 383 F.3d 905 (9th Cir. 2004)..	30
<i>In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011</i> , 670 F.3d 1335 (11th Cir. 2012)	21, 31, 52
<i>In re Grand Jury Subpoenas Served Feb 27, 1984</i> , 599 F. Supp. 1006 (E.D. Wash. 1984).....	27
<i>League of Women Voters v. Commonwealth</i> , 178 A.3d 737 (Pa. 2018)	40
<i>McElree v. Darlington</i> , 187 Pa. 593, 41 A. 456 (1898)	44
<i>Michigan v. Long</i> , 463 U.S. 1032 (1983)	34
<i>Murphy v. Waterfront Commission</i> , 378 U.S. 52 (1964).....	12, 13

<i>Pap’s A.M. v. City of Erie</i> , 571 Pa. 375, 812 A.2d 591 (2002)	34, 38
<i>Pennsylvania v. Muniz</i> , 496 U.S. 582 (1990)	15, 16, 19, 40
<i>Respublica v. Gibbs</i> , 3 Yeates 429 (Pa. 1802).....	43, 44, 48
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	13
<i>Schmerber v. California</i> , 384 U.S. 757 (1966).....	18, 19
<i>Seo v. State</i> , 109 N.E.3d 418 (Ind. Ct. App. 2018).....	passim
<i>Sprague v. Cortes</i> , 636 Pa. 542, 145 A.3d 1136 (2016).....	40
<i>State v. Andrews</i> , 2018 WL 5985982 (N.J. App. Div. Nov. 15, 2018)	53
<i>State v. Stahl</i> , 206 So.3d 124 (Fla. 2d Dist. Ct. App. 2016).....	53
<i>Stilp v. Commonwealth</i> , 588 Pa. 539, 905 A.2d 918 (2006)	40
<i>The Trial of William Penn and William Mead</i> , 6 Howell's State Trials (1670) 951 (1816 ed.) (No. 230)	47
<i>United States v. Apple MacPro Computer</i> , 851 F.3d 238 (3d Cir. 2017).....	31, 51
<i>United States v. Arthur Young & Co.</i> , 465 U.S. 805 (1984).....	25
<i>United States v. Dionisio</i> , 410 U.S. 1 (1973).....	18
<i>United States v. Green</i> , 272 F.3d 748 (5th Cir. 2001).....	22, 23
<i>United States v. Hubbell</i> , 530 U.S. 27 (2000)	passim
<i>United States v. Kirschner</i> , 823 F. Supp. 2d 665 (E.D. Mich. 2010).....	17, 21
<i>United States v. Mitchell</i> , 76 M.J. 413, 2017 WL 3841376 (C.A.A.F. 2017).....	52
<i>United States v. Nobles</i> , 422 U.S. 225 (1975)	16
<i>United States v. Ponds</i> , 454 F.3d 313 (D.C. Cir. 2006).....	29
<i>United States v. Sideman & Bancroft, LLP</i> , 704 F.3d 1197 (9th Cir. 2013).....	27
<i>United States v. Spencer</i> , 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018).....	17, 30
<i>Washington v. Dep’t of Public Welfare</i> , 188 A.3d 1135 (Pa. 2018)	40, 42
<i>Zauflik v. Pennsbury Sch. Dist.</i> , 629 Pa. 1, 49, 104 A.3d. 1096 (2014).....	41

Statutes

Pennsylvania Constitution, Article I, Section 25	9, 38
Pennsylvania Constitution, Article I, Section 9	9
Pennsylvania Statutes Title 42, Section 5941(a)	39, 49

Other Authorities

Abe Fortas, <i>The Fifth Amendment: Nemo Tenetur Prodere Seipsum</i> , 25 J. Cleveland Bar Ass'n 91 (1954)	50
Eben Moglen, <i>The Privilege in British North America: The Colonial Period to the Fifth Amendment in The Privilege Against Self-Incrimination: Its Origins and Development</i> (R.H. Helmholz et al., eds., 1997).....	46, 48
Henry E. Smith, <i>The Modern Privilege: Its Nineteenth Century Origins in The Privilege Against Self-Incrimination: Its Origins and Development</i> (R.H. Helmholz et al., eds., 1997).....	44
Jennifer Friesen, <i>State Constitutional Law: Litigating Individual Rights, Claims, and Defenses</i> § 12.02[2] (4th ed. 2008 & 2015 Supp.).....	41, 51
Ken Gormley, <i>The Pennsylvania Constitution: A Treatise on Rights and Liberties</i> § 12.6[a] (2004)	49
Leonard Levy, <i>Origins of the Fifth Amendment and Its Critics</i> , 19 Cardozo L.Rev. 821 (1997).....	47
Leonard Sosnov, <i>Criminal Procedure Rights Under the Pennsylvania Constitution: Examining the Present and Exploring the Future</i> , 3 Widener J. Pub. L. 217 (1993).....	37
Leonard W. Levy, <i>Origins of the Fifth Amendment: The Right Against Self-Incrimination</i> (2d ed. 1986).....	43, 46, 47
Ronald J. Allen & M. Kristin Mace, <i>The Self-Incrimination Clause Explained and Its Future Predicted</i> , 94 J. Crim. L. & Criminology 243 (2004).....	14
Thomas Raeburn White, <i>Commentaries on the Constitution of Pennsylvania</i> 104 (1907).....	50

STATEMENT OF JURISDICTION

This Court has jurisdiction under 42 Pa.C.S. § 724(a) (allowance of appeal from final order of Superior Court). The Superior Court entered judgment on November 30, 2017, and denied reargument on February 5, 2018. This Court granted Mr. Davis’s petition on October 3, 2018.

The Luzerne County Court of Common Pleas entered the underlying order on June 30, 2016, granting a motion to compel Mr. Davis to disclose his computer password. Mr. Davis filed a timely notice of appeal on July 15, 2016, invoking collateral order jurisdiction under Pa.R.A.P. 313.

ORDERS IN QUESTION

The Order granting allowance of appeal states:

PER CURIAM

AND NOW, this 3rd day of October, 2018, the Petition for Allowance of Appeal is **GRANTED**. The issue, as stated by Petitioner, is:

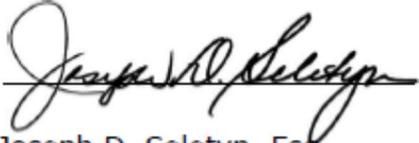
May [Petitioner] be compelled to disclose orally the memorized password to computer over his invocation of privilege under the Fifth Amendment to the Constitution of the United States, and Article I, [S]ection 9 of the Pennsylvania Constitution?

The Order and Opinion of the Superior Court are reported at 176 A.3d 869.

It requires that Mr. Davis “provide the password that will allow access to his lawfully seized encrypted computer.” Appendix A. The Order reads:

Order affirmed.

Judgment Entered.



Joseph D. Seletyn, Esq.
Prothonotary

Date: 11/30/2017

STATEMENT OF THE SCOPE AND STANDARD OF REVIEW

For questions of law, including those “involving a constitutional right,” as here, this Court’s scope of review is plenary; the standard of review is *de novo*. *Commonwealth v. Molina*, 628 Pa. 465, 104 A.3d 430, 441 (2014).

QUESTION PRESENTED FOR REVIEW

May Mr. Davis be compelled to disclose a memorized computer password over his invocation of privilege under the Fifth Amendment to the U.S. Constitution and Article I, Section 9, of the Pennsylvania Constitution?

Answer: “No.”

STATEMENT OF THE CASE

A. Form of Action and Procedural History

This matter arises from an interlocutory appeal in a prosecution for distributing child pornography. Mr. Davis was arrested on October 20, 2015 and 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). (R.15a). The charges stem from two incidents, one in July 2014 and the other in October 2015, in each of which the Pennsylvania Office of the Attorney General (“POAG”) identified an illicit video shared on the peer-to-peer platform “edonkey2000/eMule.” (R.18a, 20a). In an Information filed February 11, 2016, the Commonwealth charged Mr. Davis in four bills with the same offenses. (R.4a).

On December 17, 2015, the Commonwealth filed a Motion to Compel Defendant to Provide Password for Encryption Enabled Device. (R.27a). The Commonwealth averred that it:

knows with reasonable particularity that there is likely child pornography and/or evidence of child pornography files on the computer seized from the Defendant’s residence, and that the Defendant was utilizing a Windows based version of eMule (the file sharing program utilized by the Defendant in this case) on those computers... It is a foregone conclusion that the device seized from the Defendant contains child pornography and/or evidence of child pornography files, and thus, there is no violation of a self-incrimination privilege.

(R.28a-29a). The Commonwealth therefore requested that the trial court “Order the defendant to provide the Commonwealth with the password” to his computer. (R.29a).

The trial court held an evidentiary hearing on January 14, 2016, at which three POAG investigators testified, and the trial court took the matter under advisement. (R.32a-46a). Mr. Davis filed his opposition on January 28, 2016.

(R.48a). On June 30, 2016, the court issued an opinion and order concluding that “the Commonwealth has prior knowledge of the existence as well as the whereabouts of the documents,” and thus the “Defendant’s act of production loses its testimonial character because the information is a ‘foregone conclusion.’” (R.56a; Appendix B).

The trial court granted a motion for appeal, amending its Order as required. (R.57a-59a). Mr. Davis then filed a timely notice of appeal pursuant to Pa.R.A.P. 313(b). (R.64a). Mr. Davis filed a Pa.R.A.P. 1925(b); the trial court incorporated by reference its June 30 opinion into its Rule 1925(a) opinion. (R.59a, 64a). The Superior Court referred any issues of appealability to the merits panel. (R.64a).

On November 30, 2017, the Superior Court issued an opinion affirming the trial court. (R.66a). The panel concluded that the “act of providing the password in question is not testimonial in nature and his Fifth Amendment right against self-incrimination would not be violated.” *Commonwealth v. Davis*, 2017 Pa. Super. 376, 176 A.3d 869, 876 (Appendix A). The court further ruled that the Pennsylvania Constitution (Art. I § 9) “affords no greater protections against self-incrimination than the Fifth Amendment to the United States Constitution”; it did not independently analyze the state constitutional claim. *Id.* at 874 n.6 (quoting *Commonwealth v. Knoble*, 615 Pa. 285, 42 A.3d 976, 979 n.2 (2012)). Following

denial of reargument, Mr. Davis filed a timely Petition for Allowance of Appeal, which this Court granted on October 3, 2018. (R.66a).

Since October 20, 2015, Mr. Davis has been held in pretrial detention on \$200,000 cash bail. (R.2a, 25a). Attempts to reduce the bail amount have been rebuffed. He has now been confined for over three years. (R.7a-8a). The trial court has stayed any action in the case, including the resolution of a pretrial motion to suppress (R.53a), until this appeal is resolved. (R.63a).

B. Factual Background

In July 2014, POAG found a video depicting child pornography that was shared on eMule. (R.33a). After downloading the video, POAG's investigators determined that the IP address from which it was shared was registered with Comcast. (R.34a). The Commonwealth obtained a court order to compel Comcast to provide subscriber information, which disclosed Mr. Davis's name and contact information. *Id.*

POAG Agent Justin Leri executed a search warrant on September 9, 2014 at Mr. Davis's apartment. *Id.* Agent Leri informed Mr. Davis that he was not under arrest but verbally provided him with *Miranda* warnings.¹ (R.35a). Mr. Davis acknowledged that he lived alone and was the sole user of a Dell computer. *Id.* He

¹ This factual background is based on the testimony and sworn statements of Agents Leri, Block, and Cook. Mr. Davis did not testify at a hearing below.

also disclosed a prior child pornography sentence. *Id.* He denied that computer contained any contraband images. (R.19a). He then declined to answer additional questions without a lawyer. (R.35a).²

On October 4, 2015, another POAG investigator, Daniel Block, identified a different child pornography video that was shared on eMule. (R.37a). An administrative subpoena to Comcast seeking IP subscriber information again produced Mr. Davis's name and address. *Id.* On October 20,³ investigators executed another search warrant. (R.38a). Mr. Davis told them he lived alone and had a desktop computer hardwired to the Internet. (R.39a). When the agents entered, they found the cable modem—which provides Internet access—disconnected. (R.43a).

Agent Block described Mr. Davis as using “hardwired Internet services, which are password protected and only he knows the password.” (R.39a). Agent Block asked Mr. Davis for the password to his computer, but Mr. Davis refused to disclose it. *Id.* Mr. Davis advised that he watches football and “gay X-rated movies” on his computer, which he described as “legal porn” that he purchased with a credit card. (R.22a). The agents arrested Mr. Davis for the eMule distributions and seized his computer. *Id.*

² The agents seized a computer and two DVDs, but made no arrest. (R.35a). The computer seized in 2014 is not the subject of the Commonwealth's motion. (R.27a-28a).

³ The Superior Court erroneously gives the date as October 10.

After arresting him, Agent Block again asked Mr. Davis if he would reveal the password to his computer, to which Mr. Davis 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 fucking way I'm going to give it to you.” (R.40a). Agent Block did not say he ever asked Mr. Davis about the specific videos underlying the charges, nor did he testify to having sought clarification of his statement about the password.

Agent Block again conversed with Mr. Davis in a holding cell prior to arraignment. Mr. Davis questioned why the “government continuously spies on individuals” and also asked why, if child pornography was illegal, “why has the government not taken down these websites” that share such videos. (R.41a).

When Agent Block again asked whether Mr. Davis could remember the password to his computer, he said that he could not, and that, even if he could, it would be like “putting a gun to his head and pulling the trigger.” (R.41a). He later said that he would “die in jail before he could ever remember the password.” *Id.*

Agent Braden Cook, a senior supervisory agent in the computer forensics unit, examined the computer seized from Mr. Davis’s apartment. Upon examination, he found that a portion of the computer’s hard drive was encrypted with TrueCrypt. (R.43a). Agent Cook testified that he knows only that there is “Windows on the computer and the TrueCrypt.” (R.45a). While the computer could not be “blank,” the only files he knew were on it were “the operating

systems and the files associated with that in order for the TrueCrypt volume to have been placed on the computer in the first place.” *Id.* Agent Cook testified that he had no knowledge of any specific files on the computer other than the operating system files. *Id.*

SUMMARY OF ARGUMENT

The Superior Court affirmed a pretrial order to compel Appellant Joseph Davis to recollect and disclose a password so that investigators may decrypt data stored on a desktop computer found at his home. The objective is to obtain evidence to be used against him in a pending criminal case. Appellant has refused, invoking his state and federal constitutional rights against compulsory self-incrimination. Because the courts below wrongly assessed the principles at stake, this Court should reverse.

While encryption of personal electronic devices is relatively new, the right upon which Appellant now relies is venerable. The same is true of the dilemma faced here by law enforcement: investigators believe additional evidence of a crime exists, but they have been unable to access it. They believe appellant has the knowledge necessary to provide them with that additional evidence. But decades, if not centuries, of precedent support the conclusion that, in cases like this one, a suspect or defendant cannot be compelled to recall and use information that exists only in his mind in order to aid the prosecution. *See Curcio v. United States*, 354

U.S. 118, 128 (1957). This is no technicality; it is a fundamental protection of human dignity, agency, and integrity that the Framers enshrined in the Fifth Amendment to the U.S. Constitution, and that the People of Pennsylvania likewise declared in our Commonwealth's founding document (Art. I, § 9) to be forever protected. Pa.Const., Art. I, § 25.

Appellant cannot be forced to assist the Commonwealth in gathering information that would tend to incriminate him. The Commonwealth attempts to make an end-run around this long-established Fifth Amendment right by asserting that the Constitution's protections do not reach him because what they seek to compel Mr. Davis to say is a "foregone conclusion." This argument is unsupported by either the law or the facts.

First, there is no exception that allows the Commonwealth to sidestep an accused's right against self-incrimination in the context of compelled oral or written testimony. The prosecution's demand in this case is for oral or written testimony of appellant's computer password, and that is absolutely prohibited by the state and federal Constitutions.

Second, even if the prosecution had instead asked the trial court to order appellant to enter his password into his computer directly (rather than reveal that password through written or oral testimony)—which it did not, and which is not what the trial court ordered—it would still be barred by the Fifth Amendment. To

accomplish the act of entering his password into a computer, appellant would have to recollect and use the contents of his mind in order to comply. The very purpose of the constitutional privilege is to ensure “a private inner sanctum of individual feeling and thought.” *Couch v. United States*, 409 U.S. 322, 327 (1973).

The so-called “foregone conclusion” rationale, applied a single time in a starkly different context by the U.S. Supreme Court, *see Fisher v. United States*, 425 U.S. 391 (1976), has never been applied to require a witness to remember, think, use, or disclose the contents of his mind. *Doe v. United States*, 487 U.S. 201, 208 n. 6 (1988) (hereafter “*Doe I*”). Moreover, even if the manual entry of a password —again, not the demand the Commonwealth made in the instant case— could be said to be a pure “act of production” involving no mentation, it would still have communicative aspects that are privileged under the Fifth Amendment. The act of production can be functionally testimonial, revealing custody and control, and authenticating documents. These messages implicit in the act of production bring it within the purview of the privilege not subject to any “foregone conclusion” exception.

Indeed, the Supreme Court of the United States has never referred to the foregone conclusion inquiry as a “doctrine,” but merely utilized it as a rationale—one which, “whatever [its] scope,” the Court has rejected in each of the “act of production” cases it has considered since *Fisher*. *See United States v. Hubbell*, 530

U.S. 27 (2000); *Doe I*, 487 U.S. 201. Cases that have relied on *Fisher* to conclude that an act of production is a “foregone conclusion” almost exclusively involve subpoenas for business documents, not for personal information. Here, the Commonwealth seeks to take *Fisher* much farther. The prosecution now argues that the “foregone conclusion” rationale can be used to force an accused to give oral or written testimony, or otherwise use his personal thoughts to incriminate himself. The Fifth Amendment privilege, like the similar privilege included 15 years earlier in Pennsylvania’s Declaration of Rights, was designed to prevent this.

The self-incrimination privilege enshrined in the Pennsylvania Constitution independently protects appellant from compulsion to reveal his password—and because its protection is even greater than that provided by the federal constitution, this Court should choose to reach it whether or not it decides the question presented under federal law.

ARGUMENT

I. The Fifth Amendment to the U.S. Constitution Protects Against Compelled Disclosure of a Computer Password.

The Fifth Amendment to the U.S. Constitution prohibits any governmental authority from compelling appellant to disclose his computer password. The Fifth Amendment guarantees, in part, that “[n]o person shall be . . . compelled in any

criminal case to be a witness against himself.” This privilege against self-incrimination is a “protection against the prosecutor’s use of incriminating information derived directly or indirectly” from compelled testimony. *Hubbell*, 530 U.S. at 38. Moreover, “compelled testimony that communicates information that may ‘lead to incriminating evidence’ is privileged even if the information itself is not inculpatory.” *Id.* (quoting *Doe I*, 487 U.S. at 208 n.6); accord *Hoffman v. United States*, 341 U.S. 479, 486 (1951) (“The privilege ... embraces those [answers] which would furnish a link in the chain of evidence needed to prosecute the claimant”). To successfully invoke the Fifth Amendment’s self-incrimination privilege, an individual must show: (1) that the evidence is testimonial in nature, (2) that the evidence is self-incriminating, and (3) that the evidence is compelled. *Hubbell*, 530 U.S. at 34. Only the first of these is in dispute here.

The privilege against self-incrimination is rooted in our nation’s “unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt,” “our respect for the inviolability of the human personality and of the right of each individual ‘to a private enclave where he may lead a private life,’” and “our realization that the privilege, while sometimes ‘a shelter to the guilty,’ is often ‘a protection to the innocent.’” *Doe I*, 487 U.S. at 212–13 (quoting *Murphy v. Waterfront Comm’n*, 378 U.S. 52, 55 (1964)).

Compelled decryption also encroaches on “the right of each individual ‘to a private

enclave where he may lead a private life.” *Couch*, 409 U.S. at 616, *citing Murphy*, 378 U.S. at 55. Electronic devices, “[w]ith all they contain and all they may reveal, . . . hold for many Americans ‘the privacies of life.’” *Riley v. California*, 134 S. Ct. 2473, 2494–95 (2014) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)); *see also Commonwealth v. Gary*, 625 Pa. 183, 245, 91 A.3d 102 (2014) (Todd, J., dissenting) (explaining that laptops and smartphones “are digital treasure troves which contain significant amounts of highly sensitive personal and business information”). Electronic devices may thus contain “a digital record of nearly every aspect of [users’] lives — from the mundane to the intimate.” *Riley*, 134 S. Ct. at 2490.

To force a suspect to use his thoughts and memories to assist in a prosecution against himself violates the long-standing principles enshrined in the Fifth Amendment. In a case like this one, without the privilege, those using encryption to protect their personal privacy on digital devices would face an unacceptable choice: either provide the prosecution with the allegedly incriminating information they possess; lie about their inability to do so; or be held in contempt for failure to cooperate.⁴ The privilege was designed exactly to prevent suspects from facing this “cruel trilemma.” *See Doe I*, 487 U.S. at 212.

⁴ The order here highlights the untenable position facing an accused who is required to provide testimony to assist in their own prosecution. A person who does not know or cannot remember the password to a device may be unable, not merely unwilling, to comply with a

A. The Fifth Amendment Prohibits the Commonwealth from Compelling Appellant to Disclose his Computer Password, Either Orally or in Writing.

The Superior Court’s order here would require appellant to recall and disclose the password to an encrypted computer. The compelled recollection and subsequent disclosure of a memorized password is quintessentially testimonial.

The privilege against self-incrimination protects against government compulsion that would require a person to use “the contents of his own mind” to truthfully communicate some fact. *Curcio*, 354 U.S. at 128. It protects any “cognition caused by the state, the paradigmatic example being the retrieval of information from memory.” Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and Its Future Predicted*, 94 J. Crim. L. & Criminology 243, 268 (2004). Providing his password would reveal the contents of Mr. Davis’s mind—a memorized sequence of numbers, letters, or other characters that he mentally associates with a particular device. Simply put: Because the password is information appellant would have stored in his brain, the State cannot compel its disclosure.

The privilege applies regardless of whether appellant would be required to

court’s order. The self-incrimination privilege ensures that an innocent person cannot be imprisoned for failing to comply with an order if the court erroneously fails to credit the representation that he has forgotten it. *Cf.* R.41a.

reveal his password to law enforcement agents orally or in writing. The Fifth Amendment protects both “verbal and nonverbal conduct,” *Pennsylvania v. Muniz*, 496 U.S. 582, 595 n. 9 (1990), privileging all communications that require a person to use “the contents of his own mind.” *Hubbell*, 530 U.S. at 43 (citing *Curcio*, 354 U.S. at 128); *see Muniz*, 496 U.S. at 595 (Fifth Amendment right spares an accused from “having to share his thoughts and beliefs with the Government”).

Even routine questions that may not directly incriminate are privileged. In *Muniz*, 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 could not be compelled to answer a question regarding the date of his birthday. It would be trivial for the police to determine the suspect’s birthdate, and the date itself was not directly incriminating. And being forced to try to recall it would only lead to an incriminating inference that the suspect was intoxicated (if he could not, in fact, recall it). Nevertheless, the Supreme Court held that the police could not force the suspect to speak his birthdate. The distinction between counting from one to nine and disclosing the birthday follows from the rule that the Fifth Amendment privilege protects both “thoughts” and “beliefs.” *Id.* at 595. *Accord Curcio*, 354 U.S. 118 (custodian of records could not be compelled to answer questions about whereabouts of books and records he failed to produce).

Any contrary rule would have drastic consequences for the values that the

Fifth Amendment privilege against self-incrimination was meant to safeguard. It would be pure spectacle, and an affront to human dignity, to permit the prosecution to force an accused to answer incriminating questions or make confessions of guilt—in a police station, or in court—merely because the authorities believed they already had reliable information concerning the answer. *See, e.g., Muniz*, 496 U.S. at 596 (Fifth Amendment prevents cruelty “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”). The privilege is not just about information, let alone information useful to the prosecution—it is about a core of individual autonomy into which the state may not encroach. *See, e.g., United States v. Nobles*, 422 U.S. 225, 233 (1975) (“The Fifth Amendment privilege against compulsory self-incrimination is an ‘intimate and personal one,’ which protects ‘a private inner sanctum of individual feeling and thought and proscribes state intrusion to extract self-condemnation.’” (quoting *Couch*, 409 U.S. at 327)).

Disclosure of memorized passwords is precisely the type of testimonial communication that is protected by the Fifth Amendment. *See G.A.Q.L. v. State*, 2018 WL 5291918 (Fla. 4th Dist. Ct. App., Oct. 24, 2018); *Seo v. State*, 109 N.E.3d 418 (Ind. Ct. App. 2018); *Commonwealth v. Baust*, 89 Va. Cir. 267 (4th Jud. Cir. 2014) (“[P]roduction of a password forces the Defendant to ‘disclose the

contents of his own mind.”); *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (quashing subpoena for computer passwords; under *Hubbell* and *Doe*, the subpoena would have required the suspect “to divulge through his mental processes his password”); *In re Boucher*, 2007 WL 4246473 (D. Vt. Nov. 29, 2007) (Magistrate Judge op.), *rev’d on other grounds*, 2009 WL 424718 (D. Vt. Feb. 19, 2009).⁵ Compelling appellant to disclose his password—whether orally or in writing—would require him to remember and disclose a fact held in his mind. Without exception, the privilege against self-incrimination does not allow the Commonwealth to compel him to do so.

B. Even an Order Compelling Appellant to Decrypt his Computer by Entering his Password Himself Would Violate the Fifth Amendment Because the Self-Incrimination Privilege Applies to Non-Verbal Acts that Require the Witness’s Mental Capacity to Perform.

The Superior Court order under review would force appellant Davis to testify as to information stored in his memory. This is both unprecedented and unconstitutional. Even if the Commonwealth had obtained an order compelling appellant to physically enter his password into the computer to decrypt the device

⁵ Even courts that have misapplied the “foregone conclusion” rationale to the compelled production of computer passwords in other respects (an argument discussed below) have acknowledged that “the government could not compel [the target of the inquiry] to state the password itself, whether orally or in writing.” *United States v. Spencer*, 2018 WL 1964588, at *2 (N.D. Cal. Apr. 26, 2018).

and then allow the prosecution access to the information stored there (rather than compelling him to speak or write down his password), as in some other similar cases, such an order would violate the Fifth Amendment privilege against self-incrimination. First, that particular type of compelled act would constitute a modern form of written testimony, which is categorically protected by the Fifth Amendment for the reasons stated above. *See* Point I.A *ante*. Second, even if the Court would view that type of demand as one for action rather than for written testimony, it is protected because appellant is incapable of entering his password into the computer without using the contents of his mind, and such “acts of production” are subject to the Fifth Amendment privilege.

The Fifth Amendment protects not just against compelled written and oral testimony, but certain nonverbal acts as well. It is true that “mere physical act[s]” are not testimonial for the purposes of the right against self-incrimination if they do not express or rely on the contents of a person’s mind. *Hubbell*, 530 U.S. at 43. Illustratively, the Supreme Court has held that wearing a particular shirt, providing a blood sample, or providing a handwriting exemplar do not require a suspect to express or reveal information reposing in his brain. *See, e.g., 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). Even physical acts involving speaking may be unprotected, if they do not involve original thinking. *See Muniz*,

supra (requirement to count); *United States v. Dionisio*, 410 U.S. 1 (1973)

(compulsion to provide voice exemplar, where subject does not decide what words to speak).

In contrast, however, even a non-verbal or non-written communication is testimonial for Fifth Amendment purposes if it constitutes an “expression of the contents of an individual’s mind.” *Doe I*, 487 U.S. at 209–210 n. 9. Nonverbal conduct contains a testimonial component whenever the conduct reflects the actor’s communication of his thoughts to another. *Muniz*, 496 U.S. at 595 n.9. Such physical acts are testimonial (and protected by the Fifth Amendment) because they communicate a particular message whose genesis resides within the individual’s mind. *Doe I*, 487 U.S. at 210 n.9; *Braswell v. United States*, 487 U.S. 99, 126 (1988) (Kennedy, J., dissenting) (“Physical acts will constitute testimony if they probe the state of mind, memory, perception, or cognition of the witness.”). “A nod or head-shake is as much a ‘testimonial’ or ‘communicative’ act in this sense as are spoken words.” *Schmerber*, 384 U.S. at 761 n. 5. A witness cannot be compelled to perform these “testimonial acts” under the Fifth Amendment.

In *Hubbell*, the government subpoenaed a large number of documents. The witness asserted a Fifth Amendment right not to produce them. The government argued that it was asking only for “a simple physical act—the act of producing the documents.” 530 U.S. at 43. Characterizing that view as “anemic,” the Court held

that “it was unquestionably necessary for respondent 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.* “The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox.” *Id.*, citing *Doe I*, 487 U.S. at 210.

An act of production may also be testimonial in nature if it would be tantamount to testimony of the witness’s knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the documents. He may also by implication authenticate them. Under these circumstances, the “communicative aspects” are testimonial and privileged under the Fifth Amendment. In *Fisher*, the Supreme Court explained how the act of disclosing documents could be protected by the Fifth Amendment, even if it did not involve the disclosure of the contents of the witness’ mind. 425 U.S. at 408. There, the IRS demanded that two taxpayers produce incriminating documents. The defendants challenged the administrative summons, claiming that the content of the documents was incriminating and therefore protected by the Fifth Amendment. The Court in *Fisher* found that a demand for preexisting documents generally does not run afoul of the Fifth Amendment because it does not compel testimony, but only papers that

were previously voluntarily created. *Id.* at 409–10.⁶ Nevertheless, the Court held that complying with the summons had “communicative aspects of its own”—tacitly revealing the “existence of the papers demanded and their possession or control” by the suspect. *Fisher*, 425 U.S. at 410. These communicative aspects were sufficient to invoke the Fifth Amendment’s protection against the compelled disclosure of testimonial information.

The entry of a computer password to decrypt an electronic device—again, an issue not presented by this appeal—is much more akin to “telling an inquisitor the combination to a wall safe” (*Hubbell*, 530 U.S. at 43, citing *Doe I*, 487 U.S. at 210) because it requires him to reveal information stored in his mind. Indeed, in a case highly similar to this one, the Eleventh Circuit applied the principle in *Hubbell* to hold that entering a password the suspect has memorized is testimonial. *See, e.g., In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012) (hereinafter *Doe II*).

In *Doe II*, the government suspected the defendant was sharing child pornography. Law enforcement executed a search warrant and seized seven encrypted devices. In response to the government’s demand that the defendant recall and use his password to decrypt the devices, the Eleventh Circuit held that

⁶ In reaching this holding, the Court overruled a venerable and historically grounded landmark precedent, *Boyd*, 116 U.S. 616.

“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.” *Doe II*, 670 F.3d at 1346. In similar cases, other courts have agreed. *See Kirschner*, 823 F. Supp. 2d at 669.

As the Indiana Court of Appeals recently explained in *Seo*, compelled decryption is testimonial for an additional reason: it involves a translation of information for law enforcement:

Furthermore, we consider Seo’s act of unlocking, and therefore decrypting the contents of her phone, to be testimonial not simply because the passcode is akin to the combination to a wall safe as discussed in *Doe*. We also consider it testimonial because her act of unlocking, and thereby decrypting, her phone effectively recreates the files sought by the State. As discussed above, when the contents of a phone, or any other storage device, are encrypted, the cyphertext is unintelligible, indistinguishable from random noise. In a very real sense, the files do not exist on the phone in any meaningful way until the passcode is entered and the files sought are decrypted. Thus, compelling Seo to unlock her phone goes far beyond the mere production of paper documents at issue in *Fisher*, *Doe*, or *Hubbell*. Because compelling Seo to unlock her phone compels her to literally recreate the information the State is seeking, we consider this recreation of digital information to be more testimonial in nature than the mere production of paper documents.

Seo, 109 N.E.3d at 431.

Unsurprisingly, courts have refused to compel defendants to produce evidence in similar contexts. For example, in *United States v. Green*, 272 F.3d 748 (5th Cir. 2001), one arresting officer requested that the suspect enter a combination lock to unlock a briefcase and a safe. Inside were multiple weapons. The suspect

was then charged with being a felon illegally in possession of firearms. On appeal, he challenged the prosecution's use of his unlocking of the safe and briefcase on Fifth Amendment grounds. The government argued that the defendant's act of opening the combination locks was non-testimonial. The Fifth Circuit soundly rejected this argument:

Supreme Court precedent forecloses any argument that [the defendant's] directing the agents to the two cases containing firearms and opening the combination locks were not testimonial acts.

In *Doe v. United States*, the majority implicitly held that this precise behavior was testimonial communication so expressing the defendant's mind as to constitute compelled self-incriminatory statements. There is no serious question but that Green's actions in disclosing the locations and opening the combination locks of the cases containing firearms were testimonial and communicative in nature. These compelled acts disclosed Green's knowledge of the presence of firearms in these cases and of the means of opening these cases.

Id. at 753 (citations omitted).

Appellant's password that will unlock data on his computer is no different from a combination that unlocks a briefcase or a safe. Like that combination, entering a password would be a testimonial communication expressing the appellant's mind. Here, as in *Green*, this Court can readily dismiss the Superior Court assertion that entering a passcode is *not* testimonial. That conclusion is foreclosed by Supreme Court precedent, specifically *Doe I*, and there is "no serious question" that it could be otherwise.

Appellant’s password exists in his mind. No governmental authority can lawfully require him, by word or by deed, to remember the password, nor to reveal it. A person’s thoughts and knowledge are at the core of Fifth Amendment privilege.

C. The “Foregone Conclusion” Rationale Does Not Apply to the Compelled Disclosure or Entry of Computer Passwords to Decrypt Electronic Devices.

The Superior Court improperly relied on a theory of “foregone conclusion” to conclude that Mr. Davis’ compelled recitation of his memorized password raises no Fifth Amendment concerns. *See* Appendix A. The court’s reliance on the so-called “foregone conclusion” inquiry to defeat Mr. Davis’s testimonial privilege was wholly misplaced.

The Superior Court order asserts that the U.S. Supreme Court case of *Fisher* supports its application of a “foregone conclusion” rationale to Appellant’s case. 176 A.3d at 875. But a closer look at *Fisher* shows that that conclusion is mistaken. The facts of *Fisher* were highly unusual, and do not support a “foregone conclusion” exception to the privilege against self-incrimination. Other than *Fisher*, the Supreme Court has never since upheld a “foregone conclusion” rationale. The lower courts that have relied on “foregone conclusion” to defeat an individual’s Fifth Amendment rights have done so in error.

Fisher arose out of a tax investigation. The taxpayers' accountants had prepared documents related to the preparation of tax returns. The accountants then gave the documents that they had created to the taxpayers, who passed them along to the taxpayers' attorneys. The IRS then served administrative summonses on the accountants.⁷ Notably, the people asserting the privilege neither created nor possessed the documents in question. Understandably, these idiosyncratic facts occupy most of the Court's analysis. The taxpayers were neither compelled to create the documents, nor were they personally compelled to turn them over.

The question before the Supreme Court was whether the attorneys, as agents of the taxpayer, could be forced to produce the documents. All parties agreed that if the taxpayers were privileged under the Fifth Amendment from disclosure, then their attorneys—by operation of the attorney-client privilege—could not be compelled either. The order, noted the Court, did not compel oral testimony, as the Superior Court order here does. Nor did the order implicitly compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought. The taxpayer was not competent to authenticate the papers, anyhow. 425 U.S. at 413. Since the accountants prepared the papers and could independently authenticate

⁷ The federal courts, unlike Pennsylvania, do not recognize any accountant-client privilege. See *United States v. Arthur Young & Co.*, 465 U.S. 805, 817 (1984); *Couch*, 409 U.S. at 335.

them, “the Government is in no way relying on the ‘truth-telling’ of the taxpayer to prove the existence of or his access to the documents.” *Id.* at 411.

In sum, *Fisher* stands for the proposition that where (1) the target of an investigation is not being asked for testimony, (2) the target neither created nor possesses the documents sought, (3) there is an independent source for the papers, and (4) the prosecution is not relying on the witness’s truth-telling to authenticate the documents, then the state learns nothing from the target’s disclosure of those papers. In other words, in such circumstances, the information tacitly communicated by the act of production is a “foregone conclusion,” and the act compelled does not rise to the level of Fifth Amendment protection. Needless to say, these facts are utterly absent in this case. The Superior Court demands that appellant testify as to a password he created for a computer that he purportedly controls, and the Commonwealth is entirely reliant on appellant telling the truth about what he recalls his password to be. *Fisher* in no way supports application of a “foregone conclusion” theory here.

Since *Fisher*, the Supreme Court has never held that an act of disclosure is unprotected by the Fifth Amendment because its implicit messages are a foregone conclusion. To the contrary, in only one other case did the Court even consider whether the testimonial aspects of an act of disclosure are a foregone conclusion, and it rejected that argument. *Hubbell*, 530 U.S. at 33–34. In *Hubbell*, the Supreme

Court revisited *Fisher*, firmly rejecting the government’s bid to expand the “foregone conclusion” exception to a new context.

There, the Court held that a witness could not be compelled to produce papers where it would require him “to make extensive use of the contents of his own mind in identifying the hundreds of documents responsive to the requests in the subpoenas.” *Id.* at 40. The government could not take advantage of the narrow foregone conclusion exception established in *Fisher* to compel mental processes or disclosure of thoughts and knowledge. The “prosecutor needed respondent’s assistance both to identify potential sources of information and to produce those sources.” *Id.* at 41. And that assistance would require the defendant to make “mental and physical steps” to provide a “truthful” response that would lead the prosecutors to incriminating evidence. *Id.* at 42. The Court had “no doubt” that the Fifth Amendment prohibited the government from compelling that assistance, and that the narrow “foregone conclusion” exception established in *Fisher* did not apply. *Id.* at 43–45.

Some lower courts have held that, where the mere act of production of documents has communicative aspects separate from the witness’s cognition, the state may—again, in narrow circumstances—be able to overcome the invocation of a privilege against self-incrimination if it already knows everything the act of production would reveal. But those courts have overwhelmingly been ruling in

cases concerning the compelled production of business and other financial records. *See, e.g., United States v. Sideman & Bancroft, LLP*, 704 F.3d 1197, 1200 (9th Cir. 2013) (production of business and tax records); *In re Grand Jury Subpoenas Served Feb 27, 1984*, 599 F. Supp. 1006, 1012 (E.D. Wash. 1984) (records related to business partnership). “Whatever the scope of this ‘foregone conclusion’ rationale,” *Hubbell*, 530 U.S. at 44, expanding it beyond its narrow application to the act of production of documents would greatly erode the self-incrimination privilege.

The court in *Goldsmith v. Superior Court*, 152 Cal. App. 3d 76 (1984)—another case reversing an order compelling the production of a weapon allegedly used in a crime—identified the broader problem with orders like the one the Commonwealth seeks here:

Implicit in the prosecution’s position ... is the argument that independent evidence establishes defendant’s possession of the gun at the time of the offense and after [... , and therefore] the evidence is unworthy of Fifth Amendment protection. ... The [prosecution’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, 152 Cal. App. 3d at 87 n.12 (quotations and citations omitted).

The Superior Court below adopted just such a “curious” argument, articulating a rule that would allow testimony to be compelled once the State has

satisfied an amorphous evidentiary standard. *See* Appendix A. That approach represents a serious departure from the traditional conception of the self-incrimination privilege.

D. Even if the “Foregone Conclusion” Rationale Could Apply to the Compelled Decryption of a Computer, the Commonwealth Cannot Satisfy It Here.

According to the Supreme Court of the United States, a “foregone conclusion” exists only when the resulting act of production “adds little or nothing to the sum total of the Government’s information.” *Fisher*, 425 U.S. at 411. For this rationale to apply, all the facts suggested by that production must be already known to the government. In *Fisher*, it was a “truism” and “self-evident” that the taxpayer under investigation had access to those documents because, “the Government already knew that the documents were in the attorneys’ possession and could independently confirm their existence and authenticity through the accountants who created them.” *Hubbell*, 530 U.S. at 44–45. And in *Hubbell*, “the Government [had] not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent.” *Id.* at 45. These are plainly bars that are exceedingly difficult to scale.

Though the U.S. Supreme Court has never endorsed it, some courts have articulated a “foregone conclusion” analysis that asks whether law enforcement

agents know with “reasonable particularity” the location, existence, and authenticity of the evidence sought. *See, e.g., United States v. Ponds*, 454 F.3d 313 (D.C. Cir. 2006); *In re Grand Jury Subpoena Dated April 18, 2003*, 383 F.3d 905 (9th Cir. 2004). Even if that articulation is correct, a misapplication of it in the context of compelled decryption would thoroughly undermine the Fifth Amendment privilege. Some courts have argued that all the “reasonable particularity” rubric means, in the context of compelled decryption, is that “the government need only show it is a foregone conclusion that [an accused] has the ability to decrypt the device[.]” *Spencer, supra* note 5, 2018 WL 1964588 at *3. But it would be inconsistent with the Supreme Court’s discussions of “foregone conclusion” to reduce the inquiry to one in which the only information at stake is so limited. *See Seo*, 109 N.E.3d at 434 (“What is being compelled here is not merely the passcode... but the entire contents of” the device.).

Indeed, it is not merely the device whose location, existence, and authenticity the government seeks to know through a compelled act—it is also, in fact principally, that of the *files* on that device. While access to an encrypted device is an initial step, the Fifth Amendment privilege “not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a *link in the chain of evidence* needed to prosecute the claimant for a federal crime.” *Hoffman*, 341 U.S. at 486

(emphasis added). And the compelled entry of a password to decrypt a digital device would lead to an unknown number of potentially incriminating files—files that, on a simplistic theory of “foregone conclusion,” the accused would have been forced to deliver directly to prosecutors by using the contents of his mind.

Courts that have applied the “reasonable particularity” rubric in the context of compelled decryption have recognized as much. Rather than accept claims that the government knows with reasonable particularity whether an accused possesses and controls a *device*, these courts require that the government “be able to describe with reasonable particularity the *discrete* contents on” that device. *Seo*, 109 N.E. 3d at 434; *see United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3d Cir. 2017) (“[T]he Government has provided evidence to show both that files exist on the encrypted portions of the devices and that Doe can access them,” citing *Doe II*, 670 F.3d at 1348–49). While these courts may not require that the government have a complete and total inventory of a device’s contents, they do demand that it “be able to demonstrate some knowledge that files do exist on the encrypted devices.” *Apple MacPro*, 851 F.3d at 248; *see Seo*, 109 N.E.3d at 434; *Doe II*, 670 F.3d at 1349 (explaining that the government had failed the “foregone conclusion” analysis because it had not “shown a basis with reasonable particularity . . . that encrypted *files* exist on the drives” (emphasis added)).

On the record of this case, the “foregone conclusion” theory would not properly justify an order to provide the password. It is not a “foregone conclusion” that Mr. Davis even knows the password at this time. If, as the agents say he once claimed, it is 64 characters long, and even if he once knew that very long string of digits, letters and/or characters by heart (as an agent testified he once said), it is by no means certain that he remembers it accurately after three years in jail with no occasion to use it. Presumably the password is or was once written down somewhere, but the record reveals nothing on that score. And even if Mr. Davis said once (in October 2015) that he knew the password, R.39a (*see also* R.40a), he later claimed that he no longer remembered it. (R.41a). In short, even if there is a valid “foregone conclusion” to invoke, if that inquiry applies to knowledge of the password, it is not “foregone” that Mr. Davis knows it.

Likewise, even if the “foregone conclusion” inquiry goes to the presence of contraband on the seized computer (as some of the cases discussed above would suggest), that too, is less than “foregone” on the present record. Agent Cook, the forensic technician, admitted that he could not tell what might be on the seized computer. (R.45a). When the search party arrived, the computer was not connected to the Internet at all. (R.43a–44a). There is simply no proof that the device they seized is the one used to share videos on eMule. Accordingly, the lower courts’

“foregone conclusion” rationale is not only legally erroneous under the Fifth Amendment, it is also factually inapt.

II. The Self-Incrimination Privilege Enshrined in Article I, Section 9 of the Pennsylvania Constitution, Independently Protects Appellant Davis from Compulsion to Reveal the Password for his Encrypted Computer, Notwithstanding Any Conclusion this Court May Reach under the United States Constitution.

Granting the Commonwealth’s pretrial motion to compel, the trial court ordered the defendant, Joseph Davis, to “supply the Commonwealth with any and all passwords used to access the HP Envoy 700 desktop computer...” Appendix B; R.56a. On interlocutory appeal, the Superior Court upheld this order over Mr. Davis’s objection that it violated his state and federal constitutional rights to be free from compulsory self-incrimination. For all the reasons explained under Point I of this brief, the Superior Court erred in holding that this order did not violate the Fifth Amendment to the U.S. Constitution, and in particular in applying the “act of production” doctrine and its “foregone conclusion” exception, as articulated and applied by the Supreme Court of the United States in its 1976 *Fisher* decision. But this Court rightly allowed the present appeal to consider not only the federal question but also whether Article I, Section 9, of the Pennsylvania Constitution independently protects Mr. Davis from complying with the trial court’s order. The Court should now hold that it does.

Even if this Court reverses on federal constitutional grounds, as it should, the Court should nevertheless proceed to address the state constitutional issue. Doing so would ensure the finality of its decision in this case. *See Commonwealth v. Muniz*, 640 Pa. 699, 164 A.3d 1189, 1219 (2017) (holding SORNA unconstitutional under both state and federal *Ex Post Facto* clauses; noting that independent state constitutional ruling protects against potentially time-wasting appeal to the U.S. Supreme Court).⁸ That approach would be particularly just here, as it would avoid further delay. This criminal case has already lingered, with the defendant detained in jail, for more than three years since his arrest on October 20, 2015. *See R.R.1*. And of course, if this Court were to rule adversely to appellant Davis on the federal question, it would be obliged to reach and decide the state constitutional issue.

Alternatively, the Court might choose to avoid deciding exactly what the contours and present viability of the Fifth Amendment *Fisher* holding may be (and in particular its “foregone conclusion” rationale), as applied to the novel circumstances of the present case. “When the federal constitutional jurisprudence has been unclear or in a state of flux, ‘this Court has not hesitated to render its inde-

⁸ This protection of the judgment applies, however, only if this Court makes clear by “plain statement” that its interpretation of the state constitution is “independent” of federal doctrine. *See Michigan v. Long*, 463 U.S. 1032, 1041–42 (1983).

pendent judgment as a matter of distinct and enforceable Pennsylvania constitutional law.” *Commonwealth v. Molina*, 628 Pa. 465, 104 A.3d 430, 441 (2014) (opinion for 3 of 5 participating Justices), quoting *Pap’s A.M. v. City of Erie*, 571 Pa. 375, 812 A.2d 591, 607 (2002).

The order issued by the trial court in this case requires disclosure, for the benefit of the prosecutor, of the previously-unrecorded contents of the defendant’s own mind. For the reasons elaborated in this Point of appellant’s brief, the text and history of Pennsylvania’s own, pre-existing Self-Incrimination Clause, found in Article I, Section 9, of the State Constitution – as reflected in some 215 years of this Court’s precedent and over 300 years of deeply principled tradition – absolutely prohibits any such order. Section 9 provides, in pertinent part: “In all criminal prosecutions, the accused ... cannot be compelled to give evidence against himself”⁹

Even if the trial court’s order were wrongly viewed, as the Superior Court seemingly understood it, as requiring a physical act rather than a mental and verbal disclosure, this Court has never approved, under our state’s Constitution, the federal “act of production” limitation on the Fifth Amendment’s protection for compulsory disclosure of the defendant’s pre-existing papers, much less the dubious and ill-defined “foregone conclusion” exception to that doctrine, and

⁹ The 1776 and 1790 wording was very slightly (but immaterially) different.

Article I, Section 9, should not be interpreted now to allow it.¹⁰ The Pennsylvania Constitution provides a sound, independent and appropriate basis for entering a judgment reversing the Superior Court’s erroneous decision in this case.

The Superior Court casually dismissed the independent state constitutional issue in this case by asserting that interpretation of Article I, Section 9, simply apes Fifth Amendment case law, citing unfortunate, overstated dictum in one of this Court’s decisions. *See* 176 A.3d at 874 n.6, quoting *Knoble*, 42 A.3d at 979 n.2. But the *Knoble* footnote was applicable only to the narrow issue then before the Court, and such comments were rejected as “overstate[d]” in *Molina*, 104 A.3d at 443. *See also Commonwealth v. Cooley*, 632 Pa. 119, 118 A.3d 370, 375 n.8 (2015) (quoting same language from *Knoble* without further analysis or appropriate limitation); *Molina*, 104 A.3d at 444 (noting additional, occasional suggestions that the state privilege only “tracks the protection afforded under the Fifth Amendment,” quoting *Commonwealth v. Arroyo*, 555 Pa. 125, 723 A.2d 162, 166 (1999) (addressing right to counsel under Art. I, § 9)). An examination of this

¹⁰ As explained under Point I.C. above, the Superior Court grievously misapplied the “foregone conclusion” concept, when it held “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.” 176 A.3d at 875–76. Because that which was directed to be disclosed is held only in the defendant’s mind, the incriminating potential of the mere “act of disclosing” is not what is at issue.

Court's self-incrimination jurisprudence shows that the Superior Court was quite wrong in its holding under the Pennsylvania Constitution.

Prior to the U.S. Supreme Court's recognition in 1965 that the Fourteenth Amendment "incorporated" the protection of the Fifth Amendment privilege and thus made it enforceable in state cases, all of this Court's self-incrimination decisions were necessarily "independent" of federal law.¹¹ And in the half-century since then, this Court has often continued to decide important self-incrimination issues by making an independent analysis under Article I, Section 9. *See, e.g., Molina*, 104 A.3d at 441–53 (2014) (scope of permissible use of pre-arrest silence); *Commonwealth v. Swinehart*, 541 Pa. 500, 664 A.2d 957 (1995) (scope of required immunity); *Commonwealth v. Lewis*, 528 Pa. 440, 598 A.2d 975 (1991) (requirement of no-adverse-inference instruction); *D'Elia v. Pennsylvania Crime Comm'n*, 521 Pa. 225, 555 A.2d 864, 867–72 (1989) (extent of required immunity protection); *Commonwealth v. Turner*, 499 Pa. 579, 454 A.2d 537 (1982) (prosecutorial reference to defendant's silence); *Commonwealth v. Triplett*, 462 Pa. 244, 341 A.2d 62 (1975) (use of unwarned but voluntary post-arrest statements to impeach).

¹¹ Ratification of the Fourteenth Amendment in 1868 made the Fifth Amendment privilege applicable to the States, as eventually recognized a century later by the Supreme Court. *See Griffin v. California*, 380 U.S. 609 (1965).

In several of these cases, contrary to the Superior Court’s holding on this issue below, this Court “has specifically concluded that the protections of Section 9 exceed those in its federal counterpart.” *Molina*, 104 A.3d at 444 (citing examples); Leonard Sosnov, *Criminal Procedure Rights Under the Pennsylvania Constitution: Examining the Present and Exploring the Future*, 3 Widener J. Pub. L. 217, 291–309 (1993). The instant case should be another. Applying a proper *Edmunds* analysis,¹² it becomes clear that this Court has never approved the federal notion – first articulated in *Fisher* in 1976 – that production of pre-existing documents can be freely required from a criminal defendant. Nor has this Court ever held that a defendant can be compelled to speak or write the contents of his own private mind and memory on the theory that the matter disclosed “would not communicate facts of a testimonial nature,” as the Superior Court put it, “beyond that which he has already acknowledged to investigating agents.” *See* 176 A.3d at 875–76. Insofar as that could be viewed as a proper application of the “foregone conclusion” theory (which Points I.C. and I.D. of this brief shows it is not), this Court should nevertheless reject it. The Court should not adopt any such limitation and restrictive gloss on the venerable and cherished privilege protected by Article

¹² *See Commonwealth v. Edmunds*, 526 Pa. 374, 586 A.2d 887, 894–95 (1991) (delineating mandated approach for presentation of an independent state constitutional law argument on appeal).

I, Section 9, part of the infeasible Declaration of Rights of our state's own Constitution. *See* Pa. Const., art. 1, § 25 (fundamental rights are “inviolable”).

An *Edmunds* analysis calls for consideration of the text of the two provisions (state and federal), pertinent history and policy factors, and the decisions in other jurisdictions. *See Molina*, 104 A.3d at 441, citing *Pap's A.M.*, 812 A.2d at 603. Upon examination of those points, it becomes apparent that the judgment of the court below must be reversed on state as well as federal law grounds.

A. Constitutional Text

There are differences in the text of Article I, Section 9's self-incrimination clause, as compared with the federal Fifth Amendment, and one of those differences in particular supports a ruling for appellant Davis. As this Court thoroughly discussed in *Molina*, 104 A.3d at 443–44, the text of the self-incrimination privilege enshrined in Pennsylvania's 1776 Declaration of Rights, as last amended in 1838 and last ratified by the voters in 1968,¹³ differs in several respects from the privilege adopted some 15 years later by Congress and ratified as part of the Fifth Amendment to the Constitution of the United States. In particular,

¹³ An additional sentence, not pertinent to the issue under consideration here, was added to Section 9 by the voters in 1984, for the purpose of overruling *Triplett*, 841 A.3d 62. *See Molina*, 104 A.3d at 443. That the Legislature and the People chose to add language rejecting one particular, narrow ruling, rather than amending the Section to require parallel construction with the federal Fifth Amendment in general, can itself be seen as an endorsement of this Court's practice of approving more protective interpretations in other cases.

as applicable here, the Fifth Amendment, by its terms, protects anyone from being “compelled in any criminal case *to be a witness* against himself.” Section Nine, on the other hand, extends protection to an “accused” person against being “compelled *to give evidence* against himself” (emphasis added to each).¹⁴

Under a Fifth Amendment analysis, the Court examines whether the defendant is being compelled “to be a witness.” To answer this question, the Court asks whether the utterance at issue is “testimonial.” *See Muniz*, 496 U.S. at 588–89; *Doe I*, 487 U.S. at 210. As shown under Point I of this brief, a correct application of the *Muniz/Doe* analysis leads to reversal on federal grounds. But even if the Court were to disagree with appellant Davis about the Fifth Amendment, where the national charter forbids compulsion “to be a witness,” the Pennsylvania Constitutional text prohibits compulsion “to give evidence.” By any measure, the order under review here would compel Mr. Davis “to give evidence against himself.”

¹⁴ Appellant Davis in this case stands “accused” of criminal offenses, and information is being demanded from him for use in that very case, so any potential limitation implicit in the focus of Section Nine on “the accused,” as contrasted with the Fifth Amendment’s application to any “person,” is immaterial. That said, this Court has long held that the state constitutional privilege applies to a *witness* who may be exposed to incrimination as well as literally to one who presently stands “accused.” *See Commonwealth v. Fisher (Appeal of Snyder)*, 398 Pa. 237, 157 A.2d 207 (1960). *See also* 42 Pa.C.S. § 5941(a) (self-incrimination privilege for all witnesses in any proceeding). Perhaps reflecting the importance of pre-Revolutionary legal history in the present context, this Court has, by contrast, relied more strictly on the same limitation of Section 9 (rights of “the accused”) when interpreting its separate guarantee of the right to counsel. *See Arroyo*, 723 A.2d at 167 (right to counsel does not attach until time of legal accusation).

“As [this Court has] emphasized ..., ‘[o]ur ultimate touchstone is the actual language of the Constitution itself.’” *Washington v. Dep’t of Pub. Welfare*, 188 A.3d 1135, 1149 (Pa. 2018) (quoting *Stilp v. Commonwealth*, 588 Pa. 539, 905 A.2d 918, 939 (2006) (in turn quoting *Firing v. Kephart*, 466 Pa. 560, 353 A.2d 833, 835-36 (1976)).¹⁵ Compulsion to reveal his memorized password would require Mr. Davis to “give evidence” whether or not that disclosure was technically “testimonial,” as that concept is used under the Fifth Amendment. See Jennifer Friesen, *State Constitutional Law: Litigating Individual Rights, Claims, and Defenses* § 12.02[2], text at n.17 (4th ed. 2008 & 2015 Supp.) (textual distinction between “be a witness” and “give evidence” “potentially broaden[s] the scope of the privilege beyond” limits recognized in U.S. Supreme Court rulings concerning the federal provision).

Taking the wording of the two charters on their face, it can easily be seen that the Pennsylvania Constitution more readily protects Mr. Davis against being compelled to reveal his computer password pretrial than does the federal

¹⁵ See also, e.g., *League of Women Voters v. Commonwealth*, 178 A.3d 737, 802 (Pa. 2018) (“The touchstone of interpretation of a constitutional provision is the actual language of the Constitution itself.” (citation omitted); *Sprague v. Cortes*, 636 Pa. 542, 145 A.3d 1136, 1154 (2016) (Wecht, J., concurring); *Zauflik v. Pennsbury Sch. Dist.*, 629 Pa. 1, 49, 104 A.3d 1096, 1124 (2014) (“[T]he polestar of constitutional analysis undertaken by the Court must be the plain language of the constitutional provisions at issue”) (citation omitted).

Constitution’s reference to protection against being a compulsory “witness.”¹⁶ The Fifth Amendment term “witness” underlies the U.S. Supreme Court’s doctrinaire view that an act must itself be “testimonial” to be privileged. That approach, in turn, led to the creation and application in *Fisher* of the so-called “foregone conclusion” exception to the “act of production” doctrine.

That entire line of reasoning in the Fifth Amendment case law is inconsistent with this Court’s overarching philosophy for construing and applying the words of the Constitution of Pennsylvania:

[I]n interpreting a constitutional provision, we view it as an expression of the popular will of the voters who adopted it, and, thus, construe its language in the manner in which it was understood by those voters. *Stilp*, 905 A.2d at 939; *Commonwealth v. Harmon*, 469 Pa. 490, 366 A.2d 895, 899 (1976). As a result, we do not consider such language in a “technical or strained manner, but are to interpret its words in their popular, natural and ordinary meaning.” *Scarnati [v. Wolf]*, 173 A.3d [1110,] 1118 [(Pa. 2017)]. Accordingly, “we must favor a natural reading which avoids contradictions and difficulties in implementation, which completely conforms to the intent of the framers and which reflects the views of the ratifying voter.” *In re Bruno*, 627 Pa. 505, 101 A.3d 635, 659 (2014) (quoting *Commonwealth ex rel. Paulinski v. Isaac*, 483 Pa. 467, 397 A.2d 760, 766 (1979)).

¹⁶ Some history-minded jurists have cautioned against making too much (or anything) of this particular difference in wording, based on Eighteenth Century usage and the contrast between constitutional interpretation and statutory construction. *See Hubbell*, 530 U.S. at 49–55 (2000) (Thomas & Scalia, JJ., concurring); *see also Carpenter v. United States*, 138 S. Ct. 2206, 2271 (2018) (Gorsuch, J., dissenting) (noting the Thomas/Scalia view with apparent approval).

Washington, 188 A.3d at 1149. *Accord Commonwealth v. Dabbierio*, 290 Pa. 174, 138 A. 679, 680–81 (1927) (applying this interpretative principle to Article I, § 9; holding that a lawful *seizure* of evidence from the accused, whether by warrant or incident to arrest, does not compel him to “give evidence against himself”).

An interpretation of Article I, Section 9, that viewed Mr. Davis’s revealing the password to his computer – whether by speaking it, by writing it down, or even by entering it manually onto a keyboard or screen – as something other than “giving evidence against himself” would be strained, unnatural, and contrary to the ordinary meaning of those words, whether viewed through an Eighteenth Century (1776/1838) or a Twentieth Century (1968) lens. It is therefore necessarily wrong.

Indeed, the Pennsylvania Constitution’s self-incrimination clause in particular has long been viewed, from this Court’s earliest days, not literally or narrowly, but as an expression and affirmation of a pre-Revolutionary evidentiary privilege, known by reference to a Latin maxim: *nemo tenetur prodere seipsum* (no one is obligated to accuse himself). *See Galbreath’s Lessee v. Eichelberger*, 3 Yeates 515, 517 (Pa. 1803) (sustaining objection as “founded in reason and good sense ... and a violation of his privileges as a citizen,” citing what is now Art. I, § 9); *Respublica v. Gibbs*, 3 Yeates 429, 437 (Pa. 1802) (charge of the Court) (also noted *sub nom. Commonwealth v. Gibbs*, 4 U.S. (4 Dallas) 253 (1802)).

The pre-Revolutionary *nemo tenetur* privilege “applied to all stages of all equity and common-law proceedings and to all witnesses as well as to the parties. ... If one’s disclosure could make him vulnerable to legal peril, he could invoke his right to silence. He might even do so if his answers revealed infamy or disgrace yet could not be used against him in a subsequent prosecution.” Leonard W. Levy, *Origins of the Fifth Amendment: The Right Against Self-Incrimination* (2d ed. 1986). As this Court stated nearly a century later: “One of these rights [which no legislation can infringe] is that he [in that case, an alleged debtor] shall not compelled to give evidence that may be used against him in a criminal prosecution, in other words, he may not be compelled to do that which may criminate himself.” *Horstman v. Kaufman*, 97 Pa. 147, 151 (1881).¹⁷ Surely, Mr. Davis has been ordered in this case “to do that which may criminate himself.”

In the Nineteenth Century, consistent with pre-Revolutionary understandings, this Court construed the broad protection against compulsion to “give evidence,” as stated in the Pennsylvania constitutional privilege, to protect a party, for example, against mandatory production of documents that may be used to support penal consequences. *See Boyle v. Smithman*, 146 Pa. 255, 23 A. 397,

¹⁷ *Horstman* has been referred to by one scholar as “[t]he leading American case on the exclusionary aspect ... of the privilege against self-incrimination.” Henry E. Smith, *The Modern Privilege: Its Nineteenth Century Origins in The Privilege Against Self-Incrimination: Its Origins and Development* (R.H. Helmholz *et al.*, eds., 1997).

397 (1892). That interpretation has never been overruled.¹⁸ This aspect of *nemo tenetur* dates at least to the landmark British case of *Entick v. Carrington* (1765),¹⁹ arising out of the trial of John Wilkes for seditious libel. Chief Justice Shippen alluded to the same aspect of the privilege in *Gibbs*, this Court’s first self-incrimination opinion. 3 Yeates at 437 (“so jealous have the legislature of this commonwealth been, of this mode of discovery of facts, that they refused their assent to a bill...to compel persons to disclose on oath, papers as well as facts...”); *see also Commonwealth v. Valeroso*, 273 Pa. 213, 116 A. 828 (1922) (defendant cannot be called upon in open court to produce an incriminating record).²⁰

Similarly, in the Twentieth Century this Court properly described the right protected by Section 9 as more than a right to refrain from testifying, but as “protecting silence as well as overt self-incrimination.” *Molina*, 104 A.3d at 446,

¹⁸ In *McElree v. Darlington*, 187 Pa. 593, 41 A. 456 (1898), this Court clarified that a defendant was not protected by the Constitution from an order to allow examination of corporate books and records he had prepared, but which were not his own papers.

¹⁹ 19 How. St. Tr. 1029, 1073 (1813 ed.) (“any forcible and compulsory extortion of a man’s own testimony or of his private papers to be used as evidence to convict him of crime ... is within the condemnation of that judgment [*i.e.*, *Entick*],” at 630).

²⁰ In this decision, striking down a statute requiring a debtor to reveal under oath the whereabouts of allegedly concealed property, the Court distinguished its earlier precedent of *Commonwealth v. Johnson*, 115 Pa. 369, 9 A. 78, 81 (1887), which held that Article I, Section 9, was not violated when the defendant in a murder case was directed to stand and demonstrate the sound of his voice by repeating certain words, to allow identification by a Commonwealth witness.

discussing *Commonwealth v. Dravec*, 424 Pa. 582, 227 A.2d 904 (1967) (plurality op.). Rejection of the Superior Court’s stilted view of the privilege would thus be consistent with the language of Article I, Section 9, as construed by this Court for more than 215 years.

For these reasons, while “the textual distinctions between Section 9 and the Fifth Amendment do not definitively speak to the issue before the Court,” *Molina*, 104 A.3d at 444, the language of the Pennsylvania Constitution contributes strongly to a conclusion that Mr. Davis cannot be compelled to reveal the password to his encrypted computer.

B. History and Policy

The foregoing discussion of the state Constitution’s text and this Court’s case law has already touched on questions of history and policy, as implicated by an *Edmunds* analysis. But there is more. Pennsylvania’s 1776 Declaration of Rights was the second of the former colonies’ to be adopted after Independence. Much of its wording was taken from George Mason’s draft, which had just been adopted in Virginia, with edits at the Pennsylvania convention by Benjamin Franklin. Pennsylvania, like Virginia, included the privilege among an interrelated bundle of rights associated with a fair trial by jury in criminal cases.²¹ *See Eben*

²¹ The federal text, by contrast, was drafted years later by James Madison. He not only used different terminology, but also included it in a grab bag of miscellaneous and general fair

Moglen, *The Privilege in British North America: The Colonial Period to the Fifth Amendment* in Helmholz *et al.*, *supra* note 17, at 134–35.²²

Franklin’s interest in the privilege dated back at least four decades. He had authored and published a series of three popular pamphlets in 1735 in defense of Samuel Hemphill, who was convicted of heresy in Philadelphia based in part on an adverse inference drawn from his refusal to submit his sermons for inspection.²³ Franklin declared this process “contrary to the common Rights of Mankind, no Man being obliged to furnish Matter of Accusation against himself.” Levy, *supra* at 382–83.²⁴

Pennsylvania could hardly have omitted this protection from its Declaration of Rights, considering the experience of its founder. William Penn had been tried with a co-defendant at Old Bailey in 1670 for holding Quaker Meeting in the street without a permit. They were famously denied the right to a fair trial. Among those

process rights (Fifth Amendment), not among the trial rights of the accused (federal Sixth Amendment), as in Virginia and Pennsylvania.

²² Seven of the original thirteen colonies, plus Vermont (which was independent until 1791), included an explicit self-incrimination protection in their founding Constitutions, all similar to Virginia and Pennsylvania’s. *See* Levy, *supra*, at 409–10 (citing Virginia, Pennsylvania, Delaware, Maryland, North Carolina, Vermont, Massachusetts, and New Hampshire).

²³ Hemphill, like Franklin, was a Presbyterian deist, more interested in principles of good government than in Biblical exegesis. *See* Levy, *supra*, at 383.

²⁴ Levy responded to certain criticisms that Moglen leveled against his treatise in *Origins of the Fifth Amendment and Its Critics*, 19 Cardozo L.Rev. 821, 849–59 (1997). None of the two historians’ differences about the colonial period is material to the issue before this Court in the present case.

outrages was a direct inquiry from the judge at trial to Penn's co-defendant, Mead, as to whether he had been present at the unlawful assembly. Mead invoked the common law privilege, leading the judge to rebuke him before the jury and to banish Mead from their sight and to prevent him from questioning the witnesses.²⁵ Perhaps recalling this incident, the Charter of Privileges granted by Penn in 1701 to the inhabitants of Pennsylvania promised, in Section 5, that "all Criminals shall have the same Privileges of Witnesses and Council [sic] as their Prosecutors." *See, e.g.,* Moglen, *supra*, at 257 n.95.²⁶

From the beginning, this Court has interpreted the self-incrimination clause of Section 9 exceedingly broadly. In *Gibbs*, the first case (1802), the defendant was charged with assault and interfering with an election based on his angry response to an inspector of elections who demanded to know, from the defendant's father who was present with him to vote, whether he had sworn an oath of allegiance to the Crown during the Revolution. This Court (sitting as a trial court) instructed the jury that having been disloyal would not actually disqualify the elder Gibbs from voting, but would "involve him in shame or reproach," thus giving rise to a right not to answer. And if he had been unlawfully directed to answer, on pain of being

²⁵ *The Trial of William Penn and William Mead*, 6 How. St. Tr. (1670) 951, 957 (invocation of privilege), 960 (Mead's banishment to "bale-dock") (1816 ed.) (No. 230).

²⁶ The full text of Pennsylvania's Charter may be found, *inter alia*, at http://avalon.law.yale.edu/18th_century/pa07.asp (last visited Nov. 16, 2018).

denied his right to vote, then if “the election was obstructed or interrupted, it seems most reasonable to attribute it to [the inspectors]” rather than to the defendant. 3 Yeates at 437. So instructed, the jury returned a verdict of Not Guilty. *Id.* at 438.

In the *Galbreath* case the next year, the Court held that both the common law privilege and the state Constitution conferred on a witness in a civil action over a land title the privilege to refuse even to be sworn for examination on the subject of whether he had acquired the title from his father by fraud, for which he might at some later time be indicted. 3 Yeates at 516–17. And even if “an indictment would not lie against the witness...yet the combination itself was nefarious and immoral, and would justly subject every person concerned in it to ignominy and contempt, and was therefore within the construction of the maxim,” *id.* at 517, citing *Gibbs*, as well as Article I § 9. The privilege against being compelled to “give evidence,” in other words, was held to protect him from being made a witness at all, and not just to protect him from answering specific incriminating questions.²⁷

²⁷ The Court overruled that holding in *In re Eckstein*, 148 Pa. 509, 24 A. 63 (1892) (per curiam), declaring that a witness, other than a criminal defendant, must appear and take the oath, and may then interpose a privilege objection to any particular question that she views as having the potential to incriminate. *See also* 42 Pa.C.S. § 5941(a). The *Eckstein* Court did not overrule the broad reading of “incriminate,” however, as also reaching questions that would subject the witness to ignominy, obloquy, infamy, disgrace, shame, ill repute, or reproach.

Against this historical backdrop, it is unsurprising that this Court has recognized the privilege under Section 9 as “the ‘crown jewel’ of all rights afforded the accused under federal and state constitutions.” *Molina*, 104 A.3d at 446, quoting Ken Gormley, *The Pennsylvania Constitution: A Treatise on Rights and Liberties* § 12.6[a], at 386 (2004). In the same spirit, future Justice Abe Fortas wrote, in response to abuses of the McCarthy period:

[I]n the course of man’s battle for his individual sanctity, history has given preferred position to the individual’s right to defend himself by withholding incriminating evidence. This right is not subject to defeasance upon a showing of probable cause, as is a man’s right to be protected against search of his household and person.

The fundamental value that the privilege reflects is intangible, it is true; but so is liberty, and so is man’s immortal soul. A man may be punished, even put to death, by the state, but if he is an American or an Englishman, or a free man anywhere, he should not be made to prostrate himself before its majesty. Mea culpa belongs to a man and his God. It is a plea that cannot be extracted from free men by human authority. To require it is to insist that the state is the superior of the individuals who compose it, instead of their instrument.

Abe Fortas, *The Fifth Amendment: Nemo Tenetur Prodere Seipsum*, 25 J.

Cleveland Bar Ass’n 91, 99–100 (1954). No better explication of the Enlightenment political and moral philosophy that lies behind the privilege has ever been penned.

The first great scholar of the state Constitution characterized Article I, Section 9, as ensuring that “an accused person cannot be convicted by a process of inquisition.” Thomas Raeburn White, *Commentaries on the Constitution of*

Pennsylvania 104 (1907). In other words, “[N]o person can be compelled to answer any question put to him, either in a civil or criminal proceeding, if the reply might, in the opinion of the trial judge, tend to show him to be guilty of a crime, or even which might subject him to ignominy and contempt.” *Id.* at 104–05 (footnotes omitted). For these same reasons, “this Court has long protected a defendant’s silence as part of the right against self-incrimination.” *Molina*, 104 A.3d at 447. Mr. Davis’s ancient right to silence and to be free from having to aid in his own conviction were violated by the trial court’s order that is presently before this Court.

C. Decisions in Other Jurisdictions

Under an *Edmunds* analysis, this Court will “also consider the opinions of our sister states. In so doing, our goal is not to create a ‘score card,’ but rather to consider whether the underlying logic of the decisions informs our analysis of the related Pennsylvania provision.” *Molina*, 104 A.3d at 451. Sometimes, in making such an assessment, this Court will also examine the status of an issue in the federal courts as well. *Id.* at 451 & n.19. In the end, however, the Court must “base our decision on the Pennsylvania [C]onstitution and our precedent applying the right against self-incrimination.” *Id.* at 452. In this instance, other courts are divided on the precise question presented, with the greater number (mostly federal)

favoring the Commonwealth's position, but the better reasoned decisions (mostly in the States, and particularly recently) supporting the defendant.

While 48 of the 50 states have self-incrimination protections in their own state constitutions (all but New Jersey and Iowa), more than half of those mimic the federal wording, while 23 utilize the historic Virginia/Pennsylvania language of "give evidence" or "furnish evidence." *See* Friesen, *supra*, § 12.02[2], text & nn. 16–17.²⁸

As noted by the Superior Court below, 176 A.3d at 875, the U.S. Court of Appeals for the Third Circuit addressed the question of compelled production of a computer password in *Apple MacPro*, 851 F.3d 258. That case is of extremely limited utility as precedent here for several reasons. First, the case arose in the context of a mere investigation, ancillary to the execution of a search warrant; the subject was not yet accused under an indictment or information, as here. Second, the suspect in that case was directed merely to enter the password into his computer, rather than to provide it to the police, as here. Third, the court of appeals ruled that the suspect had failed to object in a timely manner, rendering his claim either unreviewable or at best reviewable only for what the federal courts call "plain error," available only when the error is obvious and the judicial system

²⁸ Professor Friesen says there are 20, but undersigned counsel have identified 24, including Pennsylvania. A table listing these is attached to this brief as an Addendum .

would be called into disrepute by a failure to address it. That standard was not met. In any event, the court of appeals could only review the federal constitutional issue, which as already shown is not identical to that arising under Article I, Section 9. And even as to the federal issue, the Third Circuit mistakenly thought itself obligated by U.S. Supreme Court precedent to apply the “foregone conclusion” theory.²⁹

The only other federal Circuit to have addressed the issue in depth came to a conclusion opposite to the Third, as did the U.S. Court of Appeals for the Armed Forces. *See Doe II*, 670 F.3d 1335; *United States v. Mitchell*, 76 M.J. 413, 2017 WL 3841376 (C.A.A.F. 2017).³⁰ For these reasons, the *Apple MacPro* decision has little to contribute to this Court’s *Edmunds* analysis.

The relatively few state courts to have addressed the decryption password issue have reached divergent conclusions, sometimes even within the same state, and few have considered the impact of their states’ own constitutions’ self-incrimination clauses on such cases. *Compare G.A.Q.L.*, 2018 WL 5291918 (Fla. Dist. Ct. 2018) (applying Fifth Amendment to bar compelled disclosure of

²⁹ The decisions of the Third Circuit are not binding on this Court as to federal constitutional issues. *E.g.*, *Goldman v. SEPTA*, 618 Pa. 501, 57 A.3d 1154, 1169 n.12 (2017).

³⁰ A panel of the Sixth Circuit, in a non-precedential opinion, refused to grant Fifth Amendment protection in a similar case on the highly dubious ground that the privilege against compulsory self-incrimination does not apply in a probation revocation proceeding. *See United States Smalcer*, 464 Fed.Appx. 469 (6th Cir. 2012).

password; citing but not separately analyzing Fla.Const., art. I, § 9); *Seo v. State*, 109 N.E.3d 418 (holding unconstitutional under Fifth Amendment an order to defendant to decrypt computer; not separately addressing state constitution); and *Baust*, 89 Va.Cir. 267 (finding Fifth Amendment violation in order to provide computer password; not addressing state constitution); with *State v. Andrews*, 2018 WL 5985982 (N.J. App. Div. Nov. 15, 2018) (following *Apple MacPro*); *State v. Stahl*, 206 So.3d 124 (Fla. 2d Dist. Ct. App. 2016) (sustaining compulsion order over Fifth Amendment objection; not addressing state constitution); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014) (order that defendant enter decryption key, without disclosing it, did not violate either state or federal self-incrimination privilege) (under reconsideration *sub nom. Commonwealth v. Jones*, SJ-2018-0221 (Mass., argued Nov. 6, 2018)); *cf. Albertson v. Albertson*, 73 Va. Cir. 94 (19th Jud.Cir. 2007) (authorizing wife's expert in divorce action, without husband's participation, to override password to access protected files on computer wife took from marital home; held, no Fifth Amendment violation; no state constitutional analysis).

Notably, branches of the Florida and Virginia intermediate appellate courts are both in conflict within those states, and Massachusetts – the only state whose highest court has addressed the issue – is actively reconsidering its precedent. All of these states but New Jersey have state constitutional self-incrimination

protections in the same terms as Pennsylvania's, thus differing from the Fifth Amendment, although almost none address it. This survey shows that there is no "weight of authority" on the issue presently before the Court. The current national trend is toward greater protection, not less. Of all the cases, appellant would respectfully suggest that the recent *Indiana Seo* case is the most thoughtful and thorough.

**D. Conclusion Under the Article I, Section 9 Privilege:
The Judgment of the Superior Court Must Be Reversed**

As demonstrated in the foregoing sections of this Point of appellant's argument, this Court has given a broad and sympathetic reading to the Pennsylvania Constitution's self-incrimination clause throughout this Commonwealth's 240-year history. Never has the Court countenanced the sort of parsing that would be required to treat the order under examination here as anything other than a kind of prohibited compulsion on the accused to "give evidence" against himself. The trial court, with approval from the Superior Court, directed Mr. Davis to make a statement, based on the content of his own mind and memory, telling the police how to gain access to a locked repository of potential evidence. Article I, Section 9, forbids that order.

A statement revealing a memorized password is not like disclosure of a pre-existing written record, which federal law might allow to be compelled from the

accused, subject to the “act of production” rule. This Court’s precedent, by contrast, has never allowed such compulsion under Article I, Section 9. Accordingly, this case does not necessarily call upon the Court to consider whether to recognize the federal “act of production” doctrine for the first time, much less the dubious “foregone conclusion” exception to that theory. But even if that question were truly presented (as the Superior Court thought it was) this Court should reject the federal doctrine as inconsistent with the text, history and principles behind the self-incrimination privilege of Article I, Section 9 of the Pennsylvania Constitution.

The trial court attempted, in direct violation of our Declaration of Rights, to compel Mr. Davis to give evidence against himself. The Superior Court wrongly affirmed that order. For all the reasons discussed in this brief, the order appealed from must be reversed.

CONCLUSION

Under both the state and federal constitutions, the order of the Superior Court must be reversed. Appellant Davis cannot be compelled to reveal the password to his computer.



Brett Max Kaufman*
Jennifer S. Granick*
American Civil Liberties Union
125 Broad St., Floor 18
New York, NY 10004
(t) 212.549.2500

* *Pro hac vice* pending



Witold J. Walczak, Pa. I.D. 62976
Andrew Christy, Pa. I.D. 322053
ACLU of Pennsylvania
P.O. Box 60173
Philadelphia, PA 19103
(t) 215.592.1513 x138
(f) 267.225.0447
achristy@aclupa.org



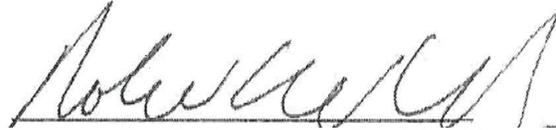
Steven Greenwald, Pa. I.D. 42890
Chief Public Defender
Luzerne County Public Defender
20 N. Pennsylvania Avenue
Wilkes-Barre, PA 18701
(t) 570-825-1754

Attorneys for Appellant Joseph Davis

Respectfully submitted,



Peter Goldberger, Pa. I.D. 22364
50 Rittenhouse Place
Ardmore, PA 19003
(t) 610.649.8200
peter.goldberger@verizon.net



Robert E. Welsh, Pa. I.D. 28143
Catherine M. Recker, Pa. I.D. 56813
Welsh & Recker, P.C.
Philadelphia, PA 19103
(t) 215.972.6430

Addendum

State Constitutions that Protect Against Compelled Disclosure of “Evidence”

Alabama	Article 1, Section 6	...and he shall not be compelled to give evidence against himself ...
Arizona	Article 2, Section 10	No person shall be compelled in any criminal case to give evidence against himself...
Connecticut	Article 1, Section 8	No person shall be compelled to give evidence against himself ...
Delaware	Article 1, Section 7	...he or she shall not be compelled to give evidence against himself or herself
Illinois	Article 1, Section 10	No person shall be compelled in a criminal case to give evidence against himself nor be twice put in jeopardy for the same offense.
Kentucky	Article 1, Section 11	He cannot be compelled to give evidence against himself...
Louisiana	Article 1, Section 16	No person shall be compelled to give evidence against himself.
Maine	Article 1, Section 6	The accused shall not be compelled to furnish or give evidence against himself or herself...
Maryland	Decl. of Rights, Article 22	That no man ought to be compelled to give evidence against himself in a criminal case
Massachusetts	Part 1, Article 12	No subject shall ... be compelled to accuse, or furnish evidence against himself.
Mississippi	Article 3, Section 26	... and he shall not be compelled to give evidence against himself ...
Nebraska	Article 1, Section 12	No person shall be compelled, in any criminal case, to give evidence against himself ...
New Hampshire	Part 1, Article 15	... or be compelled to accuse or furnish evidence against himself ...
North Carolina	Article 1, Section 23	... and not be compelled to give self-incriminating evidence ...
Oklahoma	Article 2, Section 21	No person shall be compelled to give evidence which will tend to incriminate him ...
Pennsylvania	Article 1, Section 9	In all criminal prosecutions, the accused ... cannot be compelled to give evidence against himself ...

Rhode Island	Article 1, Section 13	No person in a court of common law shall be compelled to give self-criminating evidence.
South Dakota	Article 6, Section 9	No person shall be compelled in any criminal case to give evidence against himself ...
Tennessee	Article 1, Section 9	... shall not be compelled to give evidence against himself.
Texas	Article 1, Section 10	He shall not be compelled to give evidence against himself ...
Utah	Article 1, Section 12	The accused shall not be compelled to give evidence against himself ...
Vermont	Chapter 1, Article 10	... nor can a person be compelled to give evidence against oneself ...
Virginia	Article 1, Section 8	... nor be compelled in any criminal proceeding to give evidence against himself ...
Washington	Article 1, Section 9	No person shall be compelled in any criminal case to give evidence against himself ...

Appendix A

J. A20044/17

2017 PA Super 376

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

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 “foregone 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

J. A20044/17

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.

A handwritten signature in black ink, appearing to read "Joseph D. Seletyn", written over a horizontal line.

Joseph D. Seletyn, Esq.
Prothonotary

Date: 11/30/2017

Appendix B

IN THE COURT OF COMMON PLEAS OF LUZERNE COUNTY

COMMONWEALTH OF PENNSYLVANIA :
v. : CRIMINAL DIVISION
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).

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

CERTIFICATE OF COMPLIANCE WITH WORD LIMIT

I certify, pursuant to Pa.R.A.P. 2135, that this brief does not exceed 14,000 words, to wit, no more than 13,807 words, including footnotes.

CERTIFICATE OF COMPLIANCE WITH PUBLIC ACCESS POLICY

I certify that this filing complies with the provisions of the Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts that require filing confidential information and documents differently than non-confidential information and documents.

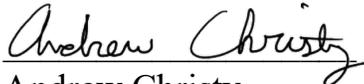
CERTIFICATE OF SERVICE

I hereby certify that the foregoing document was served upon the parties at the addresses and in the manner listed below:

Via USPS and PACFile

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

Dated: November 19, 2018


Andrew Christy