The University of New Hampshire Law Review

Volume 20 | Number 1 Article 4

12-1-2021

Reconsidering the Foregone Conclusion Doctrine: Compelled Decryption and the Original Meaning of Self-Incrimination

Norman Hobbie Jr.

Norman Hobbie Jr.

Reconsidering the Foregone Conclusion Doctrine: Compelled Decryption and the Original Meaning of Self-Incrimination

20 U.N.H. L. Rev. 51 (2021)

ABSTRACT. The Self-Incrimination Clause of the Fifth Amendment prohibits the government from compelling an individual "to be a witness against himself." The Supreme Court of the United States has long interpreted "witness" as "one who gives testimony." Undoubtedly, this interpretation prevents the government from compelling a witness to take the stand and testify to his own demise. This interpretation also extends to the act of producing documents, giving rise to the so-called "act of production" doctrine. Yet if a court deems the testimonial value of the act minimal—in other words, not "sufficiently testimonial"—the government can compel production under the "foregone conclusion" exception. As technology has advanced, the extension and application of this doctrine has become increasingly challenging.

Recently, however, two sitting Supreme Court Justices have called into question the entire act of production doctrine. Specifically, on separate occasions, Justices Thomas and Gorsuch have indicated a willingness to revisit the meaning of "to be a witness." In their view, substantial evidence shows that the original meaning of "to be a witness" was "to furnish evidence." According to that reading, the government could no longer compel individuals to "give" evidence. While that interpretation may be faithful to the text of the Constitution, it may not be practical given recent technological advances. This Article contributes to recent self-incrimination clause debate by underscoring the potential difficulties that accompany the application of an original meaning approach to the "to be a witness" requirement. Namely, in the era of personal data privacy, taking the doctrine in a different direction may leave us no better off even if the revised path more faithfully adheres to the text and original meaning of the Fifth Amendment's Self-Incrimination Clause.

AUTHOR. Graduate of the University of Virginia School of Law, J.D. 2020. I am grateful for the support and helpful comments of Justin W. Aimonetti and Jack W. Hobbie. I would also like to thank the members of *The University of New Hampshire Law Review* for their careful editing and feedback. Any errors are my own.

INTRODUCTION

In the last decade, the judiciary has waded into the national debate about data security.[1] In *Riley v. California*, for example, the Supreme Court held that the Fourth Amendment requires a warrant before the government searches the data contents of a phone.[2] That decision left many data security questions unanswered. What happens, for instance, when the government has a warrant to search the contents of an iPhone, only to be stopped in its tracks at the lock screen? Can the government compel the owner of the device to unlock the phone?

The Fifth Amendment prevents a person from being compelled in any criminal case to be a witness against himself.[3] The protection "is limited to criminal matters, but it is as broad as the mischief against which it seeks to guard."[4] The breadth of this privilege has perplexed scholars and courts alike.[5] It certainly protects one from having to take the stand in his own criminal case.[6] This protection also has been interpreted to shield individuals from being compelled to produce documents.[7] The documents themselves, however, receive no protection. Rather, it is the implicit testimony communicated by the physical act of handing over documents that anchors in a constitutional safe harbor.[8] This protection is commonly referred to as the "act of production doctrine."[9] The doctrine applies only when the act is

---

1 See David Alpert, *Beyond Request-and-Respond: Why Data Access Will Be Insufficient to Tame Big Tech*, 120 COLUM. L. REV. 1215, 1215–17 (2020) (discussing increasing public interest in data privacy).

2 Riley v. California, 573 U.S. 373, 403 (2014).

3 U.S. CONST. amend. V.

4 Counselman v. Hitchcock, 142 U.S. 547, 562 (1892).

5 *See* Thea A. Cohen, *Self-Incrimination and Separation of Powers*, 100 GEO. L.J. 895, 899–901 (2012) ("[The privilege] can focus on any or all of four interrelated questions: What person can invoke the privilege? What is a criminal case? What is compulsion? What is a witness?").

6 *Counselman*, 142 U.S. at 562 ("It is impossible that the meaning of the constitutional provision can only be that a person shall not be compelled to be a witness against himself in a criminal prosecution against himself. It would doubtless cover such cases; but it is not limited to them. The object was to ensure that a person should not be compelled, when acting as a witness in any investigation, to give testimony which might tend to show that he himself had committed a crime.").

7 Fisher v. United States, 425 U.S. 391, 411 (1976) (creating the act of production doctrine).

8 *Id.* at 410 ("The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the paper produced.").

9 *See generally* Mark A. Cowen, *The Act of Production Privilege Post-Hubbell:* United States v. Ponds *and the Relevance of the "Reasonable Particularity" and "Foregone Conclusion" Doctrines*, 17 GEO. MASON L. REV. 863, 863–64 (2010).

"testimonial," permitting the suspect to invoke his Fifth Amendment rights.[10]

The "foregone conclusion doctrine," however, provides an exception to the act of production doctrine. In *Fisher v. United States*, the Supreme Court propounded the foregone conclusion exception, allowing the government to compel certain acts.[11] That is, if the testimony implicit in the compelled physical act is of "minimal testimonial significance," then the Fifth Amendment does not shield the act of production.[12] Put differently, the government must already know of the possession, existence, and authentication of documents. The testimony, then, is said to be a foregone conclusion. But the exception remains underdeveloped and arguably limited. In fact, the Supreme Court has only opined on this exception in the physical document production context.

Not all agree on whether the foregone conclusion rationale should extend to other contexts—namely, encrypted devices. Commentators and lower courts have struggled with an initial question: is the act of decrypting a device testimonial?[13] Courts have also disagreed as to what, in fact, that potentially testimonial act even is communicating.[14] If the Fifth Amendment *does* apply to protect against compelled decryption, courts diverge over whether the foregone conclusion doctrine extends beyond document production to compelled decryption of passcodes.[15] And if the foregone conclusion doctrine is applicable, courts have disagreed about whether it applies merely to the passcode, or the underlying documents too.[16]

Scholarly debate has illuminated these questions and the rationales behind the different approaches.[17] More recently, two state supreme courts have addressed whether the foregone conclusion doctrine applies to compelled device decryption. In *Commonwealth v. Davis*, a slim majority of the Supreme Court of Pennsylvania declined to extend the foregone conclusion exception to compelled decryption,

---

[10] *Fisher*, 425 U.S. at 408 ("It is also clear that 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.").

[11] *Id.* at 411 ("It is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testimony within the protection of the Fifth Amendment. . . . The existence and location of the papers are a foregone conclusion and the taxpayers adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers.").

[12] *See id.* at 412.

[13] *See infra* Part II.

[14] *See infra* Part II.B.

[15] *See infra* Part II.

[16] *See infra* Part II.

[17] *See infra* Part II.A.

holding that the exception was "extremely limited."[18] In 2020, the Supreme Court of New Jersey in *State v. Andrews* ultimately sided with the *Davis* dissent.[19] The *Andrews* majority allowed the government to compel the defendant to decrypt his devices.

From those opinions, one thing is abundantly clear: scant Supreme Court precedent has misguided courts. The fact is, only one sentence in the *Fisher* Court's decision unpacked the foregone conclusion exception: "[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."[20] Subsequent cases have only briefly mentioned it. Not only have lower courts been stranded to make inferences about the expanse of this exception, but also they must determine what handing over a password is saying in the form of "testimony." Herein lies a question that will likely shape the exceptions interaction with data encryption given the originalist bent of the modern Supreme Court: has the Self-Incrimination clause jurisprudence strayed too far from the constitutional text?

In Justice Thomas's words, "In a future case, I would be willing to reconsider the scope and meaning of the Self-Incrimination Clause."[21] He is not alone. Justice Gorsuch has also suggested a willingness to revisit the confusing Self-Incrimination Clause doctrine, because it stems from a misreading of the Constitution's text.[22] In so doing, both Justices call into question the entire testimonial versus non-testimonial distinction that has shaped the Self-Incrimination Clause jurisprudence for decades. In their view, substantial evidence from the founding shows that the phrase "to be a witness" in the Self-Incrimination Clause was

---

[18] Commonwealth v. Davis, 220 A.3d 534, 549, 551 (Pa. 2019) ("Indeed, we conclude the compulsion of a password to a computer cannot fit within this exception."); *see also infra* Part II.B.

[19] State v. Andrews, 234 A.3d 1254, 1274 (N.J. 2020) ("We agree with the Davis dissent that the proper focus here is on the Fifth Amendment and that the Fourth Amendment's privacy protections should not factor into analysis of the Fifth Amendment's applicability.").

[20] *See* Fisher v. United States, 425 U.S. 391, 411 (1976).

[21] United States v. Hubbell, 530 U.S. 27, 49 (2000) (Thomas, J., concurring) (". . . I write separately to note that this doctrine may be inconsistent with the original meaning of the Fifth Amendment Self-Incrimination Clause. A substantial body of evidence suggests that the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence. In a future case, I would be willing to reconsider the scope and meaning of the Self-Incrimination Clause.").

[22] Carpenter v. United States, 138 S.Ct. 2206, 2271 (2018) (Gorsuch, J., dissenting) (". . . [T]here is substantial evidence that the privilege against self-incrimination was also originally understood to protect a person from being forced to turn over potentially incriminating evidence.").

originally understood to mean "to furnish evidence."[23] And so, in theory, the entire act of production doctrine should give way to the original meaning in the absence of the testimonial versus non-testimonial distinction. Adopting the originalist reading propounded by Justices Thomas and Gorsuch would offer broader protections to criminal defendants—an outcome not uncommon to originalists.[24] Namely, the government could no longer compel individuals to produce any incriminating evidence.

In his work that gained the attention of the Justices, Professor Richard Nagareda outlines the originalist approach to "to be a witness."[25] If the original meaning of "to be a witness" were revived, producing private papers would be considered "furnishing evidence." This approach would allow the government to unilaterally "take," while prohibiting it from compelling individuals to "give." Put differently, the government would have broad power to search and seize, or "take," but could no longer compel production, or "giving," of incriminating documents. The act of production cases would not survive. That is, the testimonial versus non-testimonial distinction would be obsolete, as would the foregone conclusion mess.

This begs the question whether lower courts should even continue down the foregone conclusion rabbit hole. Perhaps the compelled device decryption cases present the proper "future case" that Justice Thomas has been looking for. Justice Baer of the Supreme Court of Pennsylvania seems to suggest so, writing, "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."[26]

While the world has changed due to technological advances, the Constitution has not. The conservative majority of the Supreme Court could revisit the Self-Incrimination Clause. At first glance, the "give" versus "take" distinction seems easier to administer than the testimonial versus non-testimonial regime. That said, complex questions will arise that need to be answered. While the foregone conclusion doctrine would not survive the doctrinal shift, there is reason to believe that certain compelled physical acts would still be permissible. And if that is the case, what do we make of compelling a defendant to physically enter a passcode? It may seem like this is compelling one to furnish evidence, but what if the government already lawfully seized the device and has a valid warrant to search its

---

[23] *See generally infra* Part II.C.

[24] *See generally* Crawford v. Washington, 541 U.S. 36, 68–69 (2004).

[25] Richard A. Nagareda, *Compulsion "To be a Witness" and the Resurrection of Boyd*, 74 N.Y.U. L. Rev. 1575, 1590–99 (1999).

[26] *See* Commonwealth v. Davis, 220 A.3d 534, 555 n. 3 (Pa. 2019) (Bear, J., dissenting).

contents?

In this Article, I seek to engage with some of these questions. Little doctrine from an originalist perspective exists to speculate about the future of the Self-Incrimination Clause. But some cases that are clearly established under the current regime would move into the proverbial gray area.[27] In Part I, I discuss the current state of the Self-Incrimination Clause and the act of production doctrine. I then explore the foregone conclusion exception. In Part II, I review debate among commentators and lower courts, before turning to the dueling cases in Pennsylvania and New Jersey. After engaging with the confusing debate, I analyze the original meaning of "to be a witness," adopted by Professor Nagareda and cited by Justices Thomas and Gorsuch. In Part III, I conclude by applying the originalist meaning to the cases in Pennsylvania and New Jersey, and I address some complicated questions that may accompany this doctrinal shift.

I. COMPELLED PASSWORD PRODUCTION AND THE FIFTH AMENDMENT

The Fifth Amendment protects a person from being "compelled in any criminal case to be a witness against himself . . . ."[28] While a pair of sitting Justices on the Supreme Court of the United States have hinted at revisiting the original meaning of this clause,[29] the Court has not done so for the better part of a century.[30] For now, Supreme Court precedent holds that the language prevents the government from compelling an individual to produce "testimony."[31] Not only are written and oral testimony protected, but also physical acts of a communicative nature.[32] This

---

[27] *See infra* Part III.

[28] U.S. CONST. amend. V.

[29] Carpenter v. United States, 138 S.Ct. 2206, 2271 (2018) (Gorsuch, J., dissenting); *see also* United States v. Hubbell, 530 U.S. 27, 49 (2000) (Thomas, J., concurring) ("A substantial body of evidence suggests that the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence.").

[30] Laurent A. Sacharoff, *Unlocking the Fifth Amendment and Encrypted Devices*, 87 FORDHAM L. REV. 203, 204–05 (2018) ("Under the hoary, nineteenth century Boyd doctrine, the Court once intertwined the two amendments into a majestic, overlapping bulwark of protection. . . . In the last fifty years, however, the Court has sought to melt this powerful alloy, separating each amendment into complementary, distinct domains."); *see also* Boyd v. United States, 116 U.S. 616, 630–31 (1886).

[31] Pennsylvania v. Muniz, 496 U.S. 582, 589 (1990) (". . . [T]he privilege [against self-incrimination] 'protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature.'" (citing Schmerber v. California, 384 U.S. 757, 761 (1966))).

[32] *Id.* at 591–92 (citing a string of cases where real or physical evidence could be compelled).

includes the act of producing documents.[33]

However, not all document production is protected.[34] Only if the act itself is compelled, incriminating, and testimonial does the privilege against self-incrimination apply.[35] Yet, even if the act of production includes implied testimony, the evidence is not necessarily exempt from compulsion.[36] That is, if the implied testimony "adds little or nothing to the sum total of the government's information," it is a foregone conclusion.[37] The government can circumvent the protection for otherwise testimonial evidence, and thus can compel the act.[38] This workaround is commonly known as the foregone conclusion exception.[39]

While initially propounded by the Supreme Court in the document production context, advances in technology have made the exception more relevant, but less clear.[40] Some courts have expanded this doctrine to personal devices, allowing the government to compel individuals to decrypt their devices.[41] The extension of the

---

[33] Fisher v. United States, 425 U.S. 391, 414 (1976).

[34] *Id.* at 411–14 (allowing for the production of defendant's tax documents).

[35] *Id.* at 408 ("It is also clear that 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.").

[36] *See id.* at 411 ("It is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testimony within the protection of the Fifth Amendment.").

[37] *Id.* ("The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers.").

[38] *Id.* ("Under these circumstances by enforcement of the summons no constitutional rights are touched. The question is not of testimony but of surrender." (internal citation omitted)).

[39] *See infra.* Part I.B.

[40] Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, 97 TEX. L. REV. ONLINE 73, 73–77 (2019) (discussing the increasing importance of cellphones); Sacharoff, *supra* note 30, at 220–22 (highlighting encryption technology on laptops and smartphones).

[41] Several recent cases address the issue. *See* United States v. Apple MacPro Computer, 851 F.3d 238, 249 (3d Cir. 2017) (allowing the government to compel decryption); *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1352 (11th Cir. 2012) (denying compelled decryption); State v. Andrews, 234 A.3d 1254, 1277 (N.J. 2020) (agreeing with jurisdictions that allow compelled decryption); Seo v. State, 148 N.E.3d 952, 955 (Ind. 2020) (rejecting application of foregone conclusion exception, not allowing for compelled decryption); Commonwealth v. Davis, 220 A.3d 534, 551 (Pa. 2019) (denying government's motion to compel decryption); Commonwealth v. Jones, 117 N.E.3d 702, 707-09 (Mass. 2019) (allowing decryption on state constitutional law grounds even where art. 12 of the Massachusetts Constitution provided broader protections against self-incrimination: "[n]o subject shall … be compelled to accuse, or furnish evidence against himself").

foregone conclusion doctrine has not been welcomed without debate.[42] In this Part, I will briefly explore the Fifth Amendment act of production doctrine before analyzing the foregone conclusion exception.

A. The Act of Production Doctrine

The Self-Incrimination Clause of the Fifth Amendment has long been understood to protect individuals against compelled, incriminating testimony.[43] Notably, the text itself does not mention "testimony."[44] Nor does the text establish the many ways in which a person may be made to incriminate himself.[45] The privilege, however, has thus far been construed to "protect[] an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature."[46] To be testimonial, "the communication must itself, explicitly or implicitly, relate a factual assertion or disclose information."[47]

The Supreme Court elaborated on this act of production doctrine in *Fisher v. United States*.[48] The facts of *Fisher* are straightforward, and the case has been covered

---

[42] United States v. Hubbell, 530 U.S. 27, 44 (2000) (questioning the scope of the foregone conclusion rationale); *see also* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767 (2019) (applying the foregone conclusion exception to device passwords); Choi, *supra* note 40, at 73–77 (disagreeing with both Kerr and Sacharoff, while defining the cell phone as an "extension of self"). *But see* Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 TEX. L. REV. Online 63 (disagreeing with Kerr's definition and application of the foregone conclusion rationale).

[43] Pennsylvania v. Muniz, 496 U.S. 582, 588–89 (1990) ("[W]e 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.'" (citing Schmerber v. California, 384 U.S. 757, 761–64 (1966))); *see also* Robert P. Mosteller, Simplifying Subpoena Law: Taking the Fifth Amendment Seriously, 73 VA. L. REV. 1, 6 (1987) ("It is firmly established that the [F]ifth [A]mendment is violated only if the defendant's conduct is compelled, testimonial, and incriminating.").

[44] *See* U.S. CONST. amend. V. ("[n]o person . . . shall be compelled in any criminal case to be a witness against himself."); *infra* Part II.B.

[45] *See Muniz*, 496 U.S. at 591–92 (citing a string of cases that allow for compelled acts); *see also* Joseph Jarone, *An Act of Decryption Doctrine: Clarifying the Act of Production Doctrine's Application to Compelled Decryption*, 10 FIU L. REV. 767, 771–76 (explaining the modern interpretation of the Self-Incrimination Clause).

[46] *See Muniz*, 496 U.S. at 589 (quotation and citation omitted).

[47] *Id.*

[48] 425 U.S. 391 (1976).

by other commentators.[49] That said, much can be gleaned from the decision itself. The ruling covered two cases involving the Internal Revenue Service (IRS).[50] In each instance, IRS agents interviewed taxpayers for the possibility of civil or criminal liability.[51] Numerous facts were uncovered during the interview.[52] Following the interview, both taxpayers retrieved certain documents from their respective accountants.[53] They also sent those documents to their respective lawyers.[54] The IRS learned of the location of these documents and served summonses on the attorneys to produce the documents.[55] Among other arguments, the taxpayers claimed compelled production of their tax documents violated their Fifth Amendment privilege against self-incrimination.[56]

In *Fisher*, the Court made several important pronouncements. First, the majority flatly rejected part of the near-century-old case, *Boyd v. United States*.[57] Namely, the *Fisher* Court rejected the *Boyd* view of a tangled Fourth and Fifth Amendment.[58] Writing for the *Fisher* majority, Justice White announced that the

---

[49] *See* Cowen, *supra* note 9, at 866–69; Nagareda, *supra* note 25, at 1590–99; Gordon Hwang, Fisher v. United States: *Compelled Waiver of Foreign Bank Secrecy and the Privilege Against Self-Incrimination*, 56 FORDHAM L. REV. 453, 456–63 (1987); Note, *The Rights of Criminal Defendants and the Subpoena Duces Tecum: The Aftermath of* Fisher v. United States, 95 HARV. L. REV. 683, 684–85 (1982) [hereinafter *Aftermath of Fisher*].

[50] See *Fisher*, 425 U.S. at 393–94.

[51] *Id.*

[52] *Id.* ("Shortly after the interviews . . . the taxpayers obtained from their respective accountants certain documents relating to the preparation by the accountants of their tax returns.").

[53] *Id.*

[54] *Id.*

[55] *Id.* ("Upon learning of the whereabouts of the documents, the Internal Revenue Service served summonses on the attorneys directed them to produce documents listed therein.").

[56] *Id.* at 395 ("[T]he attorney claimed that enforcement [of the summonses] would involve compulsory self-incrimination of the taxpayers in violation of their Fifth Amendment privilege[.]").

[57] Boyd v. United States, 116 U.S. 616, 638 (1886) (holding that government searches and seizures of private documents are violative of the Fourth and Fifth Amendments). *But see* Nagareda, *supra* note 25, at 1607, 1623 (suggesting the modern Court has rejected the *Boyd* majority holding that tangles the Fourth and Fifth Amendments, but largely misses that Justice Miller's concurrence is the correct reading of the Fifth Amendment).

[58] *See Fisher*, 425 U.S. at 408–09 ("It would appear that under that case the precise claim sustained in *Boyd* would now be rejected for reasons not there considered. The pronouncement in *Boyd* that a person may not be forced to produce his private papers has nonetheless often appeared as dictum in later opinions of this Court. To the extent, however, that the rule against compelling production of private papers rested on the proposition that seizures of or subpoenas for 'mere

"foundations for the rule have been washed away."[59] Justice White quipped, "In consequence, the prohibition against forcing the production of private papers has long been a rule searching for a rationale consistent with the proscriptions of the Fifth Amendment."[60] Rejecting that blanket protection to all private papers, Justice White paused to consider if there was testimony implicit in the act of producing documents.[61] Producing documents in compliance with a subpoena, as it turned out, conceded the existence, possession, and control of the documents.[62] Justice White then stated that determining whether the "tacit averments" were testimonial and incriminating rested on a case-by-case analysis.[63]

Recognizing that not all document production was protected, Justice White created an exception allowing the government to compel production of personal documents.[64] The rationale was that "the existence and locations of the papers [were] a foregone conclusion and the [defendant's physical act] adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers."[65] And so, "no constitutional rights [were] touched. The question [wa]s not of testimony but of surrender."[66]

Those few lines mentioning foregone conclusions have taken on a life of their own. The exception has continued to allow government compulsion of otherwise testimonial documents.[67] While receiving little attention in subsequent Supreme

---

evidence,' including documents, violated the Fourth Amendment and therefore also transgressed the Fifth, the foundations for the rule have been washed away." (citations omitted)); *see also infra* Part II.A.

59 *Fisher*, 425 U.S. at 409.

60 *Id.*

61 *Id.* ("Accordingly, we turn to the question of what, if any, incriminating testimony within the Fifth Amendment's protection, is compelled by a documentary summons.").

62 *Id.* at 410 ("Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena.").

63 *Id.* ("These questions perhaps do not lend themselves to categorical answers; their resolution may instead depend on the facts and circumstances of particular cases or classes thereof.").

64 *Id.* at 411 ("The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons 'no constitutional rights are touched. The question is not of testimony but of surrender.'" (citing *In re* Harris, 221 U.S. 274, 279 (1911))).

65 *Id.*

66 *Id.* (quotation and citation omitted).

67 *See infra* Part I.B.

Court cases, the foregone conclusion doctrine has been expanded, albeit inconsistently, among the lower courts.[68] As one circuit judge put it, district courts must use their discretion to determine the "imaginary line" or the level of prosecutorial knowledge required for information to be a foregone conclusion.[69] In the next Section, I will review the subsequent treatment of the foregone conclusion language, as well as its implication in the lower courts.

B. The Foregone Conclusion Doctrine

Following the *Fisher* rule on the foregone conclusion exception, its use and further clarification have curiously been avoided at the Supreme Court.[70] In *United States v. Doe*, the Court briefly mentioned that the government could have argued for the foregone conclusion exception but did not meet its burden.[71] On one later occasion, the Court dismissively commented on the doctrine, stating, "Whatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it."[72] Needless to say, this does not shed much light on the standing of the exception. Perhaps parsing the language of the *Fisher* majority can explain the limits—or expansiveness—of the doctrine.

Recall *Fisher*, in which the defendant-taxpayers had given their documents to

---

[68] Zara S. Mason, *Decoding the "Testimonial" Tug of War: When a Cellphone Search Warrant and a Showing of Substantial Need and Undue Hardship Justify Cellphone Passcode Compulsion*, 18 WYO. L. REV. 503, 506–07 (2018) ("There is currently no overarching federal guidance on this issue. As it stands, numerous definitions of 'testimonial' are circulating throughout state case law, giving state courts the ability to select whatever definition they want in order to fashion the desired result. The ability to pick and choose from this collection of definitions is effectively resulting in the disclosure of cellphone passcodes being categorized as a testimonial communication in some jurisdictions and a nontestimonial communication in others.").

[69] United States v. Hubbell, 167 F.3d 552, 601 (D.C. Cir. 1999) (Williams, J., dissenting) ("Somewhere in that range is an imaginary line which, unlike the equator, can never be fixed or defined with clarity. Henceforth, therefore, the operational meaning of the 'act of production' doctrine in our circuit will largely turn on district courts' discretion in this metaphysical classification of prosecutors' knowledge.").

[70] William F. Bloomer, *18th Century Constitutional Principles Meet 21st Century Technology: Compelling Individuals to Enter Passwords Into Electronic Devices Under* Commonwealth v. Gelfgatt, *468 Mass. 512 (2014) and* Commonwealth v. Jones, *481 Mass. 540 (2019)*, 101 MASS. L. REV. 65, 68–70 (2020) (reviewing the "murky genesis" of the foregone conclusion exception propounded in *Fisher*).

[71] United States v. Doe, 465 U.S. 605, 614 n.13 (1984) ("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.").

[72] United States v. Hubbell, 530 U.S. 27, 44 (2000).

their accountants. In compelling production of those documents, the government relied on an independent source—the accountants—to retrieve the evidence.[73] This independent source persuaded the majority that the implied testimony in the defendant's act was a foregone conclusion.[74] After all, the government knew that a third party had prepared the documents.[75] Thus, by conceding that the defendant had the papers, the defendant's actions "add[ed] little or nothing to the sum total of the government's information."[76] The majority distinguished this case from private papers, figuring that since the accountant prepared the documents, the defendant could not even authenticate the evidence himself.[77] No matter what the implied testimony was, the production of tax documents had no testimonial value to authenticate or incriminate; only the accountant could do so.[78] From this language, it is unclear whether a third-party authenticating witness is necessary or sufficient to meet the foregone conclusion exception. The questions do not stop there.

Expanding on his foregone conclusion creation, Justice White claimed that, similar to a handwriting sample, the act in question was not "sufficiently testimonial."[79] Treading carefully, he stated that "[a]t this juncture, we are quite unprepared to hold that either the fact of existence of the papers or of their possession by the [defendant] poses any realistic threat of incrimination to the [defendant]."[80] According to that rationale, courts must evaluate the value or

---

[73] Fisher v. United States, 425 U.S. 391, 411–13 (1976).

[74] *Id.* at 412–13 (1976) ("As for the possibility that responding to the subpoena would authenticate the workpapers, production would express nothing more than the tax payer's belief that the papers are those described in the subpoena. The taxpayer would be no more competent to authenticate the accountant's workpapers or reports by producing them than he would be to authenticate them if testifying orally. The taxpayer did not prepare the papers and could not vouch for their accuracy.").

[75] *See id.* at 414 ("Whether the Fifth Amendment would shield the taxpayer from producing his own tax records in his possession is a question not involved here; for the papers demanded here are not his 'private papers.'").

[76] *Id.* at 411.

[77] *Id.* at 413–14.

[78] *Id.* at 409–10.

[79] *Id.* at 411 (claiming that the Fifth Amendment privilege to submit handwriting exemplars has been deemed to not be "sufficiently testimonial."). *But see id.* at 429 (Brennan, J., concurring) ("This Court's treatment of handwriting exemplars is not supportive of its position. . . . It is because handwriting exemplars are viewed as strictly nontestimonial, not because they are insufficiently testimonial, that the Fifth Amendment does not protect against their compelled production." (citations omitted)).

[80] *Id.* at 412 (White, J., majority opinion).

significance of testimony.[81] If the testimony is deemed significant, then the defendant's act of production is protected. Conversely, if the testimony only implicates existence or possession, perhaps courts would find it not incriminating *enough* to warrant protection of the Fifth Amendment.

It is possible, of course, that the aforementioned language in the *Fisher* holding was intentionally narrow. Some suggest that is the appropriate reading.[82] In the meantime, other courts have continued to use this foregone conclusion rationale and extend it to other areas, including device decryption.[83] For the most part, those courts proceed with this rule: the Fifth Amendment Self-Incrimination Clause protects acts of production that are compelled, incriminating, and testimonial. If the implied testimony, however, "adds little or nothing to the sum total of the Government's information," then it is a foregone conclusion, and the government may compel the act.[84]

Difficulties accompany this rule. First, a court must distinguish those physical acts that are testimonial from those that are not. Furthermore, to determine whether testimony is of little or no value, a court must first understand what, in fact, is communicated by a physical act. More simply stated, producing documents must *say something*. If a court determines that implied states are compelled and incriminating, the court must then decide whether the foregone conclusion

---

[81] *Id.* at 429 (Brennan, J., concurring) (criticizing the "insufficiently testimonial" inquiry as misguided and unfaithful to precedent).

[82] Seo v. State, 148 N.E.3d 952, 955 (Ind. 2020) ("[A]nd this case also highlights concerns with extending the limited exception to this context."); Commonwealth v. Davis, 220 A.3d 534, 549 (Pa. 2019) ("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. . . . Indeed, it would be a significant expansion of the foregone conclusion rationale to apply it to a defendant's compelled oral or written testimony."); Garcia v. State, 302 So.3d 1051, 1057 (Fla. Dist. Ct. App.2020) (declining to extend the foregone conclusion rationale beyond *Fisher*); *see also* Cowen, *supra* note 9, at 877 ("With regard to Fisher's 'foregone conclusion' doctrine, . . . the Hubbell Court merely stood by the narrow holding in Fisher.").

[83] *See, e.g.*, United States v. Apple MacPro Computer, 851 F.3d 238, 249 (3d Cir. 2017) (allowing the government to compel decryption); *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1352 (11th Cir. 2012) (denying compelled decryption); State v. Andrews, 234 A.3d 1254, 1277 (N.J. 2020) (agreeing with jurisdictions that allow compelled decryption); *Seo*, 148 N.E.3d at 955 (rejecting application of foregone conclusion exception, not allowing for compelled decryption); *Davis*, 220 A.3d at 551 (denying government's motion to compel decryption); Commonwealth v. Jones, 117 N.E.3d 702, 707 (Mass. 2019) (allowing decryption on state constitutional law grounds).

[84] *See Fisher*, 425 U.S. at 411; *infra* Part II.A.

exception should apply.

Continuing through the *Fisher* maze, one must discern whether implied testimony is "sufficiently testimonial" to warrant the protection of the Fifth Amendment. On top of all that, a court must parse scant case law to fill in the other gaps left by *Fisher*. For instance, what is the breadth of the foregone conclusion doctrine? What must the government know? What is the government's burden or to what degree of certainty must they have independent knowledge? In the next Part, I will briefly summarize the debate in academia. I will then highlight two cases illustrating the results of this puzzling doctrine. Finally, I will review a potentially drastic solution, adopted by two sitting Justices on the Supreme Court of the United States.

II. COMMENTATORS, LOWER COURTS, AND SPECULATORS

In the decades following *Fisher*, scholars and lower courts grappled with the foregone conclusion doctrine.[85] Zooming out from this arguably narrow exception to the act of production doctrine, there have been much broader and more consequential debates about revisiting Fifth Amendment jurisprudence.[86] Justices Thomas and Gorsuch have both suggested a willingness to revisit the Self-Incrimination Clause altogether.[87] If the Court rids Fifth Amendment jurisprudence of the testimonial versus non-testimonial distinction then the act of production doctrine would not survive in its current form.[88] Before reaching the Justices' arguments, I will review the work of commentators and lower courts that advance (or limit) the foregone conclusion doctrine.

A. Foregone Conclusions and Compelled Decryption: Academic Disagreement

The expansion of the foregone conclusion doctrine has been met with much debate. Important questions remain about what, in fact, the holding in *Fisher* even means and if the holding applies to the increasingly prevalent area of password-protected devices.[89] Commentators have argued several different

---

[85] *See infra* Part II.A.

[86] *See infra* Part II.C.

[87] Carpenter v. United States, 138 S.Ct. 2206, 2271 (2018) (Gorsuch, J., dissenting) (discussing his willingness to reconsider the Fifth Amendment); United States v. Hubbell, 530 U.S. 27, 49–55 (2000) (Thomas, J., dissenting); *see infra* Part II.C.

[88] *See* Nagareda, *supra* note 25, at 1640 ("The implications for document subpoenas are clear enough: The act-of-production doctrine announced in Fisher would be added to the list of widely discarded constitutional doctrines").

[89] *See generally* Bloomer, *supra* note 68.

understandings. Recent discussion has centered around an article by Professor Orin S. Kerr in *Texas Law Review*.[90] Subsequent commentary on his piece offers further questions, clarifications, and disagreement.[91]

In his article, Professor Kerr explained the difficulties associated with the act of production doctrine and device decryption.[92] As he put it, the act of production doctrine is meant to protect implied testimony communicated by certain acts.[93] On the other hand, he continued, the foregone conclusion exception exists to prevent suspects from erecting meaningless barriers solely to gain Fifth Amendment protection.[94] Helpfully, then, Kerr highlighted a key distinction in the act of production inquiry: the underlying documents versus the device's encryption.[95] Or, as Kerr quipped, the "treasure" and the "door-opening evidence," respectively.[96] Whereas the "treasure" is of Fourth Amendment concern, the "door-opening evidence," in his view, is the only concern of the Fifth Amendment.[97] Thus, "[w]hen the testimony implicit in the door-opening is not in play, and is only an incidental matter of form rather than substance, access to the treasure should not be blocked by the Fifth Amendment privilege."[98] To receive Fifth Amendment protection, then, the implied testimony must be at issue.

---

90 *See* Kerr, *supra* note 42.

91 *See* Sacharoff, *supra* note 30; *see also* Choi, *supra* note 40.

92 *See* Kerr, *supra* note 42, at 768 ("The issue typically arises when investigators have a warrant to search a cell phone or computer, but they cannot execute the search because the data is encrypted. Investigators obtain a court order directing a suspect to produce a decrypted version of the data by entering the password without disclosing it to the government. The suspect then objects, claiming a Fifth Amendment privilege against complying with the order.").

93 *Id.* at 776 ("The act of production doctrine is reasonably intuitive. It measures implicit testimony in an act, relating to the Fifth Amendment's core concern of compelled testimony.").

94 *Id.* at 777 ("As I see it, the foregone conclusion doctrine exists to prevent suspects from exploiting the act of production doctrine to create a bar to accessing nontestimonial evidence.").

95 *Id.* ("This means that, when the government compels acts, it acquires two different kinds of evidence at once. First, it learns the testimonial statements implicit in the act identified by the act of production doctrine. Let's call that 'door-opening evidence.' Second, the government also obtains the nontestimonial evidence as a consequence of the act. Let's call that 'the treasure.'").

96 *Id.* ("The act of compliance provides the government with two things. First, compliance establishes the person's testimonial door-opening evidence: the implicit beliefs about possession, existence, and authenticity of the [sought] documents. Second, it provides access to the treasure, the documents the government is seeking.").

97 *See id.* ("The door-opening evidence is compelled testimony. But the treasure, what the government finds in the documents, is not compelled testimony.").

98 *Id.* at 778.

Importantly, Kerr claimed the only implicit testimony of producing a passcode is "I know the passcode."[99] Kerr then proposed a bright-line rule: If a defendant's knowledge of the passcode is at issue, then the government only needs independent knowledge that a suspect knows the passcode to satisfy the foregone conclusion exception.[100] That is a seemingly low hurdle for the government to meet. In the alternative, Kerr suggested the Supreme Court of the United States may have to intervene and cease "apply[ing] constitutional doctrines mechanically to the new facts of computers and the Internet."[101] Kerr pointed out that the Supreme Court granted more Fourth Amendment protection to individuals' historical cell-site location records in *Carpenter v. United States*.[102] In the cell phone encryption context, however, Kerr suggested the Supreme Court might well do a "reverse-*Carpenter*."[103] In other words, since encryption technology now affords greater protection to individuals, the government should have greater power to strike the "equilibrium," because individuals attempting to shield incriminating evidence from the government now have an unfair advantage.[104] Kerr believed that that over-reaching result by the Supreme Court could be avoided, however, because his proposed rule—enabling the government to compel passcodes when the door-opening evidence is not at issue—would serve as a "safety valve" within the current doctrine.[105]

Kerr's rule highlighted the distinction between the Fourth and Fifth Amendments in the device decryption context. Whereas Fourth Amendment "[m]ethods of evidence collection hinge on technological change[,]" he continued, "[t]he Fifth Amendment focuses on the gathering of information from a person's

---

[99] *Id.* at 779 ("Importantly, 'I know the password' is the only assertion implicit in unlocking the device.").

[100] *Id.* at 778 ("When the testimony implicit in the door-opening is not in play, and is only an incidental matter of form rather than substance, access to the treasure should not be blocked by the Fifth Amendment privilege.").

[101] *Id.* at 790–97 (discussing the potential for the Supreme Court to change course and alter the balance between individuals and the government based on technological advances).

[102] 138 S.Ct. 2206, 2221 (2018); *see* Kerr *supra* note 42, at 791–92 (discussing the Supreme Court's holding was due to "seismic shifts in digital technology" creating an imbalance between the government and individuals).

[103] *See* Kerr, *supra* note 42, at 792 ("Should *Carpenter-like* arguments about equilibrium-adjustment extend to the Fifth Amendment right against self-incrimination? I'm not sure.").

[104] *Id.*

[105] *Id.* at 798 ("Adoption of the Fifth Amendment standard proposed in this Essay can act as a safety valve that lessens the pressure to enact heavy-handed legislative solutions. If my analysis is right, governments already have considerable powers to get into encrypted devices.").

mind, not on the technological world in which he lives."[106] Unsurprisingly, then, he viewed the reasonable particularity proposals by some scholars and courts as "unilluminating" and misguided.[107] In his view, "there is a sense in which the government does need to particularly describe the evidence sought—but for the Fourth Amendment, not the Fifth Amendment."[108] Therefore, if the government already knows that the suspect possesses knowledge of the passcode, the Fifth Amendment does not bar compulsion of the passcode.

Many have critiqued or advanced Kerr's argument. Professor Laurent Sacharoff commented that when considered in light of the precedent, Kerr's rule is incorrect.[109] Instead, Sacharoff proposed a rule that Kerr criticized: the government must already know the person possesses the *files* on the device and be able to identify the files with reasonable particularity.[110] To meet the foregone conclusion exception, according to Sacharoff, the government must know precisely the existence of the underlying documentary evidence that they seek, where it is, and that it is authentic.[111] Following Sacharoff's reasoning, unless the government knows the *contents* of the documents they are searching for—before obtaining them—then the government must produce the key, the lockpick, the bulldozer, the battering ram, or the 64-character code. It should be clear that whether the foregone conclusion doctrine applies to the files (as Sacharoff argues) or only the

---

[106] *Id.* at 792 (arguing against a *Carpenter*-like adjustment to the Fifth Amendment, Kerr emphasized evidence collection as a Fourth Amendment issue that needs to change with technology, whereas the Fifth Amendment is only concerned with the compulsion aspect); *see also Aftermath of Fisher*, *supra* note 49, at 683 ("Lower courts must recognize that *Fisher v. United States* and other recent Supreme Court decisions represent a fundamental shift in fifth amendment jurisprudence from a concern with privacy to a focus on compulsion.").

[107] Kerr, *supra* note 42, at 775 ("Whatever the merits of the 'reasonable particularity' standard in the specific context of subpoenaed documents, the test is notably unilluminating as to the government's burden outside that context.").

[108] *Id.* at 787.

[109] *See* Sacharoff, *supra* note 42, at 63 ("But when we consider the analogy to the act-of-production cases closely, and match like to like, we really should arrive at a rule different from Kerr's.").

[110] *Id.* at 63–64 ("Rather, the rule should be whether the government already knows the person possesses the files on the device and can identify them with reasonable particularity."). *But see* Kerr, *supra* note 42, at 786–87 (criticizing the Eleventh Circuit's reasonable particularity approach as unclear and, if read that way, the analysis as incorrect).

[111] Sacharoff, *supra* note 42, at 63–64.

password (as Kerr sees it) is outcome determinative.[112]

Admittedly, this doctrine has become increasingly confusing. Not only must jurists determine whether the act is testimonial, but they must then interpret what the testimony is saying to determine whether it is at issue. This task is "nearly impossible."[113] Kerr believes this to be "I know the passcode."[114] As Sacharoff points out, Kerr's understanding "violates the ordinary principles of evidence law, which draws no distinction between direct and circumstantial evidence."[115] Sacharoff sees production of the passcode as testifying "I know the password, this is, then, likely my device, and thus I likely have control over and knowledge of the contents on the device."[116] In a separate response to Kerr's article, Professor Bryan H. Choi suggests a novel idea: "treating cellphones as an extension of 'self,'" potentially creating an entire area not subject to government compulsion.[117]

Much hinges on the judicial determinations about whether the entire device or only the passcode receive the protection. Imagine that a government search warrant is executed for a cell phone. In the device decryption context, the warrant has already given the government the power to take and search the device.[118] The government may even lawfully possess the device. The only thing left to be produced is the passcode. And so, is this act of compelling decryption simply handing over the passcode, as Kerr suggests, or is there more implicit testimony that deserves protection, as Sacharoff argues?

---

[112] *See* Sacharoff, *supra* note 42, at 67 ("If the only message communicated is knowledge of the password, then Kerr is right: the government need only show the person knows the password. If, however, the act of opening the device also communicates that the person likely owns the device and the files on it, then the government must show that it already knows of and can identify with reasonable particularity the actual files it seeks, or at least a class of files such as bank records for a particular account—a higher burden.").

[113] *Id.* ("[C]ourts must perform a nearly impossible task: determine what message the act of production or the entering of a password, implicitly communicates without the normal or principled way to measure what a message means—speaker intent.").

[114] *See* Kerr, *supra* note 42, at 779 ("Entering a password is testimonial because it communicates a simple statement: 'I know the password.'").

[115] *See* Sacharoff, *supra* note 42, at 69–70.

[116] *Id.* at 70 ("If a person opens a device, we can infer she owns it, whether we denominate that act direct or circumstantial evidence.").

[117] *See* Choi, *supra* note 40, at 74 ("The theory advanced here is that those judicial decisions are best understood as treating cellphones as an extension of 'self.'").

[118] *See* Kerr, *supra* note 42, at 787 ("Most compelled decryption helps the government execute a search warrant. The Fourth Amendment requires the warrant to particularly describe the evidence to be searched for and seized.").

This act of production analog—from document production to passcode production—is far from perfect. Certainly, if the government compelled the defendant to physically hand over the passcode, it would seem similar to a suspect physically handing over documents. But what does one make of the passcode? There is simply no clean-cut way to compare paper documents to the contents of an electronic device. In addition, when considering the complex encryption software that exists to protect device data, a passcode does not seem akin to a lock or a safe.

As one can see, expanding this rationale to the device decryption context is troubling and delicate, but incredibly consequential. Unfortunately, many conflate the doctrine and entangle the Fourth and Fifth Amendment.[119] This entanglement directly conflicts with the scholarship on the foregone conclusion doctrine. The extent to which the *Fisher* Court explicitly wanted to avoid this cannot be overstated.[120]

Similar to scholarly debate, lower court decisions have not proven to be much more insightful. As I will discuss, New Jersey and Pennsylvania interpret the doctrine differently in an increasingly important area.[121] They are not alone.[122] The

---

[119] But even those who criticize the approach taken by Sacharoff and others, admit that focusing solely on the passcode is hard to do in practice. *See* Nagareda, *supra* note 25, at 1594 (emphasizing that the decoupling of documents from the act of producing those documents is a "fundamental folly" of *Fisher*).

[120] *See* Michael S. Pardo, *Disentangling the Fourth and Fifth Amendment and the Self-Incrimination Clause*, 90 IOWA L. REV. 1857, 1875 (2005) ("Subsequent doctrinal developments have torpedoed Boyd's view of the overlap."); *see also* Akhil R. Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 790 (1994) ("*Boyd*'s effort to fuse the Fourth and Fifth Amendments has not stood the test of time and has been plainly rejected by the modern Court. *Boyd*'s mistake was not in its focus on the concept of the Fourth Amendment reasonableness, nor in its laudable effort to read the Fourth Amendment Reasonableness Clause in light of other constitutional provisions. . . . Rather, *Boyd*'s mistake was to misread both the Reasonableness Clause and the Incrimination Clause by trying to fuse them together. At heart, the two provisions are motivated by very different ideas; they do not 'run almost into each other' as a general matter."); Nagareda, *supra* note 25, at 1580–81 (discussing the rejection of the *Boyd* majority's fusion of the Fourth and Fifth Amendments, but adopting Justice Miller's view of the Fifth Amendment in concurrence).

[121] *See infra* Part II.B.

[122] *Compare* State v. Stahl, 206 So.3d 124, 132–33 (Fla. Dist. Ct. App. 2016) (citing a string of cases where courts "have addressed the Fifth Amendment implications for providing decryption keys and passcodes have largely applied the act-of-production doctrine and the foregone conclusion exception."), *with* G.A.Q.L. v. State, 257 So.3d 1058, 1062–63 (Fla. Dist. Ct. App. 2018) (holding that the foregone conclusion exception applies, but then applying the reasonable particularity requirement to the underlying documents); *see also* Jesse Coulon, Comment, *Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in* State v. Stahl, 59 B.C. L. REV. E-SUPPLEMENT 225 (2018). *But see* G.A.Q.L., 257 So. 3d at 1066 (Kuntz, J. concurring)

current doctrine cannot be the right way. If we continue making courts complete this impossible task, then why not just make it up? What is the best path forward? In the next section, I use two recent cases to illustrate how the courts handle this difficult doctrine.

B. Recent Debate and Disagreement: Davis *and* Andrews

Courts across the country have struggled with the interpretation of the forgone conclusion doctrine. Some courts have strictly limited the holding of *Fisher* to document production.[123] Others have expanded the foregone conclusion analysis into other areas.[124] The courts opting to apply the foregone conclusion doctrine have mixed-and-matched the different approaches.[125] As one scholar put it, the doctrine remains "surprisingly unclear."[126] To illustrate the current state of affairs in the lower courts, I will analyze two recent conflicting cases from the Supreme Courts of Pennsylvania and New Jersey.

1. *Commonwealth v. Davis*

In *Commonwealth v. Davis*, the Supreme Court of Pennsylvania had to answer "[w]hether a defendant may be compelled to disclose a password to allow the

(disagreeing with the *Stahl* decision because the exception is "judicially created," not found within the text of the Fifth Amendment, and is of limited applicability since the exception has never applied to oral testimony).

[123] *See* Commonwealth v. Davis, 220 A.3d 534, 549 (Pa. 2019) (discussing the different approaches by the Davis lower courts); G.A.Q.L., 257 So.3d at 1061 (collecting cases).

[124] *See* State v. Andrews, 234 A.3d 1254,, 1259 (N.J. 2020) (applying the foregone conclusion doctrine to cell phone decryption); *see also* United States v. Apple MacPro Computer, 851 F.3d 238, 248 (3d Cir. 2017) (upholding a lower court's determination that the foregone conclusion doctrine applies to files on several devices). *But see In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346, 1349 (11th Cir. 2012) (applying the foregone conclusion exception, but requiring the Government show with "reasonable particularity" that it knew of the underlying materials).

[125] In *Commonwealth v. Davis*, the Supreme Court of Pennsylvania discusses the procedural history of the case. Notably, the trial court applied the foregone conclusion doctrine, yet still required the government to establish 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. While upholding the trial court decision, the three-judge panel of the Superior Court focused on *the passcode* rather than the underlying evidence. Finally, in its alternative holding, the Supreme Court of Pennsylvania believed the inquiry focused on the underlying evidence, but then held the government had not met its burden. *Davis*, 220 A.3d at 539–40, 551–52.

[126] *See* Kerr, *supra* note 42, at 774 ("Three aspects of the foregone conclusion doctrine remain surprisingly unclear.").

[government] access to the defendant's lawfully-seized, but encrypted, computer."[127] Writing for the majority, Justice Todd held such compulsion violated the Fifth Amendment Self-Incrimination Clause.[128] Because the *Fisher* Court suggested that the facts of each case are important, a brief recitation of the facts in *Davis* is warranted.[129]

In 2014, agents from the Pennsylvania Office of the Attorney General (OAG) discovered an Internet Protocol (IP) address using a file-sharing network, eMule.[130] The agents used an administrative subpoena to intercept child pornography sent to the IP address.[131] Agents determined the IP address belonged to the defendant, Joseph Davis.[132] The Government obtained a lawful warrant and seized Davis's Dell computer.[133] The hard drive had been wiped.[134] Shortly thereafter Davis's IP address came up again during another investigation.[135] The OAG agents performed this process again and, unsurprisingly, discovered another computer.[136]

After being *Mirandized*, Davis told agents he was the "sole user" of the password-protected computer.[137] Davis told the officers only he knew the

---

[127] *Davis*, 220 A.2d at 537.

[128] *Id.* (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.").

[129] *Id.*; *see also* Fisher v. United States, 425 U.S. 391, 410 (1976) ("These questions perhaps do not lend themselves to categorical answers; their resolution may instead depend on the facts and circumstances of particular cases or classes thereof.").

[130] *Davis*, 220 A.3d at 538.

[131] *Id.* at 537 ("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.").

[132] *Id.* ("The information provided by Comcast disclosed the subscriber as Appellant Joseph Davis, as well as his address.").

[133] *Id.* ("[T]he OAG applied for, received, and executed a search warrant at Appellant's apartment.").

[134] *Id.* at 538 ("Later examination of the computer revealed that the hard drive had been 'wiped,' removing data entirely or rendering it unreadable.").

[135] *Id.*

[136] *Id.* ("[T]he 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.").

[137] *Id.* ("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.").

password.[138] He claimed to watch legal pornography on the computer, that he had been arrested previously for child pornography, and did not understand why it was illegal in the United States.[139] En route to his arraignment, Davis spoke about watching pornographic movies containing minors.[140] After agents asked for the computer password, 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."[141] Davis made other statements acknowledging the incriminating nature of the documents on the computer.[142] As it turned out, the computer hard drive was completely encrypted and could not be read without opening it.[143]

Considering the Government's motion to compel Davis to divulge his password, the trial court applied the foregone conclusion exception.[144] The trial court found the government needed to "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."[145] It is worth noting that the trial court focused on the government's knowledge of the pornographic files rather than the passcode.[146] Davis, by "revealing his password," the trial court found, "would not

---

138 *Id.* ("Appellant offered that only he knew the password to his computer.").

139 *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.").

140 *Id.* ("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.").

141 *Id.*

142 *Id.*

143 *Id.* ("A supervisory agent in computer forensics . . . testified that a portion of Appellant's [computer] hard drive was encrypted . . . and 'there was no data that could be read without opening the TrueCrypt volume.'").

144 *Id.* at 539 ("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*.").

145 *Id.*

146 *Id.* ("[T]he 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." (emphasis added)).

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 . . . ."[147] Thus, the trial court believed that the foregone conclusion exception was satisfied and the government could compel the production.[148] Notably, the Superior Court of Pennsylvania upheld the trial court order, but on slightly different grounds.[149] The Superior Court centered their inquiry on the passcode itself.[150]

Beginning with the Fifth Amendment, a four-justice majority of the Supreme Court of Pennsylvania acknowledged the "series of foundational, but somewhat complex" cases discussing the act of production.[151] In reaching her decision, Justice Todd mentioned a "critical distinction" regarding physical versus testimonial production.[152] This rested on some questionable dicta in *Doe v. United States* (*Doe II*).[153]

Justice Todd was persuaded by the "critical distinction," drawn briefly in a controversial footnote, which referred to a surrendered key to a strongbox versus compelled combination to a wall safe.[154] By Todd's logic, this meant that since "a

---

147 *Id.*

148 *Id.*

149 *Id.* at 540 ("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.").

150 *Id.*

151 *Id.* at 543, 552 ("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.").

152 *Id.* at 547 ("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.'" (alterations in original) (citation omitted)).

153 Doe v. United States, 487 U.S. 201, 210 n.9 (1988). The *Doe II* Court wrestled with the issue of compelling an individual to sign a consent directive for a third party to release potentially incriminating documents, but allowed it. In response to a dissenting Justice Stevens, the *Doe* majority indisputably stated that "'[t]he expression of the contents of an individual's mind' is testimonial communication for the purposes of the Fifth Amendment." *Id.*

154 *Davis*, 220 A.3d at 547, 555 n.3. It should be noted that reliance on this line has been criticized by several commentators and other courts. *See* Kerr, *supra* note 42, at 782 (**"**In my view, *Doe II*'s dicta sheds no light either way on the Fifth Amendment implications of being forced to enter a

passcode is necessarily memorized, one cannot reveal a passcode without revealing the contents of one's mind."[155] Because a passcode is "intentionally personalized" and "so unique as to accomplish its intended purpose—keeping information contained therein confidential and insulated from discovery," it is testimonial.[156] It followed that the government sought the password "not as an end, but as a pathway to the files being withheld."[157]

Recall, however, that finding an act is testimonial does not necessarily warrant Fifth Amendment protection. Todd acknowledged as much.[158] While giving a nod to the foregone conclusion exception, the *Davis* majority called it "extremely limited."[159] Not ending there, Todd continued, "[I]t would be a significant expansion of the foregone conclusion rationale to apply it to a defendant's compelled oral or written testimony."[160] Relying in part on the *Fisher* Court's ambiguous discussion and its "intentional[] superfl[uity]," Todd put an end to any hopes of expanding the foregone conclusion rationale.[161] Others disagree, including in Pennsylvania.

Illustrative of the fragility of this analysis, the *Davis* court was divided four justices to three.[162] Writing for the three-justice dissent, Justice Baer characterized

---

password. Both statements in the dicta are truisms."). *See* Davis, 220 A.3d at 555, 555 n.3 (Baer, J., dissenting) (rejecting the applicability of the wall safe versus key distinction, Justice Baer states, "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."); *see also* State v. Stahl, 206 So. 3d 124, 134 (Fla. Dist. Ct. App. 2016) ("We question whether identifying the key which will open the strongbox—such that the key is surrendered—is, in fact, distinct from telling an officer the combination. More importantly, we question the continuing viability of any distinction as technology advances.").

155 *Davis*, 220 A.3d at 548 (Todd, J., majority opinion).

156 *Id.*

157 *Id.* ("The Commonwealth is seeking the password, not as an end, but as a pathway to the files being withheld.").

158 *Id.* ("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.").

159 *Id.* at 549 ("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.").

160 *Id.*

161 *Id.* ("Thus, generally speaking, the exception to a large degree appears to be intentionally superfluous; hence, the accommodation to the government is of limited value.").

162 *Id.* at 552 (Baer, J., dissenting).

the testimony implicit in the act of production much differently.[163] Baer viewed the implied statements of the produced passcode to include existence, possession, and authenticity of the *passcode*.[164] Rather than use the passcode "as an investigative tool," the dissent argued the government was simply seeking *access* to execute a valid warrant.[165] This, in the dissent's view, became an order of surrender rather than testimony.[166]

Turning to the foregone conclusion doctrine, Baer directly addressed the appeal of the majority's conclusion.[167] Whether it be disclosing a passcode or business records, "one would expend similar mental effort when engaging in virtually any other act of production. . . ."[168] Unconvinced by the majority's sweeping pronouncement, Justice Baer cleverly responded, "The mere fact that [defendant] 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."[169] It is no surprise, then, that Justice Baer applied the foregone conclusion exception.[170]

---

[163] *Id.* at 553 ("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.").

[164] *Id.* at 555 ("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.").

[165] *Id.* ("The Commonwealth is not seeking the 64-character password as an investigative tool . . . . 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.").

[166] *Id.* ("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.").

[167] *Id.* ("There is appeal to [the majority's] conclusion, as requiring Appellant to supply his password involves some mental effort in recalling the 64 characters used to encrypt the computer files." (alteration added)).

[168] *Id.* ("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.").

[169] *Id.* (alteration added).

[170] *Id.* at 556 ("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.") (citing United States v. Apple MacPro Comput., 851 F.3d 238, 248 n.7 (3d Cir. 2017)).

In his analysis, Justice Baer first made clear that the exception focused on the evidence sought.[171] This was the dissent's critical distinction.[172] In the dissent's view, the evidence sought was solely the passcode, rather than the underlying documents.[173] In keeping with Kerr's "treasure" versus "key" distinction, Justice Baer believed if the focal point were the underlying documents, that would be a Fourth Amendment concern.[174] On the other hand, the Fifth Amendment is only concerned with incriminating, compelled evidence—here, the password.[175]

Justice Baer justified his view on several grounds. First, Baer believed the dissent remained faithful to the *Fisher* holding.[176] Second, the dissent sought and received support from several cases from other jurisdictions that apply the foregone conclusion to the password itself.[177] Finally, the dissent emphasized that the majority's holding was largely based on form rather than substance.[178] The practical effect would be "inconsistent results."[179] For instance, according to the majority's

---

171 *Id.* ("[I]t 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.").

172 *Id.* ("This change of focus is subtle, but its effect is significant.").

173 *Id.* ("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.").

174 *Id.* ("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."); *see also* Kerr, *supra* note 42, at 797.

175 *Davis*, 220 A.3d at 556 ("[T]he 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.") (Baer, J., dissenting).

176 *Id.* ("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*.'") (citing Fisher v. United States, 425 U.S. 391, 401 (1976) (emphasis in original)).

177 *Id.* at 556–57 (citing several cases holding that the foregone conclusion exception applies to the passcode itself).

178 *Id.* at 557 (arguing that, under the majority's rationale, multi-character passwords could not be compelled, but biometric passwords could).

179 *Id.* ("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

rationale, the government could compel a "biometric password, such as facial recognition or a fingerprint," but not entering a numerical passcode.[180] Baer did not view that as relevant to cases involving today's technology.[181]

The commentators in the previous section all agreed that the compelled written passcode was protected.[182] While that may be true in theory, in practice the Supreme Court of Pennsylvania was closely and sharply divided on that question.[183] Shortly after the *Davis* decision, the Supreme Court of New Jersey engaged with a similar question.[184] In *State v. Andrews*, the Supreme Court of New Jersey sided with Justice Baer and the *Davis* dissent.[185]

2. *State v. Andrews*

Robert Andrews, a law enforcement officer, allegedly furnished the target of a narcotics investigation, Quincy Lowery, with information to avoid criminal liability.[186] The incriminating information was distributed via photograph, phone calls, text messages, and in-person conversations between Andrews and the

---

cases could depend upon the *type* of password that the individual employed to protect his encrypted files." (emphasis added)).

[180] *Id.* ("For example, according to the majority, if the accused used a multi-character password . . . 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 . . . . 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.").

[181] *Id.*

[182] *See* Sacharoff, *supra* note 42, at 68 ("[Kerr] treats the act as entering the password. . . . [I]f the password were considered the thing produced, that would violate the Fifth Amendment because then the government would be compelling the person to reveal the password from their head—even Kerr concedes that we cannot compel the password itself from a person's head." (alteration added)); *see also* Kerr, *supra* note 42, at 779 (referring carefully to the act as entering the password rather than speaking or writing it to the government).

[183] *See generally Davis*, 220 A.3d at 534.

[184] State v. Andrews, 234 A.3d 1254, 1259 (N.J. 2020) ("This appeal presents an issue of first impression to our Court – whether a court order requiring a criminal defendant to disclose the passcodes to his passcode-protected cellphones violates the Self-Incrimination Clause of the Fifth Amendment to the United States Constitution. . . .").

[185] *Id.* at 1274 ("We agree with the *Davis* dissent that the proper focus here is on the Fifth Amendment and that the Fourth Amendment's privacy protections should not factor into analysis of the Fifth Amendment's applicability.").

[186] *Id.* at 1259.

target.[187] The target gave extensive detail of this information to the State.[188] Following this admission, the State obtained warrants to arrest Andrews and search his iPhones.[189] The iPhones were encrypted and thus inaccessible to investigators.[190] The State requested an order to compel the defendant to disclose the passcodes.[191] Andrews opposed the motion.[192]

Writing for the majority, Justice Solomon briefly examined the Fourth Amendment implications of the case.[193] Careful to not entangle the Fourth and Fifth Amendment, Solomon noted the State's "broad authority to effectuate searches permitted by valid search warrants."[194] Other than the trial court's limiting instruction, there were no other limitations or restrictions imposed by the Fourth Amendment.[195] Nor did Andrews challenge the search warrants.[196] The majority then turned to the Fifth Amendment.[197]

Similar to the *Davis* dissent, the *Andrews* majority began discussing the

---

[187] *Id.* at 1260.

[188] *Id.*

[189] *Id.* at 1261 ("Following their second interview with Lowery, the State obtained Communication Data Warrants for cellphone numbers belonging to Andrews and Lowery.").

[190] *Id.* ("According to the State, its Telephone Intelligence Unit was unable to search Andrews's iPhones – an iPhone 6 Plus and an iPhone 5s – because they had iOS systems greater [than] 8.1, making them extremely difficult to access without the owner/subscriber's pass code." (alteration in original) (quotation omitted)).

[191] *Id.* ("The State therefore moved to compel Andrews to disclose the passcodes to his two iPhones.").

[192] *Id.*

[193] *Id.* at 1264 ("[B]ecause the State contends that [constitutional] protections do not allow defendant to ignore a lawfully issued search warrant, we begin with a brief review of the applicable principles of our search and seizure jurisprudence." (alteration added)).

[194] *Id.*

[195] *Id.* ("Thus, the State is permitted to access the phones' contents, as limited by the trial court's order, in the same way that the State may survey a home, vehicle, or other place that is subject of a search warrant.").

[196] *Id.* ("Andrews does not challenge the search warrants issued for his cellphones. He does not claim that the phones were unlawfully seized or that the search warrants authorizing the State to comb their contents were unsupported by probable cause.").

[197] *Id.* (citing *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019); Pardo, *supra* note 120, at 1860) ("But a lawful seizure does not allow compelled disclosure of facts otherwise protected by the Fifth Amendment.").

testimonial versus non-testimonial distinction of physical acts.[198] Justice Solomon agreed that the Self-Incrimination Clause protects against compelled disclosure of contents of the mind.[199] Yet, he contrasted, the "Fifth Amendment is not an absolute bar to a defendant's forced assistance of the defendant's own criminal prosecution."[200] After parsing several act of production cases, Justice Solomon thought it clear that precedent required a sharp, but bright, distinction between the act of producing a passcode, and the underlying documents.[201]

At one point, the *Andrews* majority squarely addressed the Pennsylvania Supreme Court's holding in *Davis*. The *Andrews* majority drew its own distinction.[202] Justice Solomon thought it clear that the act of production doctrine protected *solely* the passcode.[203] After all, Justice Solomon believed the U.S. Supreme Court's language clearly drew a "fundamental distinction."[204] As the *Fisher* Court stated, the underlying documents may not be entitled to Fifth Amendment protection, "but the act of producing them may nevertheless be protected."[205] Notably, this may well be

---

198 *Id.* at 1265 ("Testimonial communications may take any form, but must 'imply assertions of fact' for the Fifth Amendment privilege against self-incrimination to attach. Thus, actions that do not require an individual 'to disclose any knowledge he might have' or 'to speak his guilt' are nontestimonial and therefore not protected by the Fifth Amendment.") (citations omitted).

199 *Id.* at 1266 ("In contrast to physical communications, however, if an individual is compelled 'to disclose the contents of his own mind,' such disclosure implicates the Fifth Amendment privilege against self-incrimination.") (citations omitted).

200 *Id.*

201 *Id.* at 1268–69 ("From those cases, which all addressed the compelled production of documents, the following principles can be inferred: For purposes of the Fifth Amendment privilege against self-incrimination, the act of production must be considered in its own right, separate from the documents sought.").

202 *Id.* at 1271–73 (citing several cases where numerous jurisdictions have found the password to be the target of the act of production inquiry).

203 *Id.* at 1273 ("To be consistent with the Supreme Court case law that gave rise to the exception, we find that the foregone conclusion test applies to the production of the passcodes themselves, rather than to the phones' contents.").

204 *Id.* at 1273–74 ("The relevant Supreme Court cases explicitly predicate the applicability of the foregone conclusion doctrine on the fundamental distinction between the act of production and the documents to be produced . . . . In light of the stark distinction the Court has drawn between the evidentiary object and its production – a division reinforced even in those cases where the foregone conclusion exception was held not to apply – it is problematic to meld the production of passcodes with the act of producing the contents of the phones.").

205 *Id.* at 1274 (citing Fisher v. United States, 425 U.S. 391 (1976)).

the view of the Third Circuit.[206] This was the view of the three-justice dissent in *Davis*.[207] And this, Justice Solomon adopted as the law in the Supreme Court of New Jersey.[208]

In addition, Solomon made an important observation regarding passcode compulsion. Solomon emphasized, "[I]ndeed, had the State succeeded in its efforts to access the phones, this case would not be before us."[209] That is, if the government hacked the phone pursuant to a lawful warrant, or if there was no passcode on the phone, there would be no Fifth Amendment violation. This means then, that the contents of the cell phone simply cannot be the focus of the inquiry. For if there were no passcode, there would be no Fifth Amendment concern for the underlying documents. It follows that the passcode must be the target of the compulsion. Therefore, the passcode is what deserves the protection, not the documents.

It bears repeating that the *Andrews* majority also mentioned the inconsistency concerns of the *Davis* dissent regarding biometric device locks. Such holdings "create[] inconsistent approaches based on form rather than substance."[210] After all, Solomon noted, "in some cases, a biometric device lock can be established only after a passcode is created."[211] It should be no surprise, then, that immediately thereafter, the *Andrews* majority "call[ed] into question the testimonial/non-testimonial

---

[206] United States v. Apple MacPro Comput., 851 F.3d 238, 248 n.7 (3d Cir. 2017) ("It is important to note that we are not concluding that the Government's knowledge of the content of the devices is necessarily the correct focus of the 'foregone conclusion' inquiry in the context of a compelled decryption order. Instead, 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 devices is 'I, John Doe, know the password for these devices.'").

[207] Commonwealth v. Davis, 220 A.3d 534, 556 (Pa. 2019) (Baer, J., dissenting) ("[I]t 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.").

[208] *Andrews*, 234 A.3d at 1273 ("To be consistent with the Supreme Court case law that gave rise to the exception, we find that the foregone conclusion test applies to the production of the passcodes themselves, rather than to the phones' contents.").

[209] *Id.*

[210] *Id.* at 1274.

[211] *Id.*; *see also* Kristen M. Jacobsen, Note, *Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and Its Chilling Effect on Law Enforcement*, 85 GEO. WASH. L. REV. 566, 582 (2017) (discussing further the troubling distinction between numeric passcodes and biometric locks).

distinction in this context."[212]

By now, it should be clear that a court's determination about the "focus" of the foregone conclusion inquiry becomes outcome-determinative. If the exception applies to only the passcode itself, it is easier for the government to meet the burden of the foregone conclusion exception. If the government knows (1) the password exists, (2) the suspect possesses it, and (3) it is authentic, the testimonial value is "minimal." Basically, if there is a password prompt on the device, the government has information regarding the suspect's use of the phone, and the password works, then the password is a foregone conclusion.

Conversely, courts that deem the underlying documents as the "focus" of the Fifth Amendment make it near impossible for government agents to access a password-protected device that has been lawfully seized with a warrant. These courts may not only misread precedent but, in doing so, bring us back to the world of *Boyd* entanglement.[213] The entanglement does not stop there. After this critical determination, courts handle the next step differently. Some have opined that the government must know with reasonable particularity the existence, possession, and authenticity of specific documents.[214] Much of this cannot be known without access to the device itself. Meanwhile, others flatly reject the application of the foregone conclusion exception.[215] Needless to say, the malleable characteristics of this doctrine are too numerous to apply consistently. This has plagued the Fifth Amendment inquiry.[216]

---

[212] *Andrews*, 234 A.3d at 1274 ("The distinction becomes even more problematic when considering that, at least in some cases, a biometric device lock can be established only after a passcode is created, calling into question the testimonial/non-testimonial distinction in this context.").

[213] *See infra* Part II.C.

[214] *See In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012) ("[I]f the Government can show with 'reasonable particularity' that, at the time it sought to compel the act of production, it already knew of the materials, thereby making any testimonial aspect a 'foregone conclusion.'"); *see also* G.A.Q.L. v. State, 257 So. 3d 1058, 1063–64 (Fla. Dist. Ct. App. 2018) (holding that the foregone conclusion exception applies, but applying the reasonable particularity requirement to the underlying documents).

[215] Seo v. State, 148 N.E.3d 952, 958 (Ind. 2020) ("Though the foregone conclusion exception does not apply to these facts, this case underscores several reasons why the narrow exception may be generally unsuitable to the compelled production of any unlocked smartphone."); Commonwealth v. Davis, 220 A.3d 534, 549 (Pa. 2019) ("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 . . . ." (emphasis added)).

[216] *See generally* Michael J. Zydney Mannheimer, *Toward a Unified Theory of Testimonial Evidence Under the Fifth and Sixth Amendments*, 80 TEMP. L. REV. 1135, 1140–42 (2007) (discussing the current "testimonial" characterization differences under the Fifth and Sixth Amendments).

According to two sitting Justices, this obfuscation is a byproduct of the increasingly unworkable testimonial versus non-testimonial distinction.[217] After all, the testimonial versus non-testimonial distinction is the foundation of the act of production doctrine.[218] The *Andrews* majority, and other jurists, have called into question this entire principle.[219] Perhaps these device decryption cases present the perfect storm, so to speak. Maybe this is the "future case" where Justices Thomas and Gorsuch separately agreed they would be willing to reconsider the Self-Incrimination Clause. In the next section, I will briefly summarize their opinions.

C. Revisiting the Fifth Amendment's "to be a witness"

Earlier, brief mention was made to the Supreme Court's holding in *United States v. Hubbell*.[220] In that case, the majority refused to apply the foregone conclusion exception.[221] With reluctance, Justice Thomas concurred.[222] Because Thomas believed the Court properly applied the doctrine, he joined the majority;[223] but he did not stop there. Thomas emphatically stated his willingness "to reconsider the scope and meaning of the Self-Incrimination Clause."[224]

More recently, Justice Gorsuch took issue with Self-Incrimination Clause jurisprudence while dissenting in *Carpenter v. United States*.[225] There, the Court faced a difficult intersection of advanced technology and its Fourth Amendment

---

[217] *See infra* Part II.C.

[218] *See supra* Part I.B.

[219] State v. Andrews, 234 A.3d 1254, 1274 (N.J. 2020) ("The [testimonial/non-testimonial] distinction becomes even more problematic when considering that, at least in some cases, a biometric device lock can be established only after a passcode is created, calling into question the testimonial/non-testimonial distinction in this context." (alteration added)); *see also infra* Part II.C (discussing other jurists who believe the testimonial versus non-testimonial distinction should no longer be followed).

[220] *See supra* Part I.B; *see also* United States v. Hubbell, 530 U.S. 27, 43–45 (2000).

[221] *Hubbell*, 530 U.S. at 44 ("Whatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it.").

[222] *Id.* at 49 (Thomas, J., concurring) ("I join the opinion of the Court because it properly applies this [act-of-production] doctrine, but I write separately to note that this doctrine may be inconsistent with the original meaning of the Fifth Amendment's Self-Incrimination Clause." (alteration added)).

[223] *Id.*

[224] *Id.* ("In a future case, I would be willing to reconsider the scope and meaning of the Self-Incrimination Clause.").

[225] Carpenter v. United States, 138 S. Ct. 2206, 2271 (2018) (Gorsuch, J., dissenting).

implications.[226] While *Carpenter* was largely decided on Fourth Amendment grounds, Gorsuch made some germane remarks regarding the Fifth Amendment.[227] Importantly, he made clear his wariness of a return to the entangled doctrine of *Boyd*.[228] Gorsuch believed the *Boyd* doctrine had "prove[n] unworkable."[229] While alluding to "substantial evidence" of the original understanding of compelled production of incriminating evidence, Justice Gorsuch continued, "We would do well to reconsider the scope of the Fifth Amendment."[230] It is no surprise then that the originalist work of Professor Nagareda had caught the attention of the justices.

Long before its complicated extension into compelled decryption, Professor Nagareda pointed out the larger folly in *Fisher*'s act of production doctrine. Addressing the root of the doctrine's fundamental flaw, Professor Nagareda blamed the Court for continued misconstruction—or utter lack of "reasoned analysis"—of the text of the U.S. Constitution.[231] He continued, "It is precisely because the Court has not parsed the phrase 'to be a witness' but, instead, has defined it only indirectly and by implication that the Court has meandered along a mistaken doctrinal path for more than a century."[232]

Following what was, in his view, the proper path, Professor Nagareda looked to the original meaning of the text and the context within which James Madison penned the phrase "to be a witness."[233] Nagareda focused on "the absence of outcry upon Madison's change in language; the understanding of the noun 'witness' in contemporaneous sources on language; the use of similar language elsewhere in the Constitution; and, perhaps most tellingly, contemporaneous common law, which

---

[226] *Id.* at 2211–13 (majority opinion) (discussing the status of cell-site location and the issues regarding the Fourth Amendment).

[227] *Id.* at 2271 (Gorsuch, J., dissenting).

[228] *Id.* ("To be sure, we must be wary of returning to the doctrine of *Boyd v. United States* . . . .").

[229] *Id.* ("*Boyd* invoked the Fourth Amendment to restrict the use of subpoenas even for ordinary business records and, as Justice Alito notes, eventually proved unworkable.").

[230] *Id.* ("Our precedents treat the right against self-incrimination as applicable only to testimony, not the production of incriminating evidence. But there is substantial evidence that the privilege against self-incrimination was also originally understood to protect a person from being forced to turn over potentially incriminating evidence." (citation omitted)).

[231] *See* Nagareda, *supra* note 25, at 1602 ("It would be one thing if the distinction were the product of reasoned analysis—indeed, of any analysis—of the language and history of the Fifth Amendment.").

[232] *Id.*

[233] *Id.* at 1604–15.

clearly barred the compelled production of self-incriminatory documents."[234] From this historical context, Nagareda concluded that "to be a witness" must be equivalent to the phrase to "give evidence."[235]

Turning back to Justice Thomas's concurrence in *Hubbell*, he began his analysis much like that of Professor Nagareda—focusing on the word "witness."[236] Echoing Nagareda's concerns about the lack of "reasoned analysis" based on the text and its meaning at the time of the founding, Justice Thomas embarked on that historical journey to determine the originalist meaning of "to be a witness."[237] Looking to dictionaries published around the time and the eighteenth century common law privilege against self-incrimination, Thomas viewed these broad protections as "enshrined in the Virginia Declaration of Rights in 1776."[238] Importantly, that document stated, "no one may 'be compelled to give evidence against himself," and seven other States adopted that specific provision.[239] Subsequently, when ratifying the Federal Constitution, similarly worded proposals were put forth by several of those states.[240]

Cautiously, Justice Thomas mentioned *Boyd v. United States*, a case that has received significant attention in act of production doctrine cases.[241] The *Boyd* Court dealt with a complicated statute related to searches and seizures, which helps

---

[234] *Id.* at 1607.

[235] *Id.* at 1603 ("To compel a person 'to be a witness,' properly understood, is to compel that person 'to give evidence'; and it is the compulsion of that act of giving evidence in itself—whether in the form of speech, production of preexisting documents, or otherwise—that violates the Fifth Amendment.").

[236] United States v. Hubbell, 530 U.S. 27, 49–50 (2000) (Thomas, J., concurring) ("The key word at issue in this case is 'witness.' The Court's opinion, relying on prior cases, essentially defines 'witness' as a person who provides testimony, and thus restricts the Fifth Amendment's ban to only those communications 'that are "testimonial" in character.'" (citation omitted)).

[237] *Id.* at 50 ("None of this Court's cases, however, has undertaken an analysis of the meaning of the term at the time of the founding. A review of that period reveals substantial support for the view that the term 'witness' meant a person who gives or furnishes evidence, a broader meaning than that which our case law currently ascribes to the term.").

[238] Importantly, that document stated "no one may 'be compelled to give evidence against himself," and seven other states adopted that specific provision.

[239] *Id.* at 52.

[240] *Id.* ("And during ratification of the Federal Constitution, the four States that proposed bills of rights put forward draft proposals employing similar wording for a federal constitutional provision guaranteeing the right against compelled self-incrimination.").

[241] *Id.* at 55–56; *see* Boyd v. United States, 116 U.S. 616 (1886).

partially to explain the complex holding.[242] The *Boyd* majority confusingly intertwined the Fourth and Fifth Amendment.[243] For the better part of a century, subsequent decisions by the Court chipped away at *Boyd*.[244] *Fisher* flatly rejected the entangled reading.[245] Meanwhile, some believe the negative treatment of *Boyd* is misguided, especially Justice Miller's concurrence.[246]

Without saying much else, Justice Miller stated it was "quite clear" that failure to produce incriminating papers "is within the protection which the constitution intended against compelling a person to be a witness against himself."[247] So while

---

[242] *Boyd*, 116 U.S. at 619–20 (quoting language from the statute at issue); *see also* Nagareda, *supra* note 25, at 1586 ("The statute that authorized the court order was particularly draconian, providing that a refusal to produce the specified document 'shall be taken' as a 'confess[ion]' of the government's underlying allegations." (alteration in original)).

[243] *Boyd*, 116 U.S. at 633 ("We have already noticed the intimate relation between the two amendments. They throw great light on each other. For the 'unreasonable searches and seizures' condemned in the fourth amendment are almost always made for the purpose of compelling a man to give evidence against himself, which in criminal cases is condemned in the fifth amendment; and compelling a man 'in a criminal case to be a witness against himself,' which is condemned in the fifth amendment, throws light on the question as to what is an 'unreasonable search and seizure' within the meaning of the fourth amendment. And we have been unable to perceive that the seizure of a man's private books and papers to be used in evidence against him is substantially different from compelling him to be a witness against himself.").

[244] *See* Fisher v. United States, 425 U.S. 391, 414–15 (1976) (Brennan, J., concurring) ("[This decision] is but another step in the denigration of privacy principles settled nearly 100 years ago in *Boyd v. United States* . . . ." (alteration added); *see also* Nagareda, *supra* note 25, at 1578 ("In the century since Boyd, the Court has steadily retreated from this position, even as the Court has extended dramatically the protection the Fifth Amendment gives to self-incriminatory statements. In the wake of the Court's 1976 decision in Fisher v. United States and its progeny, observers accurately have described Boyd as 'dead.'").

[245] *See Fisher*, 425 U.S. at 409 ("To the extent, however, that the rule against compelling production of private papers rested on the proposition that seizures of or subpoenas for 'mere evidence,' including documents, violated the Fourth Amendment and therefore also transgressed the Fifth, the foundations for the rule have been washed away." (citation omitted)).

[246] *See generally Boyd*, 116 U.S. at 638–41 (Miller, J., concurring).

[247] *Id.* at 639 ("And I am quite satisfied that the effect of the act of congress is to compel the party on whom the order of the court is served to be a witness against himself. . . . That this is within the protection which the constitution intended against compelling a person to be a witness against himself, is, I think, quite clear."). *But see* Nagareda, *supra* note 25, at 1590 ("Justice Miller did not help his intellectual legacy by omitting the reasoning behind his conclusion. What was 'quite clear' to Justice Miller in 1886 is precisely what has eluded the Court as a whole in the century that followed. My enterprise here ultimately is to resurrect the Fifth Amendment holding of Boyd . . . by explaining the soundness of Justice Miller's view.").

most agree that the *Boyd* majority view of the intertwined Fourth and Fifth Amendment is incorrect, Justice Thomas aptly stated one thing that should be clear: "this Court unanimously held that the Fifth Amendment protects a defendant against compelled production of books and papers."[248]

At least for Justices Thomas and Gorsuch, their solution is faithful to the text of the Constitution. Reading "witness" as synonymous with "to furnish evidence" would result in wholesale change to the Fifth Amendment protection against compelled self-incrimination. At first glance, it also seems more clear-cut and simpler. But is simplicity always better? And would enough Justices decide to render useless decades worth of precedent on the act of production doctrine? It is at least plausible that the recent confusion regarding the device decryption and the foregone conclusion exception may motivate the Supreme Court to revisit the doctrine.

This Article envisions the future of the foregone conclusion doctrine through the lens of Thomas, Gorsuch, and Nagareda. While other approaches have lasted, some argue that they are unfaithful to the precedent and the Constitution. Continuing down the current path will grant us precedent only deriving from the ether. Not only that, but this entanglement of the Fourth Amendment and Fifth Amendment self-incrimination protection has been almost unanimously rejected. Although Justice Thomas called the entire act of production doctrine into question, it is not quite clear that the new regime would be much clearer. Could a foregone conclusion-type doctrine survive? That analysis is the subject of the final Part.

III. COMPELLED DECRYPTION AND THE ORIGINAL MEANING OF "TO BE A WITNESS"

If the original meaning of "be a witness" were revived, producing private papers would be considered "furnishing evidence."[249] Certainly, the government may still search and seize, or "take," documents pursuant to the Fourth Amendment. But they could no longer compel production, or compel "giving," of incriminating documents under the Fifth Amendment. Thus, document production would not survive in its current form, if it survives at all. There would be no further use for the testimonial versus non-testimonial distinction. As an exception to the act of production doctrine, foregone conclusions would be a thing of the past. The new interpretation would certainly be more sweeping and afford individuals greater

---

[248] United States v. Hubbell, 530 U.S. 27, 55 (2000) (Thomas, J., concurring).

[249] *See* Nagareda, *supra* note 25, at 1605 ("The most plausible construction of the phrase 'to be a witness' is as the equivalent of the phrase 'to give evidence' found in contemporaneous state sources.").

Fifth Amendment protection. At first blush, this new interpretation seems to suggest the government could not compel decryption of devices. But it is easy to see potential complications under the originalist interpretation. In this Part, I will discuss several uncomfortable uncertainties that may accompany compelled decryption under the new regime. Finally, I will turn to discuss the application of the new interpretation to the dueling cases in Pennsylvania and New Jersey.

A. Give or Take—It's Not That Simple

The importance of the Court defining "give" and "take" cannot be overstated. A poor interpretation could bring us right back to the testimonial versus non-testimonial regime.[250] While it is hard to speculate on the future of the Self-Incrimination Clause, the troublesome testimonial inquiry will no longer exist.[251] Even though Justices Thomas and Gorsuch both cited to Professor Nagareda's article, it would be reaching to suggest they wholly adopt the views in the article beyond the extensive research into the original meaning. This Article does not want to speculate based on a single Thomas concurrence[252] and a Gorsuch dissent, citing that Thomas concurrence.[253] It is indisputable, however, that these jurists want to revisit the doctrine based on the original meaning.

For argument's sake, this Article will proceed with the revisionist view put forward by Nagareda. That is, while the government has power through the Fourth Amendment to "take" evidence unilaterally, the Fifth Amendment protects individuals from being compelled to "give" evidence.[254] In place of the extinct testimonial versus non-testimonial distinction, courts evaluating a subpoena to compel entering a passcode to an iPhone would only have to ask whether the government compelled the person to "give evidence." That should be easier than the testimonial versus non-testimonial distinction. One cannot be so sure. After all, would courts now have to define what it means to "give" and to "take"?

To exemplify this dilemma, it is helpful to look at some examples offered by

---

[250] *Id.* at 1602 ("The creation of a separate, less protective, unduly complicated, and wrong set of Fifth Amendment principles for document subpoenas stems, at bottom, from the modern Court's implicit construction of the phrase 'to be a witness' in terms of testimonial communication.").

[251] *Id.* at 1640 ("The implications for document subpoenas are clear enough: The act-of-production doctrine announced in Fisher would be added to the list of wisely discarded constitutional doctrine.").

[252] *See Hubbell*, 530 U.S. at 50–51 (Thomas, J., concurring).

[253] *See* Carpenter v. United States, 138 S. Ct. 2206, 2271 (2018) (Gorsuch, J., dissenting).

[254] *See* Nagareda, *supra* note 25, at 1623 ("A reading of the phrase 'to be a witness' as synonymous with the phrase 'to give evidence' would lend unity to Fifth Amendment doctrine . . . .").

Professor Nagareda. First, consider when the government compels a suspect to stand in a lineup.[255] This compelled physical act, according to Nagareda, would clearly be constitutional under the new framework.[256] That is because a suspect's body would be considered "legitimately in police custody, in the same manner as the police might have obtained custody, through a duly authorized seizure, of a locked safe or computer . . . ."[257] Unhelpfully explained, this was because the government *could* "through its own investigative savvy, plus the help of Madame Tussaud's Wax Museum—ha[ve] constructed a highly accurate life-size model of a particular person and then, say, placed on the model the suspicious garment or propped up the model in a police lineup."[258] According to that rationale, so long as the object or person is in legitimate police custody, any acts incidental to that power to arrest would be considered constitutionally "taking" evidence.[259]

Similarly, this rationale could justify compelled giving of blood. Since "the Fourth Amendment places the 'persons' of 'the people' on par with their 'papers, and effects,'" the *giving* of blood could be seen as a *taking* by the government.[260] That is, in Nagareda's view, it is "taking" blood; since it requires the target to do nothing, they "literally ha[ve] to sit still," like the person in legitimate police custody standing in a lineup.[261] Again, we are left with an imperfect analogy that I am hesitant to accept.

My hesitation stems from two places: (1) the qualifying phrase amounting to "if the government can use its own investigative savvy"; and (2) Nagareda's explanation that "[t]he garment and lineup cases are readily explicable on the ground that, having legitimately seized the person of the defendant, the government effectively has constructed a life-sized model of the person's body. And, having done so, the government should be no worse off with the person's actual body legitimately in its custody than the government would have been if it had constructed a life-size model."[262]

---

[255] *Id.* at 1627–28; *see generally* United States v. Wade, 388 U.S. 218 (1967).

[256] Nagareda, *supra* note 25, at 1627 ("There plainly would be no Fifth Amendment objection . . . .").

[257] *Id.*

[258] *Id.* at 1627–28 (alteration added).

[259] *Id.* at 1628 ("[T]he mere exhibition of a person in a police lineup, like exhibition at trial itself, 'is an incident of the State's power to arrest, and a reasonable and justifiable aspect of the State's custody resulting from arrest.'").

[260] *Id.* at 1627.

[261] *Id.* (alteration added).

[262] *Id.* at 1627–28.

Applying this to the device context, does this mean that *if* the government through its own technological savvy, with the potential help of some hackers, *could* decrypt your device, then they could lawfully compel you to perform the act of entering the passcode? After all, the government lawfully has seized the phone and could hack it, shouldn't they be "no worse off"? If that were the case, our Fifth Amendment protection would ebb and flow with the advances in government investigative technology.

It just so happens that Nagareda analogized the drawing of blood to permissible device searches under the originalist regime.[263] Since the government could search devices so long as the defendant would just "sit still—figuratively—while the police might use their own ingenuity to gain access."[264] Because taking a locked device and searching it is fine, so too here, the unilateral taking of blood would be valid. In the suspect's case, his body is analogous to the device. The government drawing blood is the government extracting data. Nagareda defines each of these instances as "taking evidence."

To complicate matters, in the same stroke where Nagareda allowed device searches, he thought there was a meaningful distinction between drawing blood and lineups versus document subpoenas.[265] Nagareda claimed the whole reason compelling document production was prohibited "is that the government could not have constructed the document through its own police work."[266]

Unfortunately, if we draw the line precisely at government capabilities through its own police work, this creates distinctions based on form rather than substance. For instance, biometric passcodes could permissibly be compelled, whereas numerical passcodes likely would not be. And then, we would also have a malleable Fifth Amendment protection based on police capabilities. Perhaps there is more to it than just that. In his discussion of handwriting and voice exemplars, we get some clearer analogs to device decryption.[267]

According to Nagareda, voice or handwriting exemplars could not be compelled—it would be "giving."[268] Perhaps the most helpful instruction on the

---

263 *Id.* at 1627.

264 *Id.*

265 *Id.* at 1628 ("[T]wo of the later bodily evidence cases—involving the compelled generation of handwriting and voice exemplars—are much closer calls.").

266 *Id.*

267 *Id.* at 1628–29.

268 *Id.* at 1629 ("What the government may not do is to compel the person to produce exemplars in order to provide a link in the chain of incriminatory evidence.").

issue comes from Justice Fortas's dissent in part in *Gilbert v. California*.[269] In *Gilbert*, the Court was faced with several questions, including whether compelled handwriting exemplars violated the Self-Incrimination Clause.[270] The majority believed it constitutional.[271] Dissenting in part, Justice Fortas provided some insight when arguing that such samples should not be permitted.[272] Unlike the suspect in a lineup, a defendant giving the handwriting sample is "compelled to cooperate, not merely to submit; to engage in a volitional act, not merely to suffer the inevitable consequences of arrest and state custody; to take affirmative action which may not merely identify him, but tie him directly to the crime."[273] On the same day this case was decided, Justice Fortas took issue with voice exemplars as well.[274]

In *United States v. Wade*, the Supreme Court upheld compelled speech during lineup identifications.[275] Again, dissenting in part, Justice Fortas believed compelled voice exemplars were unconstitutional.[276] In his view, rather than "passive, mute assistance to the eyes of the victim . . . [i]t is the kind of volitional act—the kind of forced cooperation by the accused—which is within the historical permeter [sic] of the privilege against compelled self-incrimination."[277] It is here where a different line drawn might doom compelled decryption. Compelled physical decryption of one's device could be considered the sort of "cooperat[ion]" and "volitional acts" that troubled Justice Fortas.[278]

---

[269] Gilbert v. California, 388 U.S. 263, 290–92 (1967) (Fortas, J., concurring in part and dissenting in part).

[270] *Id.* at 265 (majority opinion).

[271] *Id.* at 266 ("The taking of the exemplars did not violate petitioner's Fifth Amendment privilege against self-incrimination.").

[272] *Id.* at 290–92 (Fortas, J., concurring in part and dissenting in part).

[273] *Id.* at 291–92.

[274] *See* United States v. Wade, 388 U.S. 218, 260–62 (1967) (Fortas, J., concurring in part and dissenting in part).

[275] *Id.* at 222–23 (majority opinion) ("[C]ompelling Wade to speak within hearing distance of the witness, even to utter words purportedly uttered by the robber, was not compulsion to utter statements of a 'testimonial' nature; he was required to use his voice as an identifying physical characteristic, not to speak his guilt.").

[276] *Id.* at 260 (Fortas, J., concurring in part and dissenting in part) ("[T]he accused may not be compelled in a lineup to speak the words uttered by the person who committed the crime.").

[277] *Id.*

[278] *Id.*; *see also* Gilbert v. California, 388 U.S. 263, 291–92 (1967) (Fortas, J., concurring in part and dissenting in part) (distinguishing compelled handwriting exemplars from drawing blood samples).

Personal devices, especially cell phones, are different than physical documents, and the Court has shown a willingness to treat them as such.[279] The technological differences render it nearly impossible to draw clean-cut comparisons to centuries-old examples. In the case of encrypted devices, the government already possesses the storage-keeping device, pursuant to a lawful warrant. The government has already *taken* possession of the evidence—the physical device that contains the incriminating contents. A lawful warrant gives them the right to search, seize, and *take* the contents within. But technological advances have made the device impenetrable—incomparable to a safe or strongbox. In so doing, an entire universe of documents could be unreachable from any government policing efforts—even pursuant to a lawful warrant based on probable cause. This is unlike any safe or strongbox that the government could physically take and break open through the use of force.

Without comfortable comparisons, courts must discern why the physical act of standing in a lineup is valid "take" evidence for the government, whereas handing over a key is impermissible "give" evidence. And so, another potential rationale could arise by recycling Justice Fortas's language, which could suggest that entering the passcode "is an incident of the State's power to" search and seize the device.[280] Then, requiring the defendant to remove a barrier to the government's lawful access could be considered incidental to the government's power to search pursuant to a warrant.[281] Thus, compelling the passcode would be a "reasonable and justifiable aspect of the State's custody" of the cell phone itself.[282]

The trouble I see, again, is that defining "give" and "take" is not so simple. Courts may be forced to draw these other distinctions that may also not be derived from the Constitution's text. As I noted above, the definition of "give" could turn on distinctions like cooperation versus submission,[283] if the government could recreate

---

[279] *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018); *see also* Riley v. California, 573 U.S. 373, 385–400 (2014) (analyzing the complications that cell phones pose in the Fourth Amendment context).

[280] *Wade*, 388 U.S. at 259–60 (Fortas, J., concurring in part and dissenting in part) ("[T]he exhibition of the person of the accused at a lineup is not itself a violation of the privilege against self-incrimination. In itself, it is no more subject to constitutional objection than the exhibition of the person of the accused in the courtroom for identification purposes. It is an incident of the State's power to arrest, and a reasonable and justifiable aspect of the State's custody resulting from arrest.").

[281] *Id.*

[282] *Id.*

[283] Gilbert, 388 U.S. at 291 (Fortas, J., concurring in part and dissenting in part) ("[C]ompelled to cooperate, not merely to submit . . . .").

the evidence sought by its own investigative savvy,[284] whether the suspect sits still versus performs a volitional act,[285] or acts incidental to the state's power to seize, versus non-incidental.[286] These complex distinctions look eerily familiar, not only to the testimonial versus non-testimonial, but also to the quote in *Fisher*, "The question is not of testimony but of surrender."[287] Similarly, this Article has noted how courts have long struggled with the "key to the strongbox" versus "code to a wall safe" dicta.[288]

What is clear is that under this new regime, compelled decryption of devices would be unclear. While document subpoenas would certainly not be permitted, this Article has noted how device passcodes would be treated differently from documents. After all, the government has already taken the evidence they want to look at—the cell phone or computer. It has legal authority and possession over the phone and its contents. The passcode likely provides little to no evidentiary value, beyond access to the device. It is simply a hurdle or barrier. So will courts look at the passcode as "giving" a piece of evidence, or simply a barrier impeding the government's lawful authority to "take"? In this context, a lawful Fourth Amendment search warrant giving the government legal possession and access, runs head-on into the Fifth Amendment barrier.

While at first blush, the originalist regime seems to grant broader protections to criminal defendants, decrypting the new definition will not be so simple. Although the originalist definition certainly clarifies document subpoenas better than the testimonial or non-testimonial understanding, we may be no better off in the passcode context. Not only that, currently settled Fifth Amendment questions would become unsettled; namely, handwriting and voice exemplars. In the device

---

[284] *See* Nagareda, *supra* note 25, at 1627–28 ("There plainly would be no Fifth Amendment objection if the government—through its own investigative savvy, plus the help of Madame Tussaud's Wax Museum—had constructed a highly accurate life-size model of a particular person and then, say, placed on the model the suspicious garment or propped up the model in a police lineup.").

[285] *Wade*, 388 U.S. at 260 (Fortas, J., concurring in part and dissenting in part) ("[Compelled speech in a lineup] is the kind of volitional act . . . which is within the historical permeter [sic] of the privilege against compelled self-incrimination." (alteration added)).

[286] *See* Nagareda, *supra* note 25, at 1628 ("Justice Fortas was on the right track, noting that the mere exhibition of a person in a police lineup, like exhibition at trial itself, 'is an incident of the State's power to arrest, and a reasonable and justifiable aspect of the State's custody resulting from arrest.'") (quoting *Wade*, 388 U.S. at 259–60 (Fortas, J., concurring in part and dissenting in part)).

[287] Fisher v. United States, 425 U.S. 391, 411 (1976) (quoting *In re* Harris, 221 U.S. 274, 279 (1911)).

[288] *See supra* Part II.B.

decryption context, would there be a meaningful difference between writing down a passcode versus being compelled to manually enter the code? Difficult questions certainly will arise.

B. *Application to* Davis *and* Andrews

We can make two observations about the holdings in *Commonwealth v. Davis* and *State v. Andrews*. First, the original meaning of the Self-Incrimination Clause would protect Davis and Andrews from being compelled to give the government their passcodes. Both cases involved compelled *giving* of the written passcode, rather than compelled *entering*.[289] These facts are more along the lines of compelled documentary evidence, which would become extinct under the "furnish evidence" reading. Second, if it were a compelled act of *entering* a passcode, it may well still warrant protection under the Self-Incrimination Clause. If that is the case, compelling decryption of a device would flatly be prohibited. I think that reading is more likely. This, however, may be uncertain due to the complexities accompanying devices.

Much like Justice Thomas, this Article concurs with the Supreme Court of Pennsylvania in *Davis* because the *Davis* majority properly applied the current doctrine.[290] As suggested throughout this article, however, both *Davis* and *Andrews* rest on a problematic premise. If the Fifth Amendment Self-Incrimination Clause is revised to an originalist interpretation, *Fisher* and its progeny will become inconsequential. Interpreting the Clause to prohibit compelled "furnishing" of evidence may make the document production doctrine clearer. This new approach, however, requires that courts deal differently with device decryption. Courts will be confronted with uncertainties similar to the ones mentioned above. Not only that, judges will have to deal with uncomfortable distinctions based on form rather than substance.

There are inevitable difficulties determining what exactly it means to "give" and to "take." For instance, in the context of personal devices, imagine the government lawfully seizes a device and has a search warrant for its contents. But still, the government cannot get past the encryption. Is compelling the person in custody *to enter* the passcode, more like "taking" blood and standing in a lineup? Conversely, is it more like asking someone to "give" over their documents?

---

[289] *See Davis*, 220 A.3d at 539 ("[T]he Commonwealth filed . . . a pre-trial motion to compel Appellant to *divulge* the password to his [device]." (alteration added) (emphasis added)); *see also Andrews*, 234 A.3d at 1261 ("The State therefore moved to compel Andrews to disclose the passcodes to his two iPhones." (emphasis added)).

[290] *See supra* Part II.B.1.

The standing in a lineup analogy is imperfect. It is unlike the situation outlined by Professor Nagareda. The defendant does not merely have to sit still but would have to physically push the buttons or keys to decrypt. That rationale, however, would also apply to the criminal defendant standing in a lineup. The criminal defendant would have to physically get dressed and stand in the lineup. True, the government could employ a wax sculptor, but what does one make of this analogy? The fact is, if the government did make a wax sculpture of the defendant, the defendant would not be compelled whatsoever to "give" anything. Moreover, it would likely have less evidentiary value than the physical person standing there.

Professor Nagareda's document production argument is also of no avail. Recall, Nagareda argued that in the context of document production, the government could not compel production since they could not produce the documents through their own police work.[291] But that rationale is flawed. While the government may never be able to recreate the contents of a document without seeing it, the government would eventually be able to decrypt a passcode. The government could employ the world's best hackers, analogous to Madame Tussaud's Wax Museum experts. Would a court then have to determine how likely or burdensome it would be for the government to produce the evidence on their own?[292] Or, is the mere *possibility* that the government could get the evidence through their own police work enough to allow compelled decryption? Surely, Fifth Amendment protection could not turn on such a malleable characteristic.

It should be easy to see the complications of the original meaning; namely, determining the difference between to "give" versus to "take." While a defendant or suspect clearly cannot be forced to testify in court, give an oral or written statement, or hand over incriminating documents, other areas seem murky. That grey area would include devices, but also formerly settled cases of handwriting and voice exemplars. True, some may argue that we have fixed the act-of-production doctrine by destroying it and faithfully returning to the original meaning of the Constitution. But that may not make the doctrine any easier to apply, especially in the area of compelled device decryption.

---

[291] *See supra* Part III.A.

[292] Perhaps a solution is to strip the passcode itself of its evidentiary value. For instance, if the government compels the passcode, evidence of the act must be barred from use at a subsequent trial. Formalistically, this might survive under the new interpretation. For one, the Government already has unilaterally taken the device. They lawfully are given the right to access the contents. The passcode then becomes the only target of compulsion. Rather than evidence itself, it is a hurdle or barrier to lawful government access. If that is not—and cannot be—considered "evidence," perhaps the government can compel it. For now, it is too early to speculate.

CONCLUSION

One may now see the appeal of continuing with the testimonial versus non-testimonial distinction. Because it is quite clear that no matter the interpretation, distinctions will have to be made or some arbitrary line be drawn. No matter the doctrine, there will certainly be cases where the government takes evidence pursuant to the Fourth Amendment that encroach uncomfortably on the Fifth Amendment prohibition against compelling an individual to furnish evidence. And so, while Justices Thomas and Gorsuch wait for the right future case to revisit the Fifth Amendment, it is hard to believe that the case will be a model of clarity. Difficult questions and uncertainties will arise even with the simpler sounding originalist meaning. That said, courts must decide whether difficult future questions justify remaining unfaithful to the text of the Constitution.