COMPELLED DECRYPTION AND THE PRIVILEGE AGAINST SELF-INCRIMINATION

Texas Law Review (forthcoming 2019)

Orin S. Kerr*

Abstract

This essay considers the Fifth Amendment barrier to orders compelling a suspect to enter in a password to decrypt a locked phone, computer, or file. It argues that a simple rule should apply: An assertion of privilege should be sustained unless the government can independently show that the suspect knows the password. The act of entering a password is testimonial, but the only implied statement is that the suspect knows the password. When the government can prove this fact independently, the assertion is a foregone conclusion and the Fifth Amendment poses no bar to the enforcement of the order. This rule is both doctrinally correct and sensible policy. It properly reflects the distribution of government power in a digital age when nearly everyone is carrying a device that comes with an extraordinarily powerful lock.

* Frances R. and John J. Duggan Distinguished Professor, University of Southern California Gould School of Law. Thanks to Sasha Natapoff, Laurent Sacharoff, Kevin Cole, Riana Pfefferkorn, Leah Litman, Jonathan Glater, Cristine Scott-Hayward, Robert Graham, and participants at the Southern California Criminal Justice Roundtable for comments on an earlier draft. This is a September 18, 2018 draft, please send comments to orin@orinkerr.com.

TABLE OF CONTENTS

INTRODUCTION

Encryption is everywhere. Ninety-four percent of Americans aged 18-29 carry smartphones, many of which encrypt their data by default when not in use.[1] Laptops, tablet computers, and thumb drives can be and often are encrypted.[2] Although users can decrypt electronic devices in different ways, one popular method is to enter a password.[3] To unlock the device and decrypt its contents, a person must type in a unique combination of characters that acts as the key and unlocks the device.

The widespread use of encryption has triggered an increasingly common Fifth Amendment question in criminal investigations: When can the government require a suspect to decrypt an encrypted device by entering the password?[4] 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

---

[1] *See* Mobile Fact Sheet, Pew Research Center for Internet and Technology, February 5, 2018, available at http://www.pewinternet.org/fact-sheet/mobile/ (reporting that 94% of those aged 18-29 own a smartphone).

[2] *See generally* Whitson Gordon, *The One Thing That Protects a Laptop After It's Been Stolen*, N.Y. TIMES, March 13, 208, available at https://www.nytimes.com/2018/03/13/smarter-living/how-to-encrypt-your-computers-data.html (describing how to encrypt a laptop computer or individual computer file).

[3] I use the term "password" here broadly to refer to any string of numbers, letters, or other characters that can be typed in to access data. Therefore I will label passcodes, passwords, and passphrases all as passwords. *See generally* Orin Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 994 n.24 (2018) (noting the technical differences among passcodes, passwords, and passphrases).

[4] Recent cases that have addressed this question include In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1349 (11th Cir. 2012); United States v. Apple MacPro Comput., 851 F.3d 238, 248 n.7 (3d Cir. 2017); United States v. Spencer, 2018 WL 1964588 (N.D.Ca. 2018); Seo v. State, ___ N.E.3d __ 2018 WL 4040295 (Ind. Ct. App. 2018); United States v. Mitchell II, 76 M.J. 413, 424–25 & n.5 (C.A.A.F. 2017); State v. Stahl, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016); United States v. Fricosu, 841 F.Sup.2d 1232 (D. Colo. 2012); and Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014).

objects, claiming a Fifth Amendment privilege against complying with the order.[5]

The difficult legal question is how a court should rule on the assertion of privilege: When is the order enforceable, and when would enforcing the order violate the right against self-incrimination? Put another way, how much power does the government have to compel a person to decrypt a device by entering a password? About a dozen court decisions have grappled with this question in the last decade.[6] Courts have disagreed on the correct answer,[7] as have scholars,[8] with both offering a range of standards for how the Fifth Amendment privilege should apply.[9]

This Essay answers that question in two ways. First, it offers a simple doctrinal rule that explains how the Fifth Amendment

---

[5] *See* cases cited in note 4, *supra*. This paper solely addresses the Fifth Amendment framework for compelling acts of decryption by entering passwords without disclosing it to the government. Compelled use of biometrics and compelled disclosure of passwords raise different Fifth Amendment issues. *See generally* Kerr & Schneier, *supra* note 3, at 1001-04 (summarizing the different ways of compelling action from suspects to decypt data on their devices).

[6] *See* cases cited in note 4, *supra*.

[7] *Compare* In re Grand Jury Subpoena Duces Tecum, 670 F.3d at 1349 (holding that the privilege applies unless the government can describe the incriminating files that are on the device with reasonable particularity) *with* Spencer, 2018 WL 1964588 at *3 (holding that the privilege does not apply when the government can show the suspect has the ability to decrypt the device).

[8] As Professor Sacharoff has recently explained, this is a "fundamental question bedeviling courts and scholars." Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. at 7 (forthcoming 2008), available in draft at https://papers.ssrn.com /sol3/papers.cfm?abstract_id=3156476.

[9] The scholarship on this question divides roughly between those who would interpret the Fifth Amendment as imposing a high bar to compelling a password and those who would interpret the Fifth Amendment as imposing a low bar. *Compare* Sacharoff, supra note 8 (high bar); Jason Wareham, Note, *Cracking the Code: The Enigma of the Self-Incrimination Clause and Compulsory Decryption of Encrypted Media*, 1 GEO. L. TECH. REV. 247 (2017) (same); Aaron M. Clemens, *No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or Private Key*, 8 UCLA J.L. & TECH. 2, 4 n.26 (2004) (same); *with* Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISCOURSE 298 (2014) (low bar); Timothy A. Wiseman, *Encryption, Forced Decryption, And The Constitution*, 11 I/S: J. L. & POL'Y FOR INFO. SOC'Y 525 (same); Joseph Jarone, Comment, *An Act Of Decryption Doctrine: Clarifying The Act Of Production Doctrine's Application To Compelled Decryption*, 10 FIU L. REV. 767 (2015) (same). I have also written several blog posts on this subject that argue for a low bar. *See* note 11, *infra*, for a discussion of those posts.

should apply. Expanding on my online writings about this subject,[10] it argues that the Fifth Amendment poses no barrier to compelled decryption as long as the government has independent knowledge that the suspect knows the password and the government presents the password prompt to decrypt the device to the suspect. Whenever a suspect is presented with a password prompt and is ordered to enter in the password, the only implied testimony in complying is that the suspect knows the password. That testimony will be a foregone conclusion that defeats the assertion of the privilege when the government independently can show that the person already knows the password.

My approach explains why the only federal appellate decision that squarely answers this issue, the Eleventh Circuit's 2012 decision in *In Re Subpoena Duces Tecum*,[11] either is wrongly decided or else is very confusingly reasoned. The Eleventh Circuit appears to have held that the government can compel decryption only when it can first describe with reasonable particularity what decrypted files will be found on the device.[12] This holding is incorrect. It erroneously equates the act of decrypting a device with the act of collecting and handing over the files it contains. The two acts may seem similar at first, but they have very different Fifth Amendment ramifications.

The essay next goes beyond doctrine and offers a broader perspective. In recent criminal procedure cases such as *Carpenter v. United States*,[13] the Supreme Court has signaled a willingness to

---

[10] In 2015 and 2016, I wrote several blog posts for the Volokh Conspiracy blog on the Fifth Amendment limits to decryption. In light of the continuing significance of the issue, it seemed worthwhile to expand on those posts. As a result, Part II of this essay is a greatly expanded version of arguments I have presented at the Volokh Conspiracy blog. The two most relevant blog posts are: Orin S. Kerr, *The Fifth Amendment Limits On Forced Decryption And Applying The 'Foregone Conclusion' Doctrine*, WASH. POST, June 6, 2016, available at https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine; and Orin S. Kerr, *Fifth Amendment Protects Passcode On Smartphones, Court Holds*, WASH. POST, Sept. 24, 2015, available at https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/24/fifth-amendment-protects-passcode-on-smartphones-court-holds (cited in United States v. Spencer, 2018 WL 1964588 (N.D.Ca. 2018).

[11] In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335 (11th Cir. 2012).

[12] See the discussion in notes 102-112, *infra*.

[13] 138 S.Ct. 2206 (2018).

rethink old constitutional doctrines in light of technological change. Instead of applying old doctrines mechanically, the Court has suggested, courts should reconsider old rules in light of how technology has shifted the balance of government power – a process I have elsewhere called "equilibrium-adjustment."[14] To the extent equilibrium-adjustment extends to the Fifth Amendment, beyond the Fourth Amendment sphere where it originated, cases like *Carpenter* hint that the Fifth Amendment framework for compelled decryption should look beyond precedent to the normative question: What Fifth Amendment rule offers an appropriate test in light of the role of encryption in modern life?

Here the correct doctrine is also the appropriate rule. Technology has given almost every citizen a technological tool unimaginable decades earlier. Today almost everyone carries their records in an electronic box that can be very difficult or even impossible for the government to break open. Strong encryption for everyone shifts the balance of power towards the citizen and away from the state. Before the spread of strong encryption, the search process only presented Fourth Amendment issues. Today the search process raises Fourth Amendment issues plus technological barriers plus the prospect of a Fifth Amendment bar. The result is a reverse-*Carpenter*. To the extent the doctrine is unclear, courts should interpret the Fifth Amendment so that the technology does not dramatically shift the balance of power too much against the public interest in investigating crime.[15]

The essay proceeds in three parts. Part One explains the Supreme Court's caselaw on the Fifth Amendment implications of compelled acts, namely the act of production doctrine and the foregone conclusion doctrine. Part Two applies these doctrines to compelled decryption and explains the apparent errors in the Eleventh Circuit's decision. Part Three takes a broader view and argues that its proposed doctrinal rule offers an appropriate test in light of the role of encryption in modern life.

---

[14] *See generally* Orin S. Kerr, *An Equilibrium–Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV 476 (2011).

[15] *See* Section IIIB, *infra*.

I. ACTS OF PRODUCTION AND THE FOREGONE CONCLUSION DOCTRINE

The Fifth Amendment states that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[16] This section presents an overview of the relatively specific aspect of Fifth Amendment doctrine raised by government efforts to compel entering in a password. The framework, established in *Fisher v. United States*,[17] deals with government compulsion of acts that lead to governmental knowledge of non-testimonial information. It has two parts. The first part, the act of production doctrine, assesses whether a compelled act is testimonial. The second part, the foregone conclusion doctrine, nonetheless permits compelled testimonial acts when their testimonial content is already known. This section explains the two doctrines. It then explains how the two doctrines fit together by introducing the idea of distinguishing between door-opening evidence and treasure in criminal investigations.

A. The Act of Production Doctrine

The privilege against self-incrimination applies when three conditions are met.[18] First, the person must face legal compulsion to cooperate with the government.[19] Second, the compelled conduct must be testimonial, which means that it must force a person to "disclose[] the contents" of her "own mind" and therefore "communicate" a "factual assertion" or "convey" some "information to the Government."[20] Third, the compelled testimony must be incriminating, which means that the prospect of complying "must establish reasonable ground to apprehend danger to the witness from his being compelled to answer."[21] A court must recognize an individual's privilege and block the government's effort to compel compliance only when all three conditions are satisfied.[22]

---

[16] U.S. Const. Amend. V.

[17] 425 U.S. 391 (1976)

[18] Hiibel v. Sixth Judicial Dist. Court of Nevada, Humboldt County, 542 U.S. 177, 189 (2004).

[19] *See id.*

[20] Doe v. United States, 487 U.S. 201, 210-11 (1988).

[21] *Hiibel*, 542 U.S. at 190 (quoting in part Brown v. Walker, 161 U.S. 591, 598 (1896)).

[22] *Hiibel*, 542 U.S. at 190.

The act of production doctrine considers when a compelled act is testimonial. An act is testimonial, the doctrine holds, when the act implies "tacit averments" that have "communicative aspects."[23] The basic idea is that complying with an order to *do* something can send a message just like complying with an order to *say* something. For example, say I want to find out who in my Criminal Procedure class has already taken Evidence. I can ask the class that question and let them answer in words. Alternatively, I can ask those who have taken evidence to raise their hands. In context, the act of raising hands communicates the same fact as answering "yes."

The act of production doctrine was first adopted in *Fisher*. The case considered whether it would be testimonial for a taxpayer to respond to an IRS summons seeking certain tax documents prepared by the taxpayer's accountant on Fisher's behalf.[24] According to the Court, the act of handing over papers in response to the summons implicitly testified about three different beliefs. First, it implicitly testified that the requested documents existed; second, it implicitly testified that the documents were in the person's possession; and third, it implicitly testified that the papers handed over were the documents requested.[25]

It's important to see why these three testimonial statements are implicit in the act of compelled production. An act of compliance with an order implies two kinds of beliefs. First, it implies beliefs that are necessary to comply with the order.[26] Second, an act of compliance communicates the person's belief that the act amounts

---

[23] *Id.* at 410.

[24] In a confusing twist of *Fisher*, this was only a hypothetical question in that case. *Fisher* consolidated two cases in which the government issued summons for tax documents held by the parties' attorneys. In one of the cases, No. 74-18, the attorney invoked the attorney-client privilege as a basis for refusing to comply with the summons. The parties stipulated that whether the attorney-client privilege provided a lawful basis for refusal to comply was answered by whether the client would have had a valid Fifth Amendment privilege against complying with the summons if, hypothetically, he had possessed the documents and the summons had been directed to *him*. Thus the 'facts' of *Fisher* are really a hypothetical that was answered as a result of the parties' stipulation. *See Fisher*, 425 U.S. at 402-05. To simplify matters, I will simply refer to this hypothetical as the facts of *Fisher* and refer to the client as Fisher.

[25] *Id*. at 410.

[26] That is, if doing act X requires knowing fact Y, then doing act X implies that the person knows fact Y.

to compliance.[27] In *Fisher*, producing papers in response to an order to disclose certain tax documents implies a belief that the tax documents exist because you can't hand over papers that you don't think exist. Producing them implies a belief that you possess the documents because you can't hand over what you don't think you possess. The act of production implies a belief that the papers are the tax documents requested because the production was an effort to accede to the compulsion.[28] The act of production implicitly stated, "I think these are the documents you seek." It exposed the person's thoughts about the documents' existence, possession, and authenticity.

B. The Foregone Conclusion Doctrine

That brings us to the second part of *Fisher*'s framework, the foregone conclusion doctrine. The foregone conclusion doctrine teaches that when the testimonial aspect of a compelled act "adds little or nothing to the sum total of the Government's information,"[29] any implied testimony is a "foregone conclusion"[30] and compelling it does not violate the Fifth Amendment. To apply the foregone conclusion doctrine, courts look at what the government knows before the act is compelled and ask whether the testimony implied by a compelled act is "in issue" and would add to the government's case.[31] A valid privilege exists only when the compelled act is testimonial under the act of production doctrine but is not a foregone conclusion.

The best way to show how courts apply the foregone conclusion doctrine is to study *Fisher*.[32] The Court held that the testimony implicit in handing over the tax documents was a foregone conclusion because the Government was "in no way relying on the 'truthtelling' of the taxpayer"[33] to prove it. The

---

[27] Courts label this the "act of production" doctrine because it typically applies to government orders to produce items sought by the government. The doctrine applies more broadly, however, to determine the testimony implicit in government-compelled action

[28] Production would be a "voucher of their genuineness." People v. Defore, 242 N. Y. 13, 27, 150 N. E. 585, 590 (1926) (Cardozo, J.) (quoted in Fisher, at 412 n.12).

[29] *Fisher*, 425 U.S. at 411.

[30] *Id*.

[31] *Id*. at 412.

[32] 530 U.S. 27 (2000).

[33] *Fisher*, 425 U.S. at 411.

documents "belong[ed] to the accountant, were prepared by him, and [we]re the kind usually prepared by an accountant working on the tax returns of his client." As a result, Fisher's concession that he had the documents "add[ed] little or nothing to the sum total of the Government's information."[34]

Further, Fisher's implied statement that the documents were authentic was insufficient because that implied statement did not give the government an advantage at trial.[35] "The documents would not be admissible in evidence against the taxpayer without authenticating testimony,"[36] the Court noted, and Fisher's implied statement that he believed the documents were what the government claimed was insufficient to authenticate them.[37] Fisher had not prepared the papers himself, and for purposes of authenticating documents he "could not vouch for their accuracy."[38] He was therefore not competent to authenticate the documents,[39] and his implied assertion that he believed the documents were authentic was simply his belief and not a sufficient basis to admit the documents at trial.

Three aspects of the foregone conclusion doctrine remain surprisingly unclear. The first uncertainty is whether the foregone conclusion doctrine concerns whether the implied testimony is incriminating or whether it is testimonial. *Fisher* provides no obvious answer. Because the compelled testimony implicit in the act was a foregone conclusion, *Fisher* states, the act "would involve no incriminating testimony within the protection of the Fifth

---

[34] *Id.*

[35] *Id*. at 413.

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.* At 413.The bookend to *Fisher*'s application of the foregone conclusion was provided decades later in *Hubbell*. Hubbell had been required to fully disclose his business and tax dealings as part of a prior plea agreement. In a later effort to prove that Hubbell had not complied fully with that requirement, the government subpoenaed a wide range of documents from Hubbell relating to his finances. Hubbell responded by producing 13,120 pages of documents, from which the government showed that Hubbell had in fact violated his earlier deal. The Supreme Court ruled that the foregone conclusion doctrine did not apply, and that Hubbell had a valid privilege against complying with the subpoena: "[T]he Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent."

Amendment."[40] In my view, the doctrine is better understood as concerning whether implied testimony is incriminating. The inquiry focuses on what the government knows and can otherwise prove, which doesn't change the implied statement in the act but does change whether making that implied assertion itself poses a danger to the speaker in context. But however it is characterized, the doctrine focuses on prosecutorial advantage. If the government already knows the fact or belief that is implicitly asserted, and it has some other way to prove it, then it gains no testimonial advantage by obtaining the defendant's assertions implicit in his compelled acts.

A second uncertainty about the foregone conclusion doctrine is the burden of proof to establish that a conclusion is foregone. The cases are surprising murky.[41] On one hand, courts are clear that the burden rests with the government.[42] On the other hand, there is no clear answer to how much certainty the government must establish. As Judge Calabresi recently noted for the Second Circuit, "both our court and our sister circuits have struggled with the extent of Government knowledge necessary for a foregone-conclusion rationale to apply."[43] The apparent cause of the uncertainty is that the cases typically arise when the government orders a suspect to turn over a described category of documents. In that context, courts have tended to express the burden in terms of the specificity of the government's description of the documents sought rather than the certainty of the government's knowledge.

The most often-mentioned standard is that the foregone conclusion doctrine applies if the government establishes its knowledge of the testimonial aspects of production "with reasonable particularity."[44] The basic idea is that a specific description of what the government seeks necessarily reflects greater government

---

[40] *Id.* at 414 ("We do hold that compliance with a summons directing the taxpayer to produce the accountant's documents involved in these cases would involve no incriminating testimony within the protection of the Fifth Amendment.")

[41] *See* LAFAVE, ET AL, CRIMINAL PROCEDURE § 8.13(a) (4th Ed. 2015) (notingthe uncertainty).

[42] *See, e.g.,* In re Grand Jury Proceedings, Subpoenas for Documents, 41 F.3d 377, 380 (8th Cir.1994) ("The government bears the burdens of production and proof on the questions of ... possession[ ] and existence of the summoned documents.")

[43] United States v. Greenfield, 831 F.3d 106, 116 (2d Cir. 2016).

[44] *Id.* at 116 (quoting In re Grand Jury, 1 F.3d 87, 93 (2d. Cir. 1993).

knowledge about it. If the government's specific description of the documents to be handed over shows that the government already knows their existence, possession, and authenticity -- the testimonial aspect of production -- then the foregone conclusion doctrine applies.[45] If the government can pinpoint what it needs, the thinking runs, then it is not relying on the truth-telling of the person complying with the order to figure out its case.

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. The government can compel an act that has testimonial qualitied but does not require the government to describe the evidence it is seeking. The act may be to do something, not to go get something. As a result, there may be no evidence for the target to retrieve that can be described with "reasonable particularity." The nature of the burden of proof in outside of orders to compel documents remains surprisingly unclear.

A final uncertainty with the foregone conclusion doctrine is whether the government can introduce the defendant's testimonial act at trial. Here's the question: If the government orders a testimonial act as part of the investigation, and it then overcomes assertion of privilege by showing that it has independent knowledge of the implied testimony that renders it a foregone conclusion, can the government later tell the jury about the defendant's implied testimony to help prove the defendant's guilt? Or is the government barred from relying at trial on testimonial foregone conclusions?[46]

There is surprisingly little caselaw on this question.[47] In my view, it would be appropriate for governmental reliance on the

---

[45] *Greenfield*, 831 F.3d at 116-18.

[46] Notably, this question is distinct from whether the government can grant immunity to a suspect limit to the act of production and then use the documents obtained as a result of the production. The Supreme Court answered that latter question "no" in United States v. Hubbell 530 U.S. 27, 42-43 (2000). *See generally* United States v. Ponds, 454 F.3d 313, 321 (D.C. Cir. 2006) (noting that *Hubbell* held that if immunity is granted, "the use of the contents of produced documents" are a "barred derivative use of the compelled testimonial act of production"). How far a grant of immunity must extend involves a separate question from whether the government can introduce evidence at trial when no immunity has been granted. S*ee generally* Kastigar v. United States, 406 U.S. 441 (1972); United States v. Doe, 465 U.S. 605 (1984).

[47] One district court decision has held that the government cannot rely on the foregone conclusion doctrine and then introduce evidence of the defendant's testimonial act at trial. *See* United States v. Spencer, 2018 WL

foregone conclusion doctrine to imply a subsequent bar to using that implied testimony at trial. This is a sensible limit based on estoppel principles: If the government's power to compel an act depends on not needing testimony the act implies, the government should not be allowed to later use the implied testimony it claimed not to need.[48] But this is only my view of a question that the caselaw has not clearly settled.

C. The Foregone Conclusion As A Bar to Manipulation Between Door-Opening Evidence and Treasure

Some readers may be wondering how these two doctrines fit together. The act of production doctrine is reasonably intuitive. It measures implicit testimony in an act, relating the act to the Fifth Amendment's core concern of compelled testimony. But the foregone conclusion doctrine may seem strange. The doctrine acts as an exception to the act of production doctrine. But why? There is no obvious analog to it when the government compels an answer to a direct question. It's fair to wonder why the doctrine exists.[49]

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 non-testimonial evidence. The problem is rooted in an important difference between the investigative consequences of

---

1964588 *3 (N.D.Ca. 2018) ("Once Spencer decrypts the devices, however, the government may not make direct use of the evidence that he has done so.") (citing Robert P. Mosteller, Simplifying Subpoena Law: Taking the Fifth Amendment Seriously, 73 Va. L. Rev. 1, 110 n.108 (1987)). The D.C. Circuit has dicta somewhat relevant to this issue that can be read either way. *See* In re Sealed Case, 832 F.2d 1268, 1281 n.8 (D.C. Cir. 1987) (stating in dicta that if the government seeks to use the testimonial aspect of production at trial that had been earlier declared a foregone conclusion, the defendant can then challenge a second time whether the foregone conclusion test was satisfied).

[48] The Supreme Court adopted a somewhat similar limit in Braswell v. United States, 487 U.S. 99 (1988), where the Court held that the government can compel a corporate custodian to produce records but cannot then use the act of production against the custodian in his personal capacity. *See id.* at 117-18. *See also Spencer*, 2018 WL 1964588 at *3 ("If it really is a foregone conclusion[,] . . . the government of course should have no use for evidence of the act of production itself.").

[49] *See, e.g.,* Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. Pitt. L. Rev. 27, 48-50 (1987) (noting that *Fisher* "left substantial doubt about what it meant by 'a foregone conclusion.'"); Robert P. Mosteller, *Simplifying Subpoena Law: Taking the Fifth Amendment Seriously*, 73 Va. L. Rev. 1, 29-34 (1987) (considering different rationales for the foregone conclusion doctrine).

compelling answers and compelling acts. When the government forces a person to answer a question, it collects only one kind of evidence. The government asks a question, and the person answers it. The government learns only the answer. The situation is different when the government compels acts instead of words. The purpose of compelling acts is to obtain evidence that the acts can help reveal. The government wants the person to open a door to obtain some treasure that opening the door reveals.

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 non-testimonial evidence revealed as a consequence of that act. Let's call that the treasure. When the government compels a person to open the door and let the government see the treasure inside, it obtains both the door-opening evidence and whatever treasure is revealed.

Consider a case like *Fisher*, where the government compels a person to hand over the accountant's tax documents.[50] 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 tax documents. Second, it provides access to the treasure, the documents that the government is seeking. The door-opening evidence is compelled testimony. But the treasure, what the government finds in the documents, is *not* compelled testimony.[51] As a practical matter, the door-opening evidence operates causally as a testimonial gateway to the non-testimonial treasure. The government may be unable to obtain the treasure without the door-opening. But the two are analytically distinct, and only the latter is compelled testimony.

The best explanation for the foregone conclusion doctrine is that it prevents the causal relationship between door-opening evidence and treasure from being used to shroud the treasure in the Fifth Amendment protection properly afforded the door-opening. Without the foregone conclusion doctrine, suspects could take

[50] Or at least this was the hypothetical on which the decision in Fisher rests. See the discussion in note 38, *supra*.

[51] The fact that government action leads to the acquisition of contents of the documents does not raise Fifth Amendment problems, *Fisher* explains, because the contents of the documents are not themselves compelled.

simple steps to introduce testimonial doors that block government access to their non-testimonial treasures. A person in Fisher's situation, for example, could just make sure to gather all of his records and keep them in his possession. Any act of production would have to be compelled from him instead of from the accountant, introducing an act that implies the person's testimony under the act of production doctrine.[52]

The foregone conclusion doctrine blunts the advantage from such manipulation. It evaluates if the door-opening testimony is significant or is merely a matter of easily-manipulated form. If opening the door implies incriminating testimony that the government does not already know, then the risk of compelled self-incrimination is real and the person has a privilege against opening the door that then necessarily blocks access to the treasure. On the other hand, if opening the door gives the government no prosecutorial advantage, then the risk of compelled self-incrimination is only a matter of form. At that point, as *Fisher* recognized, quoting Justice Holmes, "the question is not of testimony but of surrender."[53] 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.

II. APPLYING THE FIFTH AMENDMENT TO COMPELLED ENTERING OF PASSWORDS

We can now apply these doctrines to a compelled act of decryption. Let's return to the scenario described in the introduction. The government has a seized electronic storage device in its possession, but efforts to search the device are blocked by encryption. Seeking access, the government obtains a lawful order directing a particular person enter in the password to unlock the device. If the person pleads the Fifth, how should a court rule?

---

[52] Because the Fifth Amendment privilege is personal, the accountant could not assert the privilege on the client's behalf. *See id.* at 399-400.

[53] *Fisher*, 425 U.S. at 411 (quoting In re Harris, 221 U.S. 274, 279 (1911)). As Justice Holmes explained in *Harris*, "he right not to be compelled to be a witness against oneself is not a right to appropriate property that may tell one's story." *Harris*, 221 U.S. at 279.

This section argues that a court should reject the claim of privilege whenever the government has independent knowledge that the person knows the password. Entering a password that unlocks a device has a testimonial component: It testifies that the person knows the password that unlocks the device. But the foregone conclusion doctrine applies when the government has independent knowledge of that fact. This standard allows the government to compel a suspect to enter a password in many but not all cases. It also shows that the Eleventh Circuit's apparent confusion in the first federal circuit court on compulsion to enter a password, *In Re Subpoena Duces Tecum*.[54] This section begins by applying the act of production doctrine; turns next to the foregone conclusion doctrine; and concludes with a critical take on the Eleventh Circuit's decision.

A. The Testimonial Aspect of Entering in a Password

The first question is whether the compelled act of entering in the password that unlocks the device amounts to testimony under the act of production doctrine. The answer is clearly yes. Entering a password is testimonial because it communicates a simple statement: "I know the password." A person can be successfully ordered to do only what he has sufficient knowledge to do. If a person knows the password, he can enter it and unlock the device. If a person doesn't know the password, however, he can't enter it. As a result, the act of entering in the password and unlocking the device has simple testimonial significance. It amounts to an assertion that the person knows the password.

Importantly, "I know the password" is the only assertion implicit in unlocking the device. Because the password is entered without revealing it to the government, any communicative content that its characters might contain (such as a hypothetical password, "ISELLDRUGS") is not asserted to the government.[55] In addition, the act of unlocking the device does not communicate knowledge about the device's contents. Knowing the password and knowing the contents of a decrypted device are two different things. One person might know the device's contents but not know the password.

[54] 670 F.3d 1335 (11th Cir. 2012).

[55] In that sense compelled decryption is more like being forced to surrender a key to a strongbox containing incriminating documents than being compelled to reveal the combination to a wall safe. *See* Doe v. United States, 487 U.S. 201, 210 n.9 (1988).

Another person might know the password but not know the device's contents.

The distinction is worth illustrating with an example. I happen to know the passcode to my sister's smart phone.[56] I learned it at a family event when I wanted to use her phone to google something. I asked her for the passcode, and she told me. If the government obtained a court order requiring me to enter in the password, I could comply with the order because I know the password.[57] But critically, I have no idea what files are stored in my sister's phone. The only thing I know about my sister's phone is its password. Unlocking the phone would admit I know the passcode, but it wouldn't admit that I know what is on the phone. Because I don't.

At this point the reader may push back. Unlocking a device doesn't necessarily indicate knowledge beyond the password. But doesn't it give some good hints? After all, we normally know the passwords to devices that we regularly use. A statement admitting knowledge of a password can reveal some good clues about the device's ownership or use. Use could give the government some idea about a person's knowledge of its contents. Given all of this, it might seem that there is more testimonial content to unlocking the phone than merely the statement that the person knows the passcode.

I think this argument is wrong. It mistakenly assumes that a testimonial statement about one subject also testifies to plausible implications to be drawn from that statement. The plausible implications of a statement may make the statement incriminating, but they don't amount to additional testimony. Imagine a witness who is asked on the stand if she was present at the crime scene. Answering that question may be incriminating, as it may place her in danger of being implicated in the crime.[58] Knowing the witness was at the crime scene could help the prosecutor show her involvement in the crime. Nonetheless, admitting presence at the

---

[56] This example is adapted from my blog post, Orin S. Kerr, *The Fifth Amendment Limits On Forced Decryption And Applying The 'Foregone Conclusion' Doctrine*, WASH. POST, June 6, 2016, available at https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine.

[57] At least assuming my sister hasn't since changed it.

[58] *See* Resnover v. State, 507 N.E.2d 1382, 1389-90 (Ind. 1987) (recognizing a Fifth Amendment privilege for a witness facing compulsion to testify that she was present at the crime scene).

crime scene is distinct from admitting criminal involvement. The ability to draw an inference from testimony does not amount to testimony about that inference.

Some have argued that compelled decryption has broader testimonial significance because it effectively creates the evidence decrypted.[59] The apparent thinking is that decryption causes information to exist that did not exist before, itself resembling an act of speech that adds to the testimony inherent in the act.[60] This argument is wrong because it misses the distinction explained earlier between door-opening evidence and treasure. To be sure, the treasure revealed by door-opening can be extremely incriminating speech. It might include a signed confession. It might contain video of the defendant committing the crime. The door-opening may make that evidence exist in a way it did not exist in encrypted form. But all of this is irrelevant to the privilege against self-incrimination. The act of production doctrine considers the actor's communication implicit in the act, not what communications may result from the act. How incriminating the treasure may be, or what the computer does when a person opens the door, does not change the testimony implicit in the door-opening act.[61]

A similar error is to claim that entering a password has broader testimonial significance because it is akin to translating the entire encrypted contents from ciphertext to plaintext. On this thinking, entering the password is like a witness taking the stand and translating documents from a secret language into English. But this analogy doesn't work. Assuming that an act of translation could be incriminating,[62] and that the act of production doctrine would apply

---

[59] *See, e.g.,* Seo v. State, --- N.E.3d ----, 2018 WL 4040295 at *11 (Ct. App. Ind. 2018) ('We also consider [the act of decryption] testimonial because her act of unlocking, and thereby decrypting, her phone effectively recreates the files sought by the State.").

[60] *See id.* at *11 ("Because compelling Seo to unlock her phone compels her to literally recreate the information the State is seeking, we consider this recreation of digital information to be more testimonial in nature than the mere production of paper documents.")

[61] *Cf.* In re Application for a Search Warrant, 279 F.Supp.3d 800, 805-06 (N.D. Ill. 2017) (explaining why use of a biometric to decrypt does not gain testimonial significance based on the information revealed; "this argument . . . relies on conflating what it means for an act to be inherently testimonial versus an act yielding an incriminating result.").

[62] *Cf.* United States v. Burr, 35 F. Cas. 38 (C.C. Va. 1807) (Marshall, C.J.) (ruling that Aaron Burr's private secretary could not be compelled to testify about the meaning of Burr's encoded communications).

to it, the testimonial aspect of translation is knowing how to translate from one language to another. In contrast, entering a password implies no such knowledge. Take the case of my sister's phone. If I enter the password and the phone unlocks, my entering the password implies no knowledge about how the phone's encryption software works. I don't even know what kind of phone my sister has. The only testimony implicit in unlocking her phone is the only thing I know: The password.

A final wrong turn worth addressing is the claim that the wall safe hypothetical in *Doe v. United States,* ("*Doe II"),* [63] can settle the testimonial content of entering in a password. *Doe II* held that being compelled to sign your signature to a consent directive is not testimonial.[64] Dicta in a footnote echoed Justice Stevens' view, expressed in dissent, that that a suspect "be[ing] compelled to reveal the combination to his wall safe" by "word or deed" would be testimonial but that "in some cases be[ing] forced to surrender a key to a strongbox containing incriminating documents"[65] would not be. It's fair to ask if *Doe II*'s dicta answers how the Fifth Amendment applies to compelled decryption.[66]

In my view, *Doe II*'s dicta sheds no light either way on the Fifth Amendment implications of being forced to enter a password. Both statements in the dicta are truisms. That revealing the combination to a wall safe is testimonial should be obvious. It is a statement of a person's thoughts revealed to the government. That does not answer how the same principles apply to an act of decryption, however, because an act of decryption does not reveal the password. Granted, it's possible that the idea of revealing the combination "by deed" was intended to include opening a combination safe for investigators without actually revealing the combination. If so, that passage suggests the same conclusion reached in this section: Using the combination to open the safe testifies that the person knows the combination just as entering a

---

[63] 487 U.S. 201(1988). The label "*Doe II*" distinguishes the case from another Fifth Amendment case, United States v. Doe, 465 U.S. 605 (1984).

[64] *See Doe II*, 487 U.S. at 219 ("Because the consent directive is not testimonial in nature, we conclude that the District Court's order compelling petitioner to sign the directive does not violate his Fifth Amendment privilege against self-incrimination.")

[65] *See id.* (Stevens, J., dissenting). Justice Stevens suggested this distinction in his dissent, and the majority then indicated in a footnote that the Court agreed with the basic distinction. *See id.* at 210 n.9.

[66] *See id.* at 210 n.9

password to decrypt data testifies that the person knows the password. But that meaning is not at all clear from the brief line in *Doe II*, which on its face is about "reveal[ing] the combination"[67] and not just unlocking the safe.

Similarly, the Court's apparent view that being compelled to surrender a key would not be incriminating "in some cases" is also unilluminating. Note the caveat: in some cases. It's easy to think of examples where surrendering a key would not be incriminating. Imagine the police are searching a business, find a locked safe, and see a suspect with the safe key in his hand. The police order the suspect to drop the key and put his hands up. In that case, surrendering the key would not be testimonial. Compliance with the order would not reveal the contents of the suspect's mind. But that sheds no light on how the Fifth Amendment might apply to other efforts to force a person to surrender a key, such as issuing a subpoena requiring the target to collect the key and give to the grand jury. That kind of "surrendering" the key would be testimonial, in my view, as it admits to the existence, authenticity and possession of the key just like the it did the documents sought in *Fisher*. The answer must come from the framework identified in *Fisher*, not from the vague and unilluminating dicta from *Doe*.

B. Applying the Foregone Conclusion Doctrine to Password Entering

We now turn to how the foregone conclusion doctrine applies to an act of compelled decryption. Recall that to apply the foregone conclusion doctrine, we ask if the government gained a prosecutorial advantage by obtaining the testimony implied by the compelled act. In the language of *Fisher*, the question is whether the implied testimony is "in issue" or if obtaining it "adds little or nothing to the sum total of the Government's information"[68] for purposes of a future prosecution.

Although the foregone conclusion doctrine is often applied in a fact-specific way, a simple rule emerges when the government orders a suspect to enter a password to decrypt a device. As explained above, the only assertion implied by entering the correct password is that the person compelled knows that password. That yields a simple insight: The implied testimony cannot be in issue, and cannot add to the sum total of the Government's information,

[67] *Id.*
[68] *Fisher*, 425 U.S. at 411.

when the government provides the device to the suspect at the password prompt and the government already knows that the person knows the password. The testimony is a foregone conclusion and a court should not recognize the privilege because the government has independent proof of the entire testimonial content of the compelled act.

A bright-line rule results: When investigators present a suspect with a password prompt, and they obtain an order compelling the suspect to enter in the correct password, the suspect cannot have a valid Fifth Amendment privilege if the government independently can show that the suspect knows the password. The government's independent evidence that the suspect knows the password means that the suspect's knowledge is not in issue. It adds nothing to the sum total of the government's information for the government to learn what it already knows. As a result, the government's independent knowledge that the person knows the password makes the implied testimony of entering it a foregone conclusion.[69]

This standard should be easy for the government to satisfy in many common cases. Individuals ordinarily must know the password of devices that they regularly use. As a result, evidence that the person regularly uses a particular device should generally be sufficient to show knowledge of the password and trigger the foregone conclusion doctrine. Imagine the government seizes an encrypted smart phone from a suspect's pocket incident to his arrest.[70] The suspect's fingerprints are on the phone. Calling the suspect's known phone number makes the phone ring. In such a case, the evidence will likely indicate that the person knows the password. Establishing a foregone conclusion will pose a low bar that the government can readily meet

There are a few important caveats to make. First, a different analysis is called for when a person's awareness of the password is in issue. In such a case, the Fifth Amendment should impose a bar to compelling the act. Imagine the government obtains a search warrant to search a home for computer-stored images of child pornography. The home has three residents. The search yields one computer, and that computer has an encrypted hard drive that requires a password to use. Further assume that investigators have

---

[69] *Accord* Jarone, *supra* note 9, at 792-96.

[70] *Cf.* Riley v. California, 573 U.S. __ (2014) (requiring a warrant to search a cell phone seized incident to arrest).

no evidence about which resident owns or uses the computer. In an effort to bypass the encryption, investigators obtain court orders requiring each of the three residents to enter the password.

In such a case, each resident would have a valid Fifth Amendment privilege against complying with the order. Entering the password would show knowledge of it. Establishing knowledge would help show criminal possession of the images that may be on the computer. In a prosecution for possession of those images, a person's awareness of the password required to access the images would be "in issue."[71] If the prosecution had no information that any particular resident knew the password, each resident would have a privilege not to be compelled to enter the password to reveal they knew it. Knowledge of the password would not be a foregone conclusion.

A second important caveat is that a valid privilege can exist when the government's order includes an implicit search requirement. The critical difference is between an order to enter a password at a password prompt and an order to take a broader set of steps to produce the files in decrypted form. When agents present the user with a password prompt and compel him to enter the password, the implicit testimony is a foregone conclusion when the government can show the user knows that password. But it's a different case if agents obtain an order to produce a decrypted version of all files on the device. An order to produce all encrypted files can have an implicit search requirement: Compliance can require more than just entering a password.

The reason for the difference is that encryption is not all or nothing. A user might first encrypt a particular file and then encrypt the entire device that includes that file. A user might encrypt files in a "hidden volume" that the government can't tell exists and cannot locate without the user's help.[72] In these situations, producing the files on the device in encrypted form have more testimonial significance than merely stating knowledge of the password. Depending on the case, the production might require admitting to knowledge of the hidden volume or the presence and location of additional encrypted files. Put another way, complying with an

---

[71] *Fisher*, 425 U.S. at 412.

[72] *See* Aloni Cohen& Sunoo Park*, Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, Harv. J. L. & Tech (forthcoming 2018) available at https://papers.ssrn.com/sol3/papers.cfm ?abstract_id=3117984 at 28-29 (discussing hidden volumes).

order to produce all of the files on a device in decrypted form may require knowledge beyond just how to bypass a password gate presented to the user. In such a case, the foregone conclusion doctrine would apply only if all of the implicit statements required to conduct the search are themselves foregone conclusions. Mere knowledge of a password would not be enough.

One way to deal with this complication would be for decryption orders to order bypassing password gates instead of producing plaintext. The order could command the subject of the order to enter in passwords needed to bypass password gates presented to the subject on a particular device. The order would compel only the act of entering a password and it would not compel any searching.[73] If at any point the target asserted his Fifth Amendment right, a court could address whether the government can show independently that it knows the target knows that particular password. This approach to drafting decryption orders could avoid the possibility of an implicit search requirement that could complicate the Fifth Amendment analysis.

C. The Eleventh Circuit's Apparent Misstep In re Subpoena Duces Tecum

An important implication of my argument is that the only federal court of appeals decision directly addressing this issue, the Eleventh Circuit's ruling in *In re Subpoena Duces Tecum*,[74] is either wrongly decided or at least very confusingly written. Other courts may be understandably reluctant to disagree with a precedential

---

[73] The language of my proposed Decryption Order might state: "John Doe is hereby ordered, when presented with a password prompt on the device described below, to enter in the password needed to bypass that password prompt." The order could then describe the device.

It is possible that a device could be configured with multiple passwords, including a special password that does not decrypt all data but instead presents users with only some of the decrypted data. *See id.* at 28-31 (describing "deniable encryption"). But use of such a password seems unlikely to raise significant Fifth Amendment issues. The deniability of the encryption means that the government will not realize what the user has done. Further, whether use of such a password violates the Decryption Order depends on how the order is drafted. If the government has reason to think that a suspect has used such technologies, that raises practical problems with proceeding by compelled decryption rather than Fifth Amendment challenges. *See also* Kerr & Schneier, *supra* note 3, at 1005 (discussing remedies for failure to comply with court orders to decrypt).

[74] 670 F.3d 1335 (11th Cir. 2012).

circuit court opinion. But the opinion appears to be based on an mistake that other courts should not make.

Here's a quick rundown of the facts. A suspect known only as John Doe was served a subpoena requiring him to produce the decrypted contents of several of Doe's hard drives that were believed to contain child pornography.[75] A forensic examination of Doe's hard drives showed that they were partially encrypted with a program called TrueCrypt.[76] The examiner could access parts of the hard drives, but they were blank. At the same time, the examiner was "unable to access certain portions of the hard drives" that were encrypted using TrueCrypt.[77] The examiner could see the raw data on the drives and knew that TrueCrypt had been used. But he could not know what information (if anything) would be revealed when decrypted.[78]

In an opinion by Judge Tjoflat, the Eleventh Circuit concluded that Doe had a valid privilege against self-incrimination and could not be compelled to comply with the subpoena. Unfortunately, the court's analysis of the testimonial aspect of compulsion was very brief. According to Judge Tjoflat, complying with the subpoena would amount to Doe's testimony of his "knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files."[79] Unfortunately, the opinion contains no analysis of why these assertions would be implicit in completing the ordered act.

The court then concluded that the foregone conclusion doctrine did not apply. According to Judge Tjoflat, the foregone conclusion doctrine would apply only "if 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."[80] That was not the case, however, because "we simply do not know what, if anything, was hidden based on the facts before us."[81] According to Judge Tjoflat, the foregone conclusion doctrine could not apply

---

[75] *Id.* at 1337.
[76] *Id.* at 1340.
[77] *Id.* at 1340 n.10.
[78] *Id.* at 1340.
[79] *Id.* at 1346.
[80] *Id.*
[81] *Id*. at 1347.

because the government did "not know what, if anything, is held on the encrypted drives."[82]

The problem with applying the foregone conclusion doctrine, the Eleventh Circuit concluded, was that the government did not describe the documents it was seeking with sufficient specificity.[83] The government had not shown sufficient "knowledge as to the *files* on the hard drives at the time it attempted to compel production from Doe."[84] Without knowing "to any degree of particularity what, if anything, was hidden behind the encrypted wall,"[85] the government could not describe the files it was seeking with reasonable particularity and the foregone conclusion doctrine could not apply.

The Eleventh Circuit's reasoning is not a model of clarity. It can be read different ways. In my view, the most faithful reading is that the opinion requires the government to describe with reasonable particularity the decrypted documents it will find before an act of decryption is a foregone conclusion.[86] If so read, the Eleventh Circuit's analysis is wrong. It fails to distinguish two different roles a target can serve in carrying out a search. If evidence is in a locked box, investigators might order a suspect to unlock the box and do no more. Investigators can then take over the search, investigating the contents of box themselves and looking for the evidence. On the other hand, investigators might order a suspect to unlock the box and then execute the search himself on the government's behalf. The suspect might be ordered to unlock the box, search it, find a particular set of documents described, and then bring those responsive documents to the government. The first target role is unlocking; the second target role is unlocking and searching.

---

[82] *Id.*

[83] *See id.* ("Case law from the Supreme Court does not demand that the Government identify exactly the documents it seeks, but it does require some specificity in its requests—categorical requests for documents the Government anticipates are likely to exist simply will not suffice.")

[84] *Id*. (emphasis in original).

[85] *Id.*

[86] This interpretation is perhaps easiest to establish by how the Eleventh Circuit distinguished the contrary result in In re Boucher, No. 2:06–mj–91, 2009 WL 424718 (D.Vt. Feb. 19, 2009). According to the Eleventh Circuit, "it was crucial" to the result in *Boucher* "that the Government knew that there existed a file under [an incriminating] name." *In re Subpoena*, 670 F.3d at 1348-49. In the Eleventh Circuit's view, it appears, the foregone conclusion doctrine hinged on the government's knowledge of the file.

Under my reading of the case, the Eleventh Circuit missed this distinction. It treated a case in which the target's role was unlocking the device as if the target's role had been unlocking the device and then searching it for described evidence. When a suspect is ordered to produce a decrypted version of an electronic device, the compelled act ordinarily will be only to unlock the device. Any additional searching is the government's job, and the government need not know the what it will find when it begins to look. Whether the government knows enough about the incriminating evidence it hopes to find to describe it with reasonable particularity is simply irrelevant if government, not the target, is going to look for it. If the target doesn't have to search for the evidence the government is seeking, the target doesn't need a specific description to establish a foregone conclusion.

Granted, 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. Most compelled decryption helps execute a search warrant. The Fourth Amendment requires the warrant to particularly describe the evidence to be searched for and seized.[87] It might seem, at first blush, that Fourth Amendment's particularity requirement serves the same function as the common Fifth Amendment foregone conclusion requirement of reasonable particularity. Both help limit the searcher's discretion as to what is seized.[88]

But they do so for quite different reasons. The Fourth Amendment's particularity requirement prevents general searches.[89] It limits the searcher's discretion to ensure that he does not take away too much.[90] In contrast, the particularity standard relied on in Fifth Amendment foregone conclusion cases prevents implied statements. It limits a target's discretion to ensure that the government isn't relying on assertions implicit in the choices a target makes to carry out the order. The two standards serve different roles and satisfy different standards. When the government obtains a search warrant and a related decryption order, the only relevant

[87] U.S. Const. Amend IV.

[88] A classic (if plainly exaggerated statement) of the role of Fourth Amendment particularity is that, "[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant." Marron v. United States, 275 U.S. 192, 196 (1927).

[89] *See* Andresen v. Maryland, 427 U.S. 463, 480 (1976).

[90] *See Marron*, 275 U.S. at 196.

particularity requirement comes from the Fourth Amendment's warrant clause.[91] After the target unlocks the device, his work is done. The government must now execute the warrant to search for the evidence particularly described within it.

I noted above that there is a second way to read the Eleventh Circuit's opinion. Under the second interpretation, the opinion is confusing and poorly written but its result may be correct. Here's why. Recall that Doe was ordered to produce a decrypted version of the files on his devices that were encrypted using TrueCrypt. TrueCrypt allows users to place files in hidden volumes.[92] It's possible that Doe's Fifth Amendment objection was to being ordered to identify hidden volumes on his device. If so, perhaps the Eleventh Circuit's objection was only to compelling Doe to identify the hidden volumes in the course of the act of producing a decrypted version of the files on his device.[93] From that perspective, Doe would have a valid Fifth Amendment privilege against revealing that there was a hidden volume – something the government did not know and therefore was not a foregone conclusion. I think parts of the opinion make this reading a stretch.[94] But it points to the possibility that the Eleventh Circuit may have been inarticulately reaching the right result rather than misapplying the law.

However the Eleventh Circuit's decision is read, the case exposes how courts have so far failed to articulate a standard of proof for the foregone conclusion doctrine. Whatever the merits of the "reasonable particularity" standard when investigators seek to enforce an order to hand over certain documents, it has no application when the government seeks to an enforce an order to unlock. Fifth Amendment challenges to decryption orders require courts to identify the government's burden of proof: How clear must

---

[91] *See* United States v. Grubbs, 547 U.S. 90, 97 (2006) ("The Fourth Amendment, however, does not set forth some general particularity requirement. It specifies only two matters that must be particularly described in the warrant: "the place to be searched" and "the persons or things to be seized.").

[92] *See generally* Jill Scharr, *How to Encrypt Your Files Using TrueCrypt*, TOM'S GUIDE, Aug 7, 2013, 9:46 AM, available at https://www.tomsguide.com/us/how-to-encrypt-truecrypt,review-1832.html

[93] For such an interpretation, see Robert Graham's Twitter thread that begins at https://twitter.com/ErrataRob/status/1040718035236020230.

[94] See note 87, *supra*.

it be that the government already knows that the target knows the password? [95]

The novelty of the question is demonstrated by the fact that the two cases that have directly confronted the question have both involved compelled decryption using a Fifth Amendment framework along the lines of hat I have advocated in this article. In one recent district court case, *United States v. Spencer,*[96] Judge Breyer adopted the correct standard for the foregone conclusion doctrine – citing, I was pleased to see, a blog post of mine [97] – and then applied a clear and convincing evidence standard. He picked the burden of proof on policy grounds: A high burden was appropriate, Judge Breyer wrote, given the law's "jealous protection of the privilege against self-incrimination."[98] Another district court case on compelled decryption, *United States v. Fricosu*,[99] applied the preponderance of the evidence standard to measure the government's knowledge. But *Fricosu* simply states the standard without explanation or citation: "My findings of fact," the district judge stated, "are based on a preponderance of the evidence."[100]

Notably, *Spencer* and *Fricosu* applied different standards but neither cited any directly-related precedent. And the reason may simply be that there is little or no precedent to cite. Particularity-based standards of proof articulated in the context of subpoenas for documents have kept courts from confronting the degree of certainty

---

[95] The government has the burden of proof to show a foregone conclusion. See, e.g., United States v. Bright, 596 F.3d 683, 693 (9th Cir. 2010). U.S. v. Rue 819 F.2d 1488 n.4 (8th Cir. 1987). However, how high that burden is remains surprisingly unclear. See, e.g., Kevin R. Reitz, *Clients, Lawyers And The Fifth Amendment: The Need For A Projected Privilege* 41 Duke L.J. 572, 631 (1991) ("A critical issue, to date unresolved by the courts, is the burden of proof borne by the government in demonstrating that a particular testimonial fact is indeed a foregone conclusion."). Although Professor Reitz wrote that comment in 1991, it remains true today.

[96] 2018 WL 1964588 (N.D.Ca. 2018) (Breyer, J.).

[97] *Id* at *3 n.2 (citing See Orin Kerr, Fifth Amendment protects passcode on smartphones, court holds, Wash. Post (Sept. 24, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/24/fifth-amendment-protects-passcode-on-smartphones-court-holds ("The details of what records are on the phone should be irrelevant to whether the foregone conclusion doctrine applies because access to the phone is independent of what records are stored inside it. Handing over the passcode has the same testimonial aspect regardless of what is on the phone."))

[98] *Id*. at *3.

[99] 841 F.Sup.2d 1232 (D.Colo. 2012).

[100] *Id.* at 1234.

required for a fact to be a foregone conclusion. Whatever the best answer is,[101] a proper understanding of the foregone conclusion doctrine now requires courts to answer it.

III. COMPELLED DECRYPTION AND EQUILIBRIUM-ADJUSTMENT

This essay has so far offered a doctrinal argument for a particular application of the Fifth Amendment to compelled acts of entering in passwords. This Part takes a broader view. In recent Fourth Amendment decisions, including *Carpenter v. United States*,[102] the Supreme Court has indicated that courts should not apply constitutional doctrines mechanically to the new facts of computers and the Internet. Instead, courts should look to how old rules alter the new power dynamic between the government and the citizen in light of current and future technology.[103] This section considers whether that directive applies to compelled decryption, and if so, what Fifth Amendment standard that rule might produce. Put another way, let's put current doctrine aside and consider the implications of rules in their technological context: What kind of Fifth Amendment standard best suited to the role of encryption in modern life?

This section argues that the correct doctrinal answer is also appropriate given the broader role of encryption. Encryption is now everywhere. Most Americans carry an encrypted device with them, and all are free to use strong encryption to protect their data. As a result, technology has inserted a remarkably strong password gate in the way of routine searches across a wide range of cases. The government has various possible ways of bypassing encryption, and compelling decryption is only one of them. But adopting a high Fifth Amendment standard for compelled decryption could wrongly hide personal data from government access even when the government has a Fourth Amendment search warrant for that data

---

[101] A formalist approach to answering this might start with mining the Supreme Court's foregone conclusion cases for clues. *Fisher* has two particularly interesting ones. First, *Fisher* says the Court is "confident" that the act of production would not itself involve testimonial self-incrimination in light of the foregone conclusion doctrine. Second, *Fisher* adds that the Court was "doubtful" that assertions implicit in production were enough for the privilege to apply. *Fisher*, 425 U.S. at 411. Words like "confident" and "doubtful" might plausibly suggest a clear and convincing evidence standard along the lines of *Spencer*.

[102] 138 S.Ct. 2206 (2018).

[103] *See* notes 97-100, *infra*.

and the data the government seeks is not itself compelled under the Fifth Amendment. To the extent courts are concerned with the broader shift of power that technology creates in criminal investigations, the "seismic shifts"[104] of technological change trigged by encryption suggest uncertainty in the Fifth Amendment standard should be resolved in the government's favor.

This section makes that argument in three steps. First, it explains why there is at least a plausible case that the principles of equilibrium-adjustment should extent to the right against self-incrimination. Second, it argues that if equilibrium-adjustment is relevant, it counsels in favor of the relatively modest Fifth Amendment rule I have advocated. Third, it considers the relevance of this approach to the Fifth Amendment for the going dark debate in surveillance law.

A. Does Equilibrium-Adjustment Apply to the Right Against Self-Incrimination?

In 2011, in an article titled *An Equilibrium-Adjustment Theory of the Fourth Amendment,*[105] I argued that the Supreme Court has a recurring approach to interpreting the Fourth Amendment in response to changing technology. Traditional Fourth Amendment rules presupposed a balance of power.[106] New technologies constantly threaten that balance because old rules can apply to new technologies in ways that dramatically expand or restrict government power. [107] To ensure that mechanical application of old rules did not create a dystopia in which new technologies either gave the government too much power that could lead to abuses or too little power that would not protect the public, the Court often adjusts old rules to restore the prior equilibrium of government power.[108] "The resulting judicial decisions," I wrote, "resemble the work of drivers trying to maintain constant speed over mountainous terrain. In an effort to maintain the preexisting equilibrium, they add extra gas when facing an uphill climb and ease off the pedal on the downslopes."[109]

---

[104] *Carpenter*, 138 S.Ct. at 2219.
[105] 125 Harv. L. Rev 476 (2011).
[106] *See id.* at 485.
[107] *See id.* at 485-87.
[108] *See id.* at 487-89.
[109] *Id*. at 488.

Since 2011, the Supreme Court's application of equilibrium-adjustment principles has become particularly dramatic and explicit in Fourth Amendment cases involving digital technology.[110] The zenith of the approach appeared in the recent blockbuster decision in *Carpenter v. United States*,[111] which held that collection of historical cell-site records is a search that requires a warrant. The precedents, and the circuit court caselaw, indicated that no search occurred in *Carpenter* because the location of the phones had been disclosed to the third-party cell phone companies.[112] The Court rejected this result on the ground that "seismic shifts in digital technology"[113] gave the government so much power that it upset traditional expectations of limited government power and threatened law enforcement abuses.[114] "When confronting new concerns wrought by digital technology," the Court wrote, it was important "not to uncritically extend existing precedents."[115]

Should *Carpenter*-like arguments about equilibrium-adjustment extend to the Fifth Amendment right against self-incrimination? I'm not sure. On one hand, perhaps equilibrium-adjustment is solely a Fourth Amendment dynamic that should not extend beyond it. Search and seizure law can helpfully be understood as a way to impose a societal cost/benefit framework on police collection of evidence.[116] Methods of evidence collection often hinge on technological change. As technology changes, then, the societal costs and benefits of investigative steps regulated by Fourth Amendment also changes. It is therefore understandable that courts would want to adjust Fourth Amendment rules to restore the rough cost/benefit.[117]

The right against self-incrimination, by contrast, only involves using a person's own testimony against them. The Fifth

---

[110] *See, e.g.,* United States v. Jones, 565 U.S. 400 (2012) (holding that installing a GPS on a car is a Fourth Amendment search); Riley v. California, 134 S.Ct. 2473 (2014) (holding that a warrant is required to search a cell phone incident to arrest).

[111] 138 S.Ct. 2206 (2018).

[112] *See id.* at 2219-2220.

[113] *Id.* at 2219.

[114] *See id.*

[115] *Id.* at 2222.

[116] *See generally* Orin Kerr, *An Economic Understanding of Search and Seizure Law*, 164 U. Pa. L. Rev. 591, 595 (2016) ("[S]earch and seizure law is a way to account for investigative externalities and impose a rough cost-benefit test.").

[117] *See id.* at 616-18.

Amendment focuses on gathering information from the person's mind, not the technological world in which he lives. The implications for government power from this person-focused exchange is likely more stable. From that perspective, perhaps equilibrium-adjustment stops at the water's edge of search and seizure and does not flood into Fifth Amendment law.

But perhaps matters are not so simple. There is at least a plausible argument that the meaning of the right against self-incrimination should be attuned to equilibrium-adjustment concerns. Consider two such arguments. First, the spheres of the Fourth and Fifth Amendment are often intertwined in practice. When the government gathers evidence, it might collect the evidence itself (a Fourth Amendment concern) or might try to get a confession directly from the suspect (a Fifth Amendment concern). The two regimes arise in the same investigation, suggesting that the dynamic from one legal regime may be appropriately considered in another.[118]

Second, some Fifth Amendment caselaw has considered the effectiveness of government regulatory regimes in interpreting the right against self-incrimination. For example, in *Baltimore v. Bouknight*,[119] a juvenile court ordered a mother to produce her child suspected of being abused. The mother refused and asserted her right against self-incrimination. The Court recognized that the mother's act of producing the child would admit to custody and could aid her prosecution for abuse. But it nonetheless held the order enforceable because "the government's noncriminal regulatory powers" acted to "reduce[]" the privilege.[120] The government's regulatory interest altered the scope of the privilege.[121] If the effectiveness of a government regulatory regime can alter what the Fifth Amendment protects, something like the

---

[118] *See* Dan Terzian, *Forced Decryption as Equilibrium—Why It's Constitutional and How Riley Matters*, 109 Nw. U. L. Rev. Online 56, 60 (2014) (arguing that the Fifth Amendment privilege against self-incrimination should be included within the zone of equilibrium-adjustment). *Cf.* Orin S. Kerr, *Does Carpenter Revolutionize the Law of Subpoenas?*, Lawfare Blog, June 26, 2018, available at https://www.lawfareblog.com/does-carpenter-revolutionize-law-subpoenas (suggesting that *Carpenter*'s Fourth Amendment standard for reasonableness reflects an interest in equilibrium-adjustment in light of Fifth Amendment rules).

[119] 493 U.S. 549 (1990).

[120] *Id*. at 558.

[121] *See id.*

special needs doctrine in Fourth Amendment law, then perhaps the Fifth Amendment is properly sensitive to the new technological implications of doctrine.

In the end, the uncertain theoretical basis of the privilege against self-incrimination counsels against resolving this disagreement. As many scholars of the privilege against self-incrimination have noted, the theoretical justification of the privilege is disputed territory.[122] If judges and scholars are unsure of what the right against self-incrimination is supposed to do, then it becomes difficult to answer whether it should fall within equilibrium-adjustment. This paper instead takes a more modest path. If the right against self-incrimination does not consider equilibrium-adjustment, then I rest my argument on the doctrinal claim of Part II. On the other hand, if equilibrium-adjustment is relevant, what lessons does it teach for compelled decryption? The remainder of my article considers that question.

B. Modern Devices Insert Password Gates Into Routine Searches

Applying equilibrium-adjustment to compelled decryption should recognize the important dynamic: The computer era has inserted password gates into what would have been routine searches. Investigative steps that in the past would have only been Fourth Amendment searches now require Fourth Amendment searches plus encryption workarounds. Investigators ordinarily don't seek to

---

[122] Justice Arthur Goldberg, quoting Professor Kalven, once noted that "the law and the lawyers . . . have never made up their minds just what it is supposed to do or just whom it is intended to protect." *Murphy*, 378 U.S. at 56 n.5 (quoting Harry Kalven, Jr., Invoking the Fifth Amendment--Some Legal and Impractical Considerations, 9 Bull. Atomic Sci. 181, 182 (1953)). William Stuntz has added that "most people familiar with the doctrine surrounding the privilege against self-incrimination believe that it cannot be squared with any rational theory." William J. Stuntz, *Self-incrimination and Excuse*, 88 Colum. L. Rev. 1227, 1228 (1988). Akhil Amar and Renee Lettow Lerner make a similar point more memorably: "The Self-Incrimination Clause of the Fifth Amendment," they write, "is an unsolved riddle of vast proportions, a Gordian knot in the middle of our Bill of Rights." Akhil Reed Amar & Renée B. Lettow, *Fifth Amendment, First Principles: The Self-Incrimination Clause*, 93 Mich. L. Rev. 857, 857 (1995). *See also* Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and Its Future Predicted*, 94 J. Crim. L. & Criminology 243, 245-46 (2004) (contending that while "there is no general theoretical justification for the Fifth Amendment, there is a powerfully explanatory positive theory").

compel decryption because they want testimony. They seek to compel decryption because in some cases there is no other way to execute searches. They need to open the door to find the treasure. Because the technology is effectively hiding routine evidence behind password gates, courts should be reluctant to interpret the Fifth Amendment as imposing a high barrier to compelled decryption.

To appreciate this point, we need to begin with old fashioned searches. Traditional searches raise mostly Fourth Amendment problems. Take the case of a house. The government ordinarily needs a warrant to search a house. Once investigators have that warrant, however, there are few practical or legal barriers to conducting a highly invasive house search. Officers can break down the door if need be,[123] detain anyone found inside,[124] and they can search everywhere in the house where the evidence might be stored. No special equipment is needed.

Computer searches are different. The law of computer searches is still evolving and uncertain.[125] As a result, it is too early to draw direct comparisons. But the spread of encryption has introduced a major technological difference: In the case of end devices, and especially cell phones, it is common for computer searches to include a new investigative step of having to bypass encryption.[126] Widespread encryption has introduced what Bruce Schneier and I have called "encryption workarounds," [127] in which investigators who have satisfied the Fourth Amendment warrant requirement must nonetheless figure out a way to circumvent the powerful blocking technology of encryption that is now in routine use.[128] Encryption inserts a door in front of many forms of electronic treasure.

A range of different encryption workarounds exist.[129] Investigators might try to guess the passcode, or find a copy of it. They might try to purchase hardware or software that could be used

---

[123] *See, e.g.,* United States v. Banks, 540 U.S. 31 (2003).

[124] *See* Michigan v. Summers, 452 U.S. 692 (1981).

[125] *See generally* ORIN S. KERR, COMPUTER CRIME LAW Ch. 5 (4th Ed. 2018).

[126] *See* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L.J. 989 (2018).

[127] *See id.*

[128] *See id.* at 991.

[129] *See id.* at 996-1011.

to crack the encryption in some cases.[130] A suspect may have biometric access set up on his phone, such that investigators can use the suspect's thumbprint to unlock the phone without raising any Fifth Amendment issues.[131] But despite these various means of access, efforts to compel a suspect to enter a password is a useful and important default: It is can be used in a wide range of cases, it is scalable, and it requires only relatively modest law enforcement resources.[132]

As a result of this change, the shift from search-only to search-plus-search-for-encryption-workaround counsels against extravagant interpretations of the Fifth Amendment in the context of compelled entering of a password. Bypassing a password is a challenge for investigators, not an opportunity. Encryption is a barrier to evidence that must be overcome. Investigators seek a suspect to enter a password to decrypt the device so they can enable a subsequent search through plaintext pursuant to a warrant. Compelling testimony from the target is beside the point in most cases. It is a consequence of how the technology works, not evidence the government wants. The police don't want to know the password itself, and won't learn it anyway. The implied testimony in merely entering it without disclosing it is usually unimportant.

This is critical because of the function of the foregone conclusion doctrine explained earlier in Section I(c).[133] As explained there, the foregone conclusion doctrine prevents testimonial door-opening from denying the government access to the causally revealed treasure when the testimony of the door opening is not in play as part of building the government's case.[134] The introduction of device encryption creates a door-opening act requirement for the purpose of blocking access to treasure. That is the very point of having an encrypted device, of course. It gives the user sole control over who accesses the information stored in the device.

This is a net good in most cases. But from a Fifth Amendment perspective, it inserts a door that ordinarily is of no

---

[130] *See id.* at 1014.

[131] *See id.* at 1003-04.

[132] *See id.* at 1004 ("Notably, compelling a key raises practical and legal hurdles rather than technical ones. Sophisticated technological resources are not required, but a person who knows the key may refuse to hand it over or use it.")

[133] See Section I(c), supra.

[134] See Section I(c), supra.

testimonial interest to the government as a potential barrier to all of the computer-stored treasure that may be on the device. This is exactly the kind of non-substantive barrier that the foregone conclusion doctrine was designed to keep from blocking legitimate investigations. Consider the choice users face of whether to configure their smart phones so that a biometric form of identification such as a thumb print can be used to decrypt them. A thumb print is non-testimonial: The government can order a suspect to place his thumb on a fingerprint reader without triggering the privilege at all.[135] But investigators would rather suspects use non-testimonial biometric access than passwords, as the former is an easier door to open than the latter. Similarly, those hoping to keep the government away emphasize the benefits of using passwords and the risks of biometrics.[136] From both the standpoint of investigators and possible suspects, the relevance of using a password is the practical challenge of bypassing the lock on the door and not whatever testimony it may reveal.

In effect, the widespread use of strong encryption by users amounts to a reverse-*Carpenter*. Instead of technology expanding government power in ways that call for new rules to avoid Big Brother, widespread encryption limits government power to execute otherwise lawful searches. I don't think this requires new Fifth Amendment rules. The analysis in Part II argues that the government already can legally compel entering in a password in a range of situations under a correct reading of the doctrine, and there is no need for a shift to a new pro-government rule. But role of encryption counsels against broad readings of the Fifth Amendment privilege that might further rather than counterbalance the technological shift.[137]

---

[135] *See, e.g.,* State v. Diamond, 905 N.W.2d 870 (Minn. 2018).

[136] *See, e.g.,* Tim Cushing, *State Appeals Court Says Unlocking A Phone With A Fingerprint Doesn't Violate The Fifth Amendment*, Tech Dirt, January 25, 2017, available at https://www.techdirt.com/articles/20170121/08510936531/state-appeals-court-says-unlocking-phone-with-fingerprint-doesnt-violate-fifth-amendment.shtml ([Y]ou might be better off securing your phone with a passcode than your fingerprint. While a fingerprint is definitely unique and (theoretically...) a better way to keep thieves and snoopers from breaking into your phone, it's not much help when it comes to your Fifth Amendment protections against self-incrimination.").

[137] *Accord* Dan Terzian, *Forced Decryption as Equilibrium—Why It's Constitutional and How Riley Matters*, 109 Nw. U. L. Rev. Online 56, 62-63 (2014).

A counterargument might be that computer searches are tremendously invasive. The Supreme Court recognized in *Riley v. California*[138] that computers (and especially cell phones) can store an astonishing amount of very personal information. Perhaps this means that the Fifth Amendment standard should be high to counteract the reality that computers give the government greater access to information, much like *Riley* imposed a warrant standard for searches incident to arrest only for phones? Put another way, perhaps the treasure of digital evidence is so valuable that the law should give special protections against being compelled to open the door?

I disagree. The problem is that the greater access to information on a phone is naturally responded to by Fourth Amendment rules rather than Fifth Amendment rules. Fourth Amendment rules impose sliding scale on how much burden the government should have to find information. Technological change that enables more invasive searches through more information are readily met with tightening the rules. This is what happened in *Riley*, after all. The Court engaged in equilibrium-adjustment by ratcheting up Fourth Amendment protection. And I have argued in other scholarly work that courts should take similar steps in the execution of warrants, such as by imposing use restrictions on non-responsive data.[139]

In contrast, the greater information that can be accessed on a computer has no obvious Fifth Amendment resonance. The testimonial aspects of entering in a password are distinct from the evidence that the unlocked device may reveal. The greater treasure does not change the testimony implicit in opening the door. And the Fifth Amendment generally acts an absolute barrier to government access rather than a sliding scale of regulation. Technology's expansion of government power for computer searches merits a response from Fourth Amendment doctrine rather than the law of self-incrimination.

C. Compelled Decryption and the "Going Dark" Debate

A related policy argument for the Fifth Amendment standard I have advocated concerns the broader debate over "going dark" in

---

[138] 134 S.Ct. 2473 (2014).

[139] See generally Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech L. Rev. 1 (2015).

surveillance law. The Fifth Amendment standard I propose should undercut government efforts to encourage legislation imposing more effective decryption standards. The correct Fifth Amendment standard already opens much of the door the government needs. It should go a long way toward addressing government concerns about "going dark," and it therefore can direct attention away from more draconian approaches that otherwise may be in play.

Some context may be helpful. In the last few years, law enforcement officials have frequently complained that the default use of powerful encryption tools threatens public harm by thwarting criminal investigations. The post-crypto investigative environment, they fear, is "going dark."[140] In their view, this shift justifies considering new laws that either mandate the availability a technical means of decryption or at least provide means that can facilitate access. Civil libertarians have respond that this is not so. The shift to computerization has actually created a golden age of surveillance, they argue, in which the government has access to more and more information that would have been possible to access before.[141] New laws would therefore solve a problem that does not exist while weakening computer security.

It is too early to say how history will judge these arguments. The systematic effect of encryption on government power is a complex subject, in part because the government has a range of different encryption workarounds that may or may not work to bypass encryption.[142] It is also a rapidly evolving subject, as the technical means of encryption and its uses change from year to year. With that said, I think the Fifth Amendment standard that applies to compelled decryption has an important role in that broader debate. Knowing how the Fifth Amendment applies tells you something important about whether a more draconian solution is desirable.

The reason Fifth Amendment law can impact the debate over "going dark" is that the public interest in solving crime is something like the force of a river. Technology can influence it, but the water

---

[140] "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," Hearing before the Senate Judiciary Committee, July 8, 2015, written statements and video available at https://www.judiciary.senate.gov/meetings/going-dark-encryption-technology-and-the-balance-between-public-safety-and-privacy.

[141] *See, e.g.,* Peter Swire, *Encryption and Globalization*, 13 Colum. Sci. & Tech. L. Rev. 416, 420 (2012) (arguing that existing technology, including encryption "is actually enabling a golden age of surveillance.").

[142] *See generally* Kerr & Schneier, *supra* note 124.

will get downhill somehow. If those concerned about going dark turn out to be right, and investigators can't get into electronic devices at a high enough rate even with a warrant, the public's interest in solving crimes will encourage other alternatives. If there is no other way to ensure that the government has enough power to solve crimes involving digital evidence – which increasingly includes most crimes – then even draconian legislation may seem appealing.

Adoption of the Fifth Amendment standard proposed in this article 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 already. They will often know who knows the password, and they can then get lawful court orders compelling individuals to unlock the devices or face jail time for contempt. It won't work every time, of course. Those who know the password may be unavailable or dead. They may accept contempt sanctions rather than comply. But the Fifth Amendment's right against self-incrimination does not leave prosecutors powerless to get into encrypted devices.

For too long, the debate over "going dark" has proceeded assuming the Eleventh Circuit's standard that leaves investigators unable to compel decryption unless investigators already knew details about what they would find. Recognizing that standard as wrong means that investigators have far broader decryption powers than they realize. Investigators can harness a suspect's own awareness of his passwords to gain access to devices regardless of how strongly encrypted they are. The Fifth Amendment's limits to compelled decryption are much more modest than governments may realize.

CONCLUSION

The rise of widespread encryption gives every person a remarkable new technological tool to ensure privacy in the contents of their electronic devices. The Fourth Amendment fully protects those contents. But the Fifth Amendment right against self-incrimination offers more modest protection against compelled decryption than some, including the Eleventh Circuit, have thought. It offers no protection against being compelled to enter a password when the government can show independent knowledge that the

person knows the password. Proof of ability to enter in the password disarms the privilege against self-incrimination by rendering the testimonial aspect of production – knowledge of the password – a foregone conclusion.