COMMONWEALTH OF PENNSYLVANIA, Appellee,

v.

JOSEPH J. DAVIS, Appellant

No. 56 MAP 2018
Supreme Court of Pennsylvania, Middle District

Argued May 14, 2019
Decided Nov 20, 2019

Counsel

Robert Eugene Welsh, Jr., Welsh & Recker, P.C., for Joseph J. Davis, Appellant.
Andrew Chapman Christy, ACLU of Pennsylvania, for Joseph J. Davis, Appellant.
Demetrius Wm. Fannick, Luzerne County Public Defender's Office, for Joseph J. Davis, Appellant.
Peter David Goldberger, Law Office of Peter Goldberger, for Joseph J. Davis, Appellant.
Jennifer Stisa Granick, Pro Hac Vice, American Civil Liberties Union, for Joseph J. Davis, Appellant.
Steven M. Greenwald, Luzerne County Public Defender's Office, for Joseph J. Davis, Appellant.
Brett Max Kaufman, Pro Hac Vice, American Civil Liberties Union Foundation, for Joseph J. Davis, Appellant.
Michael Charles Kostelaba, Luzerne County Public Defender's Office, for Joseph J. Davis, Appellant.
Mark Alan Singer, Luzerne County Public Defenders Office, for Joseph J. Davis, Appellant.
Witold J. Walczak, AMERICAN CIVIL LIBERTIES UNION, for Joseph J. Davis, Appellant.
Amanda Marie Young, Luzerne County Public Defender's Office, for Joseph J. Davis, Appellant.
Joshua D. Shapiro, Pennsylvania Office of Attorney General, for Commonwealth of Pennsylvania, Appellee.
William Ross Stoycos, PA Office of Attorney General, for Commonwealth of Pennsylvania, Appellee.
Thomas Farrell, Farrell & Reisinger, LLC, for Electronic Frontier Foundation, Amicus Curiae.
Tyler R. Green, for States of Utah, Arkansas, Georgia, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisana, Maine, et al, Amicus Curiae.

Todd, Debra, Justice

OPINION

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

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

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

a Dell computer.[2] He admitted to having prior pornography convictions, but denied the computer contained any illegal pornographic images. Appellant then declined to answer additional questions without a lawyer. *Id.* Later examination of the computer revealed that the hard drive had been "wiped," removing data entirely or rendering it unreadable. *Id.* at 43-44.

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

On October 20, 2015, the OAG executed another search warrant at Appellant's apartment based upon this video. At Appellant's apartment, the agents discovered a single computer, an HP Envy 700 desktop. After being *Mirandized,* Appellant informed the agents that he lived alone, that he was the sole user of the computer, and that he used hardwired Internet services which are password protected, and, thus, not accessible by the public, such as through Wifi. *Id.* at 26. Appellant offered that only he knew the password to his computer. *Id.* Appellant also informed the agents, *inter alia,* that he watched pornography on the computer which he believed was legal; that he had previously been arrested for child pornography; and that child pornography was legal in other countries so he did not understand why it was illegal in the United States. *Id.* at 27-28. The agents arrested Appellant for the eMule distributions and seized his computer. Agent Block asked Appellant for the password to this computer and Appellant refused. *Id.* at 28. Subsequently, when in transit to his arraignment, Appellant spoke openly about watching various pornographic movies, indicating that he particularly liked watching 10, 11, 12, and 13-year olds. *Id.* at 30. Agent Block again requested that Appellant provide him with the password to the computer. Appellant responded: "It's 64 characters and why would I give that to you? We both know what's on there. It's only going to hurt me. No f*cking way I'm going to give it to you." *Id.*

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

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

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

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

The trial court focused on the question of whether the encryption was testimonial in nature, and, thus, protected by the Fifth Amendment. The trial court opined that "[t]he touchstone of whether an act of production is testimonial is whether the government compels the individual to use `the contents of his own mind' to explicitly or implicitly communicate some statement of fact." Trial Court Opinion, 6/30/2016, at 8-9 (citation omitted). As part of its analysis, the trial court looked to the "foregone conclusion" exception to the Fifth Amendment privilege against self-incrimination as articulated by the United States Supreme Court in *Fisher v. United States,* 425 U.S. 391, 409 (1976). The court noted the rationale underlying this doctrine is that an act of production does not involve testimonial communication if the facts conveyed are already known to the government, such that the individual "`adds little or nothing to the sum total of the government's information.'" Trial Court Opinion, 6/30/2016, at 9 (quoting *Fisher,* 425 U.S. at 409). The trial court offered that for this exception to apply, the government must establish its knowledge of (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the

evidence. *Id.* at 9.

Applying the foregone conclusion exception, the trial court found that, in the case at bar, the computer located in Appellant's residence had hard-wired Internet access only; Appellant admitted it was TrueCrypt encrypted; that he was the only user, and he was the only one who knew the password; Appellant indicated to the agents that "we both know what is on there," and stated that he would "die in prison before giving up the password;" and that the Commonwealth knew with a reasonable degree of certainty that child pornography was on the computer. *Id.* at 11. Based upon these facts, the trial court determined that the information the Commonwealth sought from Appellant was a foregone conclusion, in that the facts to be conveyed by Appellant's act of production of his password already were known to the government. As, according to the trial court, Appellant's revealing his password would not provide the Commonwealth with any new evidence, and would simply be an act that permitted the Commonwealth to retrieve what was already known to them, the foregone conclusion exception was satisfied. Thus, on June 30, 2016, the trial court granted the Commonwealth's motion and directed Appellant to supply the Commonwealth with any passwords used to access the computer within 30 days. Appellant filed an interlocutory appeal.

A three-judge panel of the Superior Court affirmed. *Commonwealth v. Davis,* 176 A.3d 869 (Pa. Super. 2017).[3] Like the trial court, the Superior Court found that, to qualify for the Fifth Amendment privilege, a communication must be testimonial. The Superior Court observed that the question of whether compelling an individual to provide a digital password was testimonial in nature was an issue of first impression for the court. Building upon the trial court's analysis, the Superior Court explained that the Fifth Amendment right against self-incrimination is not violated when the information communicated to the government by way of a compelled act of production is a foregone conclusion. The court reasoned that the foregone conclusion exception provides that an act of production does not involve testimonial communication where the facts conveyed already are known to the government and set forth the applicable three-prong test. *Id.* at 874-75 (citing *Fisher,* 425 U.S. at 410-13).

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

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

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

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

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

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

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

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

Appellant submits that, regardless of the scope of the foregone conclusion rationale, it is limited to the act of producing documents and that, as discussed below, the United States Supreme Court has applied the foregone conclusion exception only once since *Fisher,* rejecting its usage in the context of the compelled production of business records. *United States v. Hubbell,* 530 U.S. 27 (2000) (dismissing government's reliance on foregone conclusion exception, finding that compulsion to produce papers that would require defendant to make use of his own mind to identify hundreds of documents responsive to the request did not fall within the exception).

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

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

Our analysis begins with the United States Constitution. The Self-Incrimination Clause of the Fifth Amendment provides "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. This privilege not only applies to a defendant in a criminal trial, but "in any other proceeding, civil or criminal, formal or informal, where the answers might incriminate [the speaker] in future criminal proceedings." *Minnesota v. Murphy,* 465 U.S. 420, 426 (1984) (citation omitted). "Although the text does not delineate the ways in which a person might be made a `witness against himself,' we have long held that the privilege does not protect a suspect from being compelled by the State to produce `real or physical evidence.' Rather, the privilege `protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature.'" *Pennsylvania v. Muniz,* 496 U.S. 582, 588-89 (1990) (citations omitted). As offered by Justice Oliver Wendell Holmes, "the prohibition of compelling a man in criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material." *Holt,* 218 U.S. at 252-53. Indeed, "in order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a `witness' against himself." *Doe v. United States,* 487 U.S. 201, 210 (1988) ("*Doe II*") (footnote omitted).

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

The primary policy undergirding the Fifth Amendment privilege against self-incrimination is our country's "fierce `unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt' that defined the operation of the Star Chamber, wherein suspects were forced to choose between revealing incriminating private thoughts and forsaking their oath by committing perjury." *Muniz,* 496 U.S. at 596 (quoting *Doe II,* 487 U.S. at 212). This being the case, "the definition of `testimonial' evidence articulated in *Doe* must encompass all responses to questions that, if asked of a sworn suspect during a criminal trial, could place the suspect in the `cruel trilemma.'" *Id.* at 597. As the Supreme Court reasoned, "[t]his conclusion is consistent with our recognition in *Doe* that `[t]he vast majority of verbal statements thus will be testimonial' because `[t]here are very few instances in which a verbal statement, either oral or written, will not convey information or assert facts.'" *Id.* Thus, "[w]henever a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief, the suspect confronts the `trilemma' of truth, falsity, or silence, and hence the response (whether based on truth or falsity) contains a testimonial component." *Id.* (footnote omitted).

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

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

In *Fisher,* the high Court examined the question of what acts of production were testimonial in nature. *Fisher* involved consolidated cases in which the Internal Revenue Service ("IRS") sought to obtain voluntarily-prepared documents the defendant taxpayers had given to their attorneys. The IRS issued summonses on the defendant taxpayers' attorneys to produce the documents which included accountants' work papers, copies of the defendant taxpayers' returns, and copies of other reports and correspondence. The attorneys responded that producing the documents would violate their clients' rights against self-incrimination, after which the IRS brought an enforcement action.

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

This analysis served as the basis of the foregone conclusion exception to the Fifth Amendment, discussed below. The Court offered that, because the existence, location, and authenticity of the documents sought was known to the government, the Fifth Amendment privilege was rendered inapplicable. The Court explained that "[t]he existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers." *Id.* Thus, the Court reasoned that the defendant taxpayers' production of the documents was non-testimonial because the government knew of the existence of the documents, that the defendant taxpayers possessed the documents, and that the government could show their authenticity — not through the use of the defendant taxpayers' minds, but through the testimony of others. Thus, the Fifth Amendment privilege did not apply to the third-party production of documents requested. *Id.* at 414.

Almost a decade later, in *United States v. Doe,* 465 U.S. 605 (1984) ("*Doe I*"), the Court considered a Fifth Amendment challenge to a subpoena that did not seek specific, known files, but broad categories of general business records of a sole proprietorship. The Court found that, while the contents of the documents were not privileged, the act of producing the business documents could have testimonial aspects and an

incriminating effect. The Court opined that the enforcement of the subpoena would compel the defendant to admit that the records existed, that they were in his possession, and that they were authentic, which was sufficient to establish a valid claim of privilege against self-incrimination. While concluding that, by producing the documents, the defendant would relieve the government of the need for authentication, the Court mentioned (although did not apply) the foregone conclusion analysis: "This is not to say that the Government was foreclosed from rebutting respondent's claim by producing evidence that possession, existence, and authentication were a `foregone conclusion.' . . . In this case, however, the Government failed to make such a showing." *Id.* at 614 n.13 (citation omitted).

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

Importantly, for purposes of the issue before us, in response to a dissent by Justice John Paul Stevens, wherein he would have found the Fifth Amendment gave the defendant the right to refuse to sign the consent authorizing access to his bank accounts on the basis that he was compelled to use his mind as a witness against himself, the majority first agreed with the dissent by acknowledging that "[t]he expression of the contents of an individual's mind" is testimonial communication for purposes of the Fifth Amendment. *Id.* at 210 n.9. Thus, the Court was unanimous in its holding on this issue. The majority continued, however, that " [w]e simply disagree with the dissent's conclusion that the execution of the consent directive at issue here forced petitioner to express the contents of his mind. *In our view, such compulsion is more like `be[ing] forced to surrender a key to a strongbox containing incriminating documents' than it is like `be[ing] compelled to reveal the combination to [petitioner's] wall safe.'*" *Id.* (quoting Stevens, J. dissenting, 487 U.S. at 219) (emphasis added). Thus, the Court emphasized a clear physical/mental distinction in the context of a foregone conclusion analysis.

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

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

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

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

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

Finally, the Supreme Court's decision in *Muniz* informs our analysis. Muniz, after failing field sobriety tests, was arrested for driving while intoxicated, and asked various questions when he was being booked. 496 U.S. at 585-86. Specifically, the defendant was asked, *inter alia,* for identifying information such as his name, address, and date of birth, along with the date of his sixth birthday. The high Court considered the issue of whether the defendant's statements during the booking process were testimonial, and, thus, subject to the Fifth Amendment privilege against self-incrimination, which was implicated because the defendant had not been provided with *Miranda* warnings. *Id.* at 589-90. The Court held that descriptions by police of the defendant's speech as "slurred," although incriminating, were not testimonial, but akin to other physical characteristics that do not enjoy Fifth Amendment protection. *Id.* at 590-91. However, the substance of the defendant's answers, specifically involving his birthday, were held to be testimonial. The *Muniz* Court emphasized that the Fifth Amendment spares an accused from "having to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share this thoughts and beliefs with the Government." *Id.* at 595 (citation omitted). Moreover, the Court reasoned that when the defendant was asked about his birthday, he had to admit that he did not know, or answer untruthfully, raising the specter of the "cruel trilemma." *Id.* at 596. This, according to the Court, was entirely consistent with the Court's prior admonition that "[t]he vast majority of verbal statements thus will be testimonial" because they likely "convey information or assert facts." *Id.,* 496 U.S. at 597 (quoting *Doe II,* 487 U.S. at 213). Thus, the testimonial statements revealing the contents of the defendant's own mind disclosed consciousness of fact subject to the privilege.

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

Finally, and consistent with this historical repulsion of the prospect of compelling a defendant to reveal his or her mental impressions, we find it particularly revealing that, when addressing Justice Stevens's dissent in *Doe II,* the majority of the Court noted that compelling the defendant to sign the bank disclosure forms was more akin to "be[ing] forced to surrender a key to a strongbox containing incriminating documents" than it was to "be[ing] compelled to reveal the combination to [petitioner's] wall safe." *Id.,* at 210 n.9. This is a critical distinction. Consistent with a physical/mental production dichotomy, in conveying the combination to a wall safe, versus surrendering a key to a strongbox, a person must use the "contents of [their] own mind." If one is protected from telling an inquisitor the combination to a wall safe, it is a short step to conclude that one is protected from telling an inquisitor the password to a computer.

Based upon these cases rendered by the United States Supreme Court regarding the scope of the Fifth Amendment, we conclude that compelling the disclosure of a password to a computer, that is, the act of

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

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

This, however, does not end our analysis. As noted above, the United States Supreme Court has found information, otherwise testimonial in nature, to be unprotected where the production of such information is a foregone conclusion. In essence, this judicial toleration of certain compelled testimony renders otherwise privileged testimonial communication non-testimonial. Specifically, under a foregone conclusion analysis, the Supreme Court has reasoned that an act of production does not render communication testimonial where the facts conveyed already are known to the government such that the evidence sought "adds little or nothing to the sum total of the Government's information." *Fisher,* 425 U.S. at 411. Thus, what is otherwise testimonial in nature is rendered non-testimonial, as the facts sought to be compelled are a foregone conclusion. As described above, for the exception to apply, the government must establish its knowledge of: (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence.

Based upon the United States Supreme Court's jurisprudence surveyed above, it becomes evident that the foregone conclusion gloss on a Fifth Amendment analysis constitutes an extremely limited exception to the Fifth Amendment privilege against self-incrimination. The Supreme Court has spoken to this exception on few occasions over the 40 years since its recognition in *Fisher,* and its application has been considered only in the compulsion of specific existing business or financial records. *See Doe I*; *Doe II*; *Hubbell.* Its circumscribed application is for good reason. First, the Fifth Amendment privilege is foundational. Any exception thereto must be necessarily limited in scope and nature. Moreover, business and financial records are a unique category of material that has been subject to compelled production and inspection by the government for over a century. *See, e.g., Shapiro v. United States,* 335 U.S. 1, 33 (1948). The high Court has never applied or considered the foregone conclusion exception beyond these types of documents. Indeed, it would be a significant expansion of the foregone conclusion rationale to apply it to a defendant's compelled oral or written testimony. As stated by the Supreme Court, "[t]he essence of this basic constitutional principle is `the requirement that t22he [s]tate which proposes to convict *and punish* an individual produce the evidence against him by the independent labor of its officers, not by the simple cruel expedient of forcing it from his own lips.'" *Estelle v. Smith,* 451 U.S. 454, 462 (1981) (emphasis original). Broadly circumventing this principle would undercut this foundational right.

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

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

Hubbell; *Muniz*. When comparing the modest value of this exception to one's significant Fifth Amendment privilege against self-incrimination, we believe circumscribed application of the privilege is in order.

We acknowledge that, at times, constitutional privileges are an impediment to the Commonwealth. Requiring the Commonwealth to do the heavy lifting, indeed, to shoulder the entire load, in building and bringing a criminal case without a defendant's assistance may be inconvenient and even difficult; yet, to apply the foregone conclusion rationale in these circumstances would allow the exception to swallow the constitutional privilege. Nevertheless, this constitutional right is firmly grounded in the "realization that the privilege, while sometimes `a shelter to the guilty,' is often `a protection to the innocent.'" *Doe II,* 487 U.S. at 213. Moreover, there are serious questions about applying the foregone conclusion exception to information that manifests through the usage of one's mind. As expressed by the California Court of Appeals in a matter involving an order compelling the production of a weapon allegedly used in a crime:

> Implicit in the prosecution's position, and the court's order, is the argument that independent evidence establishes defendant's possession of the gun at the time of the offense and after. . . . The Commonwealth does not simply assert that the evidence to be gained by production is here inconsequential or nonincriminating; rather it says that the evidence is unworthy of Fifth Amendment protection because it merely enhances other persuasive evidence obtained without the defendant's help. *The Commonwealth's argument is indeed curious. It is as if we were asked to rule that a confession could be coerced from an accused as soon as the government announced (or was able to show) that [in] a future trial it could produce enough independent evidence to get past a motion for a directed verdict of acquittal.*

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

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

Thus, we hold that the compelled recollection of Appellant's password is testimonial in nature, and, consequently, privileged under the Fifth Amendment to the United States Constitution. Furthermore, until the United States Supreme Court holds otherwise, we construe the foregone conclusion rationale to be one of limited application, and, consistent with its teachings in other decisions, believe the exception to be inapplicable to compel the disclosure of a defendant's password to assist the Commonwealth in gaining access to a computer.[8], [9], [10]

For the above-stated reasons, we reverse the order of the Superior Court and remand the matter to the Superior Court, for remand to the trial court, for proceedings consistent with our Opinion.

Jurisdiction relinquished.

Chief Justice Saylor and Justices Donohue and Wecht join the opinion.

Justice Baer files a dissenting opinion in which Justice Dougherty and Mundy join.

DISSENTING OPINION

JUSTICE BAER.

I respectfully dissent from the majority's decision, which holds that the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination does not apply to the compelled disclosure of a computer password because the password manifests from one's mind. I further disagree with the majority's alternative holding that if the foregone conclusion exception would apply under the circumstances presented, the Commonwealth failed to satisfy the requisites thereof because it did not establish that it had knowledge of the various files stored on Appellant's computer hard drive in addition to the single previously identified file that contained child pornography.

Preliminarily, I acknowledge that the issue presented in this appeal is one of first impression, with which courts across the nation have struggled. *See generally* Marjorie A. Shields, *Fifth Amendment Privilege Against Self-Incrimination as Applied to Compelled Disclosure of Password or Production of Otherwise Encrypted Electronically Stored Data,* 84 A.L.R. 6th 251 (2019) (compiling Fifth Amendment cases involving "compelled

disclosure of an individual's password, means of decryption, or unencrypted copy of electronically stored data"). Upon review of the High Court's seminal decision in *Fisher v. United States,* 425 U.S. 391 (1976), which first recognized the foregone conclusion exception, and its progeny, I would hold that the foregone conclusion analysis applies to the compelled disclosure of a password to an electronic device, which the Commonwealth has seized pursuant to a warrant.

My analysis focuses on the compulsion order, which directed Appellant to "supply the Commonwealth with any and all passwords used to access" a specific desktop computer and hard drive seized from his residence. Trial Court Order, 6/30/2016. In my view, this order compels an act of production that has testimonial aspects in that it conveys, as a factual matter, that Appellant has access to the particular computer seized by the Commonwealth pursuant to a warrant, and that he has possession and control over the password that will decrypt the encrypted files stored on that computer. As discussed in detail *infra,* because the Commonwealth was already aware of these facts based upon its own investigation and Appellant's candid discussion with government agents, the password falls within the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination, and may be constitutionally compelled. Notably, critical to my position is the recognition that this case does not involve a Fourth Amendment challenge based upon Appellant's privacy rights in his encrypted computer files but, rather, solely a challenge to the compelled disclosure of his password based upon his Fifth Amendment privilege against self-incrimination.

I. The Fifth Amendment As Applied To Acts of Production

As noted by the majority, the Fifth Amendment provides, in relevant part, that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend V. Courts have interpreted the privilege as protecting a citizen "from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature." *Pennsylvania v. Muniz,* 496 U.S. 582, 588-89 (1990) (citations omitted). The Fifth Amendment "does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating." *Fisher,* 425 U.S. at 408. To be testimonial, a communication must either "explicitly or implicitly... relate a factual assertion or disclose information." *Doe v. United States,* 487 U.S. 201, 210 (1988).

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

It is well established that some compelled acts have no testimonial aspects and, thus, no Fifth Amendment protection, as the acts do not require an accused to relate a factual assertion, disclose knowledge, or "speak his guilt." *Doe v. United States,* 487 U.S. 201, at 210-11 (1988). These include, for example, furnishing a blood sample, providing a voice or handwriting exemplar, or standing in a line-up. *Id.* (collecting cases). Other compelled acts, such as the production of certain subpoenaed documents, may have a compelled testimonial aspect warranting Fifth Amendment protection where the government's demand is akin to a "detailed written interrogatory or a series of questions at a discovery deposition," characterized as a "fishing expedition." *United States v. Hubbell,* 530 U.S. 27, 36, 41-42 (2000).[1]

Finding that an act of production has testimonial aspects, however, does not necessarily mean that the Fifth Amendment privilege precludes compulsion of the evidence sought. As the majority cogently observes, the United States Supreme Court has found that information, otherwise testimonial in nature, is unprotected where the production of such information is a foregone conclusion. Majority Opinion at 20. The foregone conclusion exception applies where the existence and location of the compelled evidence "adds little or nothing to the sum total of the government's information." *Fisher,* 425 U.S. at 410. The High Court in *Fisher* explained that a foregone conclusion exists where "[t]he question is not of testimony but of surrender." *Id.* at 411 (quoting *In re Harris,* 221 U.S. 274, 279 (1911)). Thus, as the majority recognizes, "what is otherwise testimonial in nature is rendered non-testimonial, as the facts sought to be compelled are a foregone conclusion." Majority Opinion at 21.

In my opinion, the compulsion of Appellant's password is an act of production, requiring him to produce a piece of evidence similar to the act of production requiring one to produce a business or financial document, as occurred in *Fisher.*[2] *See* Trial Court Order, 6/20/2016 (directing Appellant to "supply the Commonwealth

with any and all passwords used to access the HP Envy 700 desktop computer with serial # MXX4100000042C containing Seagate 2 TB hard drive with serial # Z4Z1AAAEFM"). An order compelling disclosure of the password, here a 64-character password, has testimonial attributes, not in the characters themselves, but in the conveyance of information establishing that the password exists, that Appellant has possession and control of the password, and that the password is authentic, as it will decrypt the encrypted computer files. The Commonwealth is not seeking the 64-character password as an investigative tool, as occurred in *Hubbell,* where the government compelled the disclosure of thousands of documents to engage in a fishing expedition to discover evidence of the defendant's guilt. To the contrary, the Commonwealth already possesses evidence of Appellant's guilt, which it set forth in an affidavit of probable cause to obtain a warrant to search Appellant's computer. Stated differently, the Commonwealth is not asking Appellant to "speak his guilt," but merely to allow the government to execute a warrant that it lawfully obtained.

Because I view the compulsion order as requiring the "surrender" of Appellant's password to decrypt his computer files, I would apply *Fisher's* act-of-production test. The majority declines to apply the foregone conclusion rationale to the compelled disclosure of Appellant's computer password, finding that to do so would constitute a "compulsion of one's mental processes" in violation of the Fifth Amendment. Majority Opinion at 22. There is appeal to this conclusion, as requiring Appellant to supply his password involves some mental effort in recalling the 64 characters used to encrypt the computer files.[3] However, one would expend similar mental effort when engaging in virtually any other act of production, such as the disclosure of business or financial records, as the individual must retrieve the contents of his mind to recall the documents' location before disclosing them to the government. Under the majority's reasoning, the compelled production of documents would be tantamount to placing the defendant on the stand and requiring him to testify as to the location of the documents sought. The mere fact that Appellant is required to think in order to complete the act of production, in my view, does not immunize that act of production from the foregone conclusion rationale.

II. Application of the Foregone Conclusion Test

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

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

Respectfully, it is my position that the foregone conclusion exception as applied to the facts presented relates not to the computer files, but to the password itself. Appellant's computer files were not the subject of the compulsion order, which instead involved only the password that would act to decrypt those files. This change of focus is subtle, but its effect is significant. While the government's knowledge of the specific files contained on Appellant's computer hard drive would be central to any claim asserted pursuant to the Fourth Amendment, the same is not dispositive of the instant claim based upon the Fifth Amendment right against self-incrimination, which focuses upon whether the evidence compelled, here, the password, requires the defendant to provide incriminating, testimonial evidence. *See Doe v. United States (In re Grand Jury Subpoena),* 383 F.3d 905, 910 (9th Cir. 2004) (providing that "it is the government's knowledge of the existence and possession of the actual documents [subpoenaed by the government], not the information contained therein, that is central to the foregone conclusion inquiry"). This Court should not alleviate concerns over the potential overbreadth of a digital search in violation of Fourth Amendment privacy concerns by invoking the Fifth Amendment privilege against self-incrimination, which offers no privacy protection. The High Court in *Fisher* made this point clear by stating, "We cannot cut the Fifth Amendment loose from the moorings of its language, and make it serve as a general protector of privacy — a word not mentioned in its text and a concept directly addressed in the *Fourth Amendment.*" 425 U.S. at 401 (quoting *United States v. Nobles,* 422 U.S. 225, 233 n.7 (1975) (emphasis in original)).

Accordingly, I would align myself with those jurisdictions that examine the requisites of the foregone

conclusion exception by focusing only on the compelled evidence itself, *i.e.,* the computer password, and not the decrypted files that the password would ultimately reveal. *See, e.g., United States v. Apple MacPro Computer,* 851 F.3d 238, 248 n.7 (3rdCir. 2017) ("[A] very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production. In this case, the fact known to the government that is implicit in the act of providing the password for the device is `I, John Doe, know the password for these devices.'"); *State v. Johnson,* 576 S.W.3d 205, 277 (Mo. Ct. App. 2019) (holding that the focus of the foregone conclusion exception as applied to the compelled entering of one's cell phone passcode is the extent of the government's knowledge about the existence of the passcode, his possession and control of the phone's passcode, and the passcode's authenticity); *Commonwealth v. Gelfgatt,* 11 N.E.3d 605, 615 (Mass. 2014) (holding that the compelled decryption of computer files satisfied the elements of the foregone conclusion exception because the government already knew the implicit facts conveyed through the act of entering the encryption key, such as the defendant's ownership and control of the computers, knowledge of the encryption, and knowledge of the encryption key); *State v. Andrews,* 197 A.3d 200, 205 (N.J. Super. 2018) (holding that whether the government was aware of the possible contents of the defendant's cell phones was immaterial "because the order requires defendant to disclose the passcodes, not the contents of the phones unlocked by those passcodes").

III. Application to Future Cases

Finally, it is my belief that the majority's approach could render inconsistent results as the determination of whether there was a Fifth Amendment violation in compelled decryption cases could depend upon the type of password that the individual employed to protect his encrypted files. For example, according to the majority, if the accused used a multi-character password to encrypt computer files, as occurred here, and the government compelled the individual to supply the password, a Fifth Amendment violation would result because the password manifests through the use of one's mind. Majority Opinion at 23. However, if the individual employed a biometric password, such as facial recognition or a fingerprint, the majority's analysis would arguably lose its force. Under those circumstances, the individual is not using the contents of his mind but, rather, is performing a compelled act of placing his finger or face in the appropriate position to decrypt the files. Additional questions arise when the act of compulsion is not the disclosure of the password itself, but the entry of the password into the computer. It is my position that all these examples constitute acts of production that would be subject to the foregone conclusion rationale in the appropriate case. The same legal analysis should apply to the underlying act of compelled decryption of digital information when the government has obtained a warrant to search the digital container. To hold to the contrary would create an entire class of evidence, encrypted computer files, that is impervious to governmental search. This could potentially alter the balance of power between governmental authorities and criminals, and render law enforcement incapable of accessing relevant evidence.

IV. Conclusion

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

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

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

"SHA value," which is essentially a "digital fingerprint" that corresponds with known SHA values of child pornography files. N.T., 1/14/2016, at 20. This evidence demonstrates that Appellant possessed the password to decrypt files on the computer seized by the Commonwealth, as his own words established that he was the sole user of the computer and forensic analysis demonstrated that he was accessing the encrypted files on the days leading up to his arrest.

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

Justices Dougherty and Mundy join this dissenting opinion.

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

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

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

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

[5] *Amicus* for Appellant, the Electronic Frontier Foundation, stresses that compulsion to disclose a computer password subjects an individual to a "cruel trilemma" — to choose between providing the allegedly incriminating information; lying about the purported inability to do so; or refusing to cooperate and be held in contempt. According to *Amicus,* the privilege was designed to prevent this trilemma. In a joint *amicus* brief in support of the Commonwealth, various states provide an interesting history of modern encryption, press the troubling consequences of Appellant's position — including the altering of the balance of power, rendering law enforcement incapable of accessing large amounts of relevant evidence — and warn that adopting Appellant's position could result in less privacy, not more, in the form of draconian anti-privacy legislation.

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

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

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

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

As the Superior Court recounted below, there is a high probability that child pornography exists on Appellant's computer, as evidenced by: Appellant's IP address utilizing a peer-to-peer file sharing network to share videos depicting child pornography; the fact that the sole computer seized had hardwire Internet; and the fact that Appellant "implied as to the nefarious contents of the computer on numerous occasions." *Davis,* 176 A.3d at 876. However, for the exception to apply, the facts sought to be compelled must be already known to the Commonwealth. It is not merely access to the computer that the Commonwealth seeks to obtain through compelling Appellant to divulge his computer password, but all of the files on Appellant's computer. The password is merely a means to get to the computer's contents. While it is conceivable, and indeed, likely, that a single video containing child pornography (as previously viewed by the OAG agents) may be on the computer, the compelled revelation of the password could lead to a trove of a presently unknown number of files. Indeed, the record establishes that the entire hard drive of the computer was encrypted and "there was no data that could be read without opening the TrueCrypt volume." N.T. Hearing, 1/14/16, at 46. Agent Cook could only confirm that there was "Windows on the computer and the TrueCrypt," and he had no knowledge of any specific files other than the operating system files. *Id.* at 50-51.

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

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

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

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

[The foregone conclusion exception's] three-part test is tautological when applied to passwords because all password-protected cellphones have an "authentic" password, making the [*State v. Stahl,* 206 So.3d 124 (Fla. Dist. Ct. App. 2016)] test somewhat circular. In this regard, the court in *Stahl* said that `[i]f the phone or

computer is accessible once the passcode or key has been entered, the passcode or key is authentic. 206 So.3d at 136, which begs the question of whether sufficient evidence established that the passcode is authentic *before* it had been compelled and used successfully. The state must have sufficient proof of authenticity *before* it can compel the password's production; simply because a compelled password unlocks a cellphone after the fact doesn't make it authentic ex ante. To do otherwise is "like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox.' [citing *Hubbell*].

Pollard, 2019 WL 2528776 at *4.

Related thereto, and as noted above, the United States Supreme Court has limited the application of this narrow exception to Fifth Amendment protections to contexts where the facts sought "add[] little or nothing to the sum total of the Government's information." *Fisher,* 425 U.S. at 411. Nothing could be farther from the case here, as the password which the Commonwealth seeks to compel could disclose a vast swath of files of which the Commonwealth, it appears, currently has no knowledge.

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

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

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

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

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

End of Document.