UCLA LAW REVIEW DISCOURSE

The Fifth Amendment, Encryption, and the Forgotten State Interest

Dan Terzian

ABSTRACT

This Essay considers how the Fifth Amendment's Self Incrimination Clause applies to encrypted data and computer passwords. In particular, it focuses on one aspect of the Fifth Amendment that has been largely ignored: its aim to achieve a fair balance between the state's interest and the individual's. This aim has often guided courts in defining the Self Incrimination Clause's scope, and it should continue to do so here. With encryption, a fair balance requires permitting the compelled production of passwords or decrypted data in order to give state interests, like prosecution, an even chance. Courts should therefore interpret Fifth Amendment doctrine in a manner permitting this compulsion.

AUTHOR

Dan Terzian is a district court law clerk.

For their immeasurable contributions, I thank Peter Boos, Orin Kerr, Richard C. Miller, Shana Roth-Gormley, Gloria Sue, and Paul Yong. I welcome any comments and can be reached at Dan@danterzian.com.

TABLE OF CONTENTS

INTRODUCTION

Encrypted hard drives are virtually impenetrable, even to the government. That is by design—the whole point of encryption is to hide your data from those who should not see it.

Yet sometimes, the government not only should be able to see your data, it has the right to see it. In enforcing criminal laws, the government has seized data in the form of paper documents for decades, if not centuries. Now, these documents are increasingly digital, lying in hard drives instead of filing cabinets. This digitization and encryption of documents complicates government seizures in criminal investigations. Even if the government legally seizes a hard drive, it may still be unable to access the drive's documents. The only way to obtain them may be through subpoenas for production of the drive's password or its decrypted data.

But are these subpoenas constitutional? The Eleventh Circuit, the only federal appeals court answering this question, concluded negatively.[1] The Fifth Amendment's Self Incrimination Clause (Fifth Amendment or privilege) bars this compulsion, that court held, absent a substantial showing that the government already knows exactly what's on the drive.[2]

This Essay advances the alternative conclusion—these subpoenas are constitutional—primarily for reasons not considered by the Eleventh Circuit. At its core, the Fifth Amendment seeks a fair balance between the state's interest and the individual's. The U.S. Supreme Court has repeatedly balanced in the state's favor and limited the privilege's scope where holding otherwise would render crimes almost impossible to prosecute. These consequences would attend a privilege protecting encrypted data, with criminal investigations derailed and previously discoverable information undiscoverable. So principally for this reason, the privilege should not protect against the compelled production of passwords or decrypted data.

Courts ruling on this issue have not considered how fair balancing impacts doctrinal interpretation.[3] Nor has the relevant scholarship done

1. *See generally In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012).
2. *See generally id.* This is "known as the 'foregone conclusion' doctrine." *Id.* at 1343.
3. *See generally id.* (not considering this aim); *see also* United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012) (same); United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010) (same); United States v. Rogozin, No. 09-CR-379(S)(M), 2010 WL 4628520 (W.D.N.Y. Nov. 16, 2010) (same); *In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007) (same), *rev'd*, 2009 WL 424718 (D. Vt. Feb. 19, 2009) (same); Order Denying Application to

so.[4] Instead, both courts and scholars often see Supreme Court dicta as controlling the question. This dicta says that strongbox keys can be constitutionally compelled, but safe combinations cannot.[5] The Eleventh Circuit followed this dicta and extended it. It found passwords more like safe combinations than keys and therefore held that neither their production nor the production of decrypted data can be compelled.[6]

Passwords should not be forced into this key-combination dichotomy. They are neither a key nor a combination, and Court doctrine suggests the dichotomy should not be mechanically applied to new unlocking mechanisms. The dichotomy developed because keys and combinations have different Fifth Amendment implications—only combinations present the danger of compelling the creation of evidence. So it follows that new unlocking mechanisms with new implications should also be treated differently. Passwords for encrypted data present new implications in interest balancing and therefore should be treated

Compel Decryption, *In re* The Decryption of a Seized Data Storage Sys., No. 13-M-449 (E.D. Wis. filed Apr. 19, 2013), ECF No. 3, *available at* http://www.wired.com/images_blogs/threatlevel/2013/04/encryption-case.pdf, *overruled by* Order Granting Ex Parte Request for Reconsideration of the United States's Application Under the All Writs Act, No. 13-MJ-449 (E.D. Wis. filed May 21, 2013), ECF No. 6, *available at* http://www.wired.com/images_blogs/threatlevel/2013/05/decryptorder.pdf.

4. *See, e.g.*, John E. D. Larkin, *Compelled Production of Encrypted Data*, 14 VAND. J. ENT. & TECH. L. 253 (2012) (twice mentioning state and individual interests, but not considering how these interests affect the doctrine); Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. PA. J. CONST. L. HEIGHTENED SCRUTINY 11 (2012) (not considering fair balancing aim); Caren Myers Morrison, *Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment*, 65 ARK. L. REV. 133 (2012); Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171 (flagging fair balancing question but not analyzing); David Colarusso, Note, *Heads in the Cloud, a Coming Storm: The Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection Against Self-Incrimination*, 17 B.U. J. SCI. & TECH. L. 69 (2011) (not considering this aim); Nicholas Soares, Note, *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*, 49 AM. CRIM. L. REV. 2001 (2012) (acknowledging aim of seeking a fair state-individual balance but not elaborating upon it).

Only one author writing on this issue meaningfully elaborates upon the Fifth Amendment's aim to achieve a fair balance. *See generally* Andrew J. Ungberg, Note, *Protecting Privacy Through a Responsible Decryption Policy*, 22 HARV. J.L. & TECH. 537 (2009). Where that Note and this Essay principally differ is on how each incorporates this aim into their respective analyses. The former focuses on developing a responsible decryption policy, *see id.* at 555–56, while this Essay focuses on exploring the privilege's scope.

5. *See* United States v. Hubbell, 530 U.S. 27, 43 (2000); Doe v. United States, 487 U.S. 201, 210 n.9 (1988).

6. *In re Grand Jury Subpoena*, 670 F.3d at 1345–46; *Kirschner*, 823 F. Supp. 2d at 668–69; *In re Boucher*, 2007 WL 4246473, at *4 ("A password, like a combination, is in the suspect's mind, and is therefore testimonial and beyond the reach of the grand jury subpoena."), *rev'd*, 2009 WL 424718 (reversing because subpoena now sought the unencrypted data rather than the password itself); *see also Rogozin*, 2010 WL 4628520, at *6 (relying entirely on *Kirschner*'s reasoning).

differently. First, consider the interest balancing with safe combinations. There, a fair state-individual balance favors the individual—and compelled production is prohibited—because there is little state need; law enforcement can easily crack a safe through its own efforts. Contrast that with passwords. Law enforcement usually cannot bypass them, leaving the data inaccessible and creating great need for the password or decrypted data's production.

This Essay limits its focus to considering how the Fifth Amendment's fair balancing aim affects doctrinal interpretation. Beyond its scope is the argument—since rejected by the Eleventh Circuit[7]—that the compelled production of decrypted data is constitutional, but the compelled production of a password is not.[8] To the extent this distinction remains persuasive, this Essay seeks only to provide further support for adopting it.

Part I of this Essay provides an introduction to encryption technology and its effect on law enforcement investigations. Part II then explains the Supreme Court's Fifth Amendment doctrine, and Part III argues that a fair balance requires permitting the compelled production of decrypted data.

I. ENCRYPTION TECHNOLOGY

Encryption is "the process of concealing information."[9] It transforms consumable information (or data) "into a coded form" that is unintelligible to persons without the encryption key or password unless those persons crack the encryption.[10] But assuming a strong password is used, cracking encryption is not realistically possible.[11] Thus, "[p]ractically speaking, encryption today is impenetrable insofar as it cannot be bypassed by available means within a reasonable amount of time."[12]

7. *In re Grand Jury Subpoena*, 670 F.3d at 1346–47.
8. Reitinger, *supra* note 4, at 203–05 (noting the greater legal difficulties in compelling the production of passwords). *See generally id.* at 175–89 (advancing theory for the compelled production of unencrypted data).
9. Ungberg, *supra* note 4, at 540; *see also* Soares, *supra* note 4, at 2008.
10. Ungberg, *supra* note 4, at 540–41; *see also* Reitinger, *supra* note 4, at 173–75; Soares, *supra* note 4, at 2008. This Essay uses the phrase "crack the encryption" as shorthand to mean either cracking the encryption key or cracking the password.
11. Reitinger, *supra* note 4, at 175; *see also* Colarusso, *supra* note 4, at 77; Soares, *supra* note 4, at 2008; Ungberg, *supra* note 4, at 540–41.
12. Ungberg, *supra* note 4, at 541; *see also* Larkin, *supra* note 4, at 257–58; Soares, *supra* note 4, at 2008; Paul Rosenzweig, *Encryption Keys and Surveillance*, LAWFARE (Aug. 5, 2013, 2:00 PM), http://www.lawfareblog.com/2013/08/encryption-keys-and-surveillance-2 ("[D]ecryption can, in some cases, be effectively impossible."); *see also In re* Boucher, No. 2:06–mj–91, 2009 WL 424718, at *2 (D. Vt. Feb. 19, 2009) ("In order to gain access to the Z drive, the government is using an automated system which attempts to guess the password, a process that could take years.").

Encryption software is freely available[13] and easy to use.[14] Coupled with this mass availability, anecdotal data suggests that more people are encrypting data with strong passwords. Consider federal and state wiretaps. The latest wiretap report, for the year 2012, indicates this was the first year jurisdictions reported not being able to crack encryption, with this failure occurring in four wiretaps.[15] (Unfortunately, the report was unclear on whether this actually occurred in 2012 or instead occurred earlier and just reported in 2012.[16]) Other data indicates that commercial use of encryption is also increasing. One study found that 27 percent of surveyed corporations extensively used encryption in 2012, nearly a 70 percent increase over 2005 numbers.[17] Finally, the increasing number of cases on the Fifth Amendment and Encryption—from zero to at least seven since 2007[18]—itself suggests that more people are encrypting their data.

II. FIFTH AMENDMENT DOCTRINE

The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[19] Where applicable, it grants a person the privilege against self-incrimination, thus limiting the government's ability to obtain evidence.[20] The Amendment applies where three elements are met: "(1) compulsion, (2) a testimonial communication or act, and (3) incrimination."[21] The focus here—both in practice and in this Essay—is the communica-

13. Soares, *supra* note 4, at 2008 & n.66; *see also* Reitinger, *supra* note 4, at 172 & n.5; *Free Open-Source Disk Encryption Software for Windows 7/Vista/XP, Mac OS X, and Linux*, TRUECRYPT, http://www.truecrypt.org (last visited Jan. 29, 2014).

14. *See Mac OS X 10.6: Encrypting Your Home Folder With FileVault*, APPLE, http://support.apple.com/kb/ph7031 (last updated Aug. 6, 2013) (enumerating eight steps to encrypt data on Mac operating systems).

15. Admin. Office of the U.S. Courts, *Wiretap Report 2012*, U.S. COURTS, http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2012.aspx (last visited Jan. 29, 2014).

16. *See id.* Why jurisdictions are reporting wiretaps from prior years in the 2012 report goes unexplained. *See id.*

17. PONEMON INST., 2012 GLOBAL ENCRYPTION TRENDS STUDY 7, 46 (2013), *available at* http://www.verisec.com/sv/wp-content/uploads/sites/2/2013/03/Global-Encryption-Trends-Study-eng-ar.pdf (surveying organizations ranging in size from less than 500 employees to over 75,000).

18. *See* Kade Crockford, *Massachusetts High Court Set to Rule on Whether State Can Force You to Decrypt Your Drive*, ACLU (Oct. 31, 2013, 11:25 AM), https://www.aclu.org/blog/technology-and-liberty-national-security/massachusetts-high-court-set-rule-whether-state-can; *supra* note 6 (citing five cases); *infra* note 70 (noting one case).

19. U.S. CONST. amend. V.

20. *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1341 (11th Cir. 2012).

21. *Id.*; *see also* United States v. Hubbell, 530 U.S. 27, 34 (2000); Fisher v. United States, 425 U.S. 391, 408 (1976).

tion's testimonial qualities; there is little question that a contested subpoena involves compulsion and incriminating documents.[22]

A communication or act can be testimonial in two ways: based on any implied communication it conveys and based on its cognitive content. Implied communications arise from the process of producing documents. For example, every response to a subpoena contains the implied communications that the respondent possesses or controls the produced documents, that the documents are authentic, and that she believes them responsive to the subpoena.[23] These three implied communications alone can be testimonial.[24] But even if they are, the government can still compel production when it grants act of production immunity to the respondent. This "immuniz[es] the testimonial component of the act"—the government cannot use the act of producing a document to prove possession of that document—but still permits the government to use the substance of the documents produced.[25] Because act of production immunity is available, this Essay focuses not on implied communications but on a communication's cognitive content.

Communications can also be testimonial based on their cognitive content. Communications requiring extensive mental use are testimonial, and those requiring little are not.[26] Many compelled acts—the taking of blood, handwriting, and voice samples, for example—do not require meaningful mental use, so they are not testimonial.[27] The same analysis applies to the production of documents, with the court examining the mental effort needed to compile and produce them. If response requires the "respondent to make extensive use of 'the contents of his own mind,'" producing those documents is testimonial.[28] Such extensive use has been held to occur, for example, where the respondent must search eleven broad categories of documents to identify over 13,000 responsive pages.[29]

22. *See In re Grand Jury Subpoena*, 670 F.3d at 1341.
23. *See Hubbell*, 530 U.S. at 36; *Fisher*, 425 U.S. at 410; Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27, 57–59 (1986).
24. *See Hubbell*, 530 U.S. at 36–37; Soares, *supra* note 4, at 2005.
25. Alito, *supra* note 23, at 57–59; *see also* Reitinger, *supra* note 4, at 189–91, 196–200 (discussing the existence of contrary authority in some limited circumstances).
26. *See* Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and Its Future Predicted*, 94 J. CRIM. L. & CRIMINOLOGY 243, 247–48, 267–92 (2004) (developing and elaborating on the theory that the extent of cognition controls what is and is not testimonial); Reitinger, *supra* note 4, at 181; *see also Fisher*, 425 U.S. at 411 ("[H]is Fifth Amendment privilege is not violated because nothing he has said or done is deemed to be *sufficiently* testimonial for purposes of the privilege." (emphasis added)).
27. *See Hubbell*, 530 U.S. at 35.
28. *See id.* at 43 (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)).
29. *See id.* at 41–42.

The Supreme Court has applied this testimonial framework to other areas as well. Relevant here, the Court applied it to unlocking mechanisms similar to passwords—strongbox keys and safe combinations. In dicta, it declared that "being forced to surrender a key to a strongbox" is not testimonial, but "being compelled to reveal the combination to [a] wall safe" is.[30] No rationale was provided. Nor is one immediately obvious. Both acts involve essentially the same trivial amount of thought, and the distinction leads to apparently arbitrary results: A safe key can be compelled, but a safe combination cannot; a fingerprint that unlocks an iPhone can be compelled, but an iPhone's numeric password cannot.[31]

The best rationale for this distinction is that it presents a third way communications can be testimonial, one not based on cognition or implied communications but on another Fifth Amendment interest: concern over the compelled creation of documents.[32] The Court has indicated that such compulsion is more likely to yield a testimonial response.[33] Thus, the analyses for keys and combinations diverge. Strongbox keys always exist in the physical world, so a subpoena for the key involves only its production. But this is not so with a safe combination. It may exist only in one's mind, and producing it would require first creating a physical document.[34]

With encryption and passwords, courts' analyses gravitate to the key-combination dichotomy.[35] Take the Eleventh Circuit's recent decision in *In re*

30. Doe v. United States, 487 U.S. 201, 210 n.9 (1988) (internal brackets and quotation marks omitted); *see also Hubbell*, 530 U.S. at 43; Reitinger, *supra* note 4, at 203 & n.133.

31. *See* Larkin, *supra* note 4, at 270; Morrison, *supra* note 4, at 148; Colarusso, *supra* note 4, at 85.

32. *Cf.* Reitinger, *supra* note 4, at 203 (noting the Court's "indicat[ion] in dicta that being compelled to testify about the combination of a safe implicates the Fifth Amendment").

33. *See, e.g.*, United States v. Doe, 465 U.S. 605, 610–12 & n.10 (1984) ("The fact that the records are in respondent's possession is irrelevant to the determination of whether the creation of the records was compelled."); *see also Doe*, 487 U.S. at 221 n.2 (Stevens, J., dissenting) ("By executing the document, petitioner creates evidence that has independent significance."); Reitinger, *supra* note 4, at 203 & n.133.

34. To be sure, a safe's combination could exist in the physical world prior to a subpoena; it may already be written down. *See* Reitinger, *supra* note 4, at 195. The Court's analogy does not apparently contemplate this scenario. Rather, it writes of "surrendering" a strongbox key and "telling" an inquisitor the combination. *Hubbell*, 530 U.S. at 43. The use of "telling," rather than "surrendering," arguably implies that the combination exists only in the person's mind, with no physical copy available for surrender. Under this reading, a combination's production can be compelled if it is already written down.

35. *See generally In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1345–46 (11th Cir. 2012); United States v. Kirschner, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010); *In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *4 (D. Vt. Nov. 29, 2007) ("A password, like a combination, is in the suspect's mind, and is therefore testimonial and beyond the reach of the grand jury subpoena."), *rev'd*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009) (reversing because subpoena now sought the decrypted data rather than the password itself);

Grand Jury Subpoena Duces Tecum Dated March 25, 2011.[36] That court addressed the question of whether the Fifth Amendment bars the compelled decryption and production of the now-unencrypted data. It held affirmatively and explicitly framed the issue within this dichotomy, finding compelled decryption "most certainly more akin to requiring the production of a combination."[37]

This reasoning ignores a pivotal prefatory question: Do passwords even belong in this dichotomy? A computer password is not a safe combination. Sure, they are similar, but that does not mean they *must* be treated the same. Combinations and keys are similar—both unlock safes—yet they are treated differently because only the former implicates compelled creation concerns.

It follows, then, that courts should treat passwords and combinations differently if they have meaningfully different Fifth Amendment implications. And they do. Passwords and encrypted data implicate fair balancing concerns that support permitting compelled production, while combinations do not.

III. BALANCING INTERESTS

The Supreme Court has recognized seven "fundamental values" underlying the Fifth Amendment. They are:

> [(1)] our unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt; [(2)] our preference for an accusatorial rather than an inquisitorial system of criminal justice; [(3)] our fear that self-incriminating statements will be elicited by inhumane treatment and abuses; [(4)] our sense of fair play which dictates a fair state-individual balance by requiring the government to leave the individual alone until good cause is shown for disturbing him and by requiring the government in its contest with the individual to shoulder the entire load[]; [(5)] our respect for the inviolability of the human personality and of the right of each individual to a private enclave where he may lead a private life[]; [(6)] our distrust of self-deprecatory statements; and [(7)] our realization that the privilege, while sometimes a shelter to the guilty, is often a protection to the innocent.[38]

see also United States v. Rogozin, No. 09-CR-379 (S)(M), 2010 WL 4628520 (W.D.N.Y. Nov. 16, 2010) (relying on *Kirschner*'s reasoning).

36. 670 F.3d 1335.

37. *Id.* at 1345–46 (stating that the production of a strongbox key is the quintessential example of a physical act).

38. Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964) (citations omitted) (internal quotation marks omitted); *see also* Couch v. United States, 409 U.S. 322, 328 (1973).

Six of these seven values do not meaningfully affect the analysis here. Privacy is no longer a Fifth Amendment value.[39] As for the other five, they are not absolutes; they are only strong preferences for not permitting compulsion. We have "unwillingness" to subject the accused to a cruel trilemma; we "prefer[] . . . an accusatorial" system over an inquisitorial one; we "fear that self-incriminating statements" were the products of abuse; and we "distrust" those statements.

Forming the Fifth Amendment's core value, then, is its aim to achieve a fair state-individual balance. Where there is a real societal need to limit the privilege, the Court has repeatedly permitted compulsion upon the defendant.[40] Already the law permits compelling defendants to "produc[e] incriminating documents, giv[e] pretrial notice of defenses and of the evidence used to support them, provid[e] copies of defense investigative reports, and suppl[y] all forms of nontestimonial evidence,"[41] such as blood,[42] voice,[43] and fingerprint[44] samples.[45] While none of these compulsions force the accused to "take the stand and testify as a witness," they do "in other ways . . . treat him like a witness to be observed by the jury."[46]

This fair balancing aim often serves as a jurisprudential lodestar when the Court decides questions of the Amendment's scope. Recognizing this explicitly are a plurality opinion by Chief Justice Burger and a decision by Chief Justice Rehnquist, writing in his capacity as Circuit Justice. Both say that these ques-

39. *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993) ("The Court no longer views the Fifth Amendment as a general protector of privacy or private information, but leaves that role to the Fourth Amendment." (citing Fisher v. United States, 425 U.S. 391, 401 (1976))). Any resulting protection is not for privacy's sake but instead naturally flows from the Fifth Amendment's operation. The Framers did not intend the Fifth Amendment "to achieve a general protection of privacy"; they intended only to "deal with the more specific issue of compelled self-incrimination." *Fisher*, 425 U.S. at 400. Only to that extent is personal privacy protected by the Fifth Amendment. *See id.*

40. *See* Albert W. Alschuler, *A Peculiar Privilege in Historical Perspective: The Right to Remain Silent*, 94 MICH. L. REV. 2625, 2635 (1996) ("[O]ur legal system is substantially less accusatorial than [Supreme Court] rhetoric suggests.").

41. *Id.* at 2635–36 (footnotes omitted).

42. *See* Schmerber v. California, 384 U.S. 757 (1966).

43. *See* United States v. Dionisio, 410 U.S. 1 (1973).

44. *See* United States v. Wade, 388 U.S. 218 (1967).

45. Alschuler, *supra* note 40, at 2635–36 (footnotes omitted); *see also* United States v. Doe, 465 U.S. 605 (1984) (incriminating documents); United States v. Nobles, 422 U.S. 225 (1975) (investigative reports); Williams v. Florida, 399 U.S. 78 (1970) (pretrial notice). Alschuler's description of this physical evidence—the blood, voice, and fingerprint samples—as nontestimonial evidence is now somewhat imprecise because all evidence that may be compelled must be nontestimonial, absent a grant of immunity. Thus, the production of incriminating documents, when sufficiently limited, also falls under this nontestimonial category.

46. Akhil Reed Amar & Renée B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857, 885 (1995).

tions "must be resolved in terms of balancing the public need on the one hand, and the individual claim to constitutional protections on the other."[47]

Balancing appears throughout Fifth Amendment doctrine. The Supreme Court balanced interests in *Miranda v. Arizona*,[48] holding that the state's interest in custodial interrogation without providing a rights advisal could not overcome the accused's interests in "individual liberty" and having a "full opportunity to exercise the privilege."[49] Nearly two decades later, the Court balanced again, but this time tilting in the state's favor. Where public safety is at stake, "the need for answers . . . outweighs the need for the prophylactic rule protecting the Fifth Amendment's privilege against self-incrimination."[50] The balancing again favored the state when the Court considered what effect a belated *Miranda*-rights advisal had on a confession occurring after that advisory. In holding the confession still admissible, the Court reasoned that ruling otherwise would yield a "high cost to legitimate law enforcement activity, while adding little desirable protection to the individual's interest in not being compelled to testify against himself."[51] In a similar vein, a plurality of the Court this past term required that a defendant expressly invoke the privilege, because permitting silent invocations "would needlessly burden the Government's interest in obtaining testimony and prosecuting criminal activity."[52]

Two more recent examples cement the prevalence of balancing. A 2002 plurality opinion by Justice Kennedy balances the state's interest in running a prison—"an inordinately difficult undertaking"—against an inmate's interest in the privilege, and the state's interest prevailed.[53] Then there is *Kansas v. Cheever*.[54] There the Court found the privilege not violated where the government introduces "evidence from a court-ordered mental evaluation of a criminal defendant to rebut that defendant's presentation of expert testimony in support" of his defense.[55] The Court reached this conclusion partly through bal-

47. California v. Byers, 402 U.S. 424, 427 (1971); *see also* Balt. City Dep't of Soc. Servs. v. Bouknight, 488 U.S. 1301, 1304 (1988); *cf.* Amar & Lettow, *supra* note 46, at 871–72 (describing this pronouncement as "the Chief Justice seem[ing] to announce a new principle in self-incrimination clause cases"). Making the same point, but less explicitly, the Court in *Kastigar v. United States*, 406 U.S. 441, 445–46 (1972), stated that statutes granting immunity for compelled testimony "seek a rational accommodation between the imperatives of the privilege and the legitimate demands of government to compel citizens to testify."

48. 384 U.S. 436 (1966).

49. *Id.* at 455–58, 467.

50. New York v. Quarles, 467 U.S. 649, 657 (1984) (emphasis omitted).

51. Oregon v. Elstad, 470 U.S. 298, 312 (1985).

52. Salinas v. Texas, 133 S. Ct. 2174, 2181 (2013) (plurality opinion).

53. McKune v. Lile, 536 U.S. 24, 36–38 (2002) (plurality opinion).

54. 134 S. Ct. 596 (2013).

55. *Id.* at 598.

ancing. The court ordered evaluation is "the only effective means of challenging [the defendant's] evidence."[56] And the government's interest in the pursuit of justice "prevail[s] in the balance of considerations determining the scope and limits of the privilege against self-incrimination."[57]

A final example of balancing occurs in *Kastigar v. United States*.[58] There, the Court considered what type of immunity the Fifth Amendment requires—transactional immunity (an absolute immunity) or instead just "use and derivative use"—for witnesses who assert the privilege when compelled to testify before a grand jury.[59] The Court concluded that transactional immunity is not required, in part because requiring it would effectively grant "amnesty," and "[t]here can be no justification in reason or policy for holding that the Constitution requires [such] a[] . . . grant."[60] In other words, the state's interest in prosecution won yet again.

Now, none of this means that fair balancing displaces the doctrinal framework. No case holds that. But these cases do demonstrate that the Court often considers fair balancing. And this balancing influences the Court to interpret doctrine in a manner permitting compulsion where doing otherwise would make a crime "difficult . . . [or] almost impossible[] to prosecute."[61] That is precisely what will happen as use of encryption continues to proliferate: It will be unfairly difficult to prosecute crimes if the government cannot obtain the encrypted hard drive's password or its decrypted data. Suspects will be able to place encrypted "data beyond the reach of law enforcement," which may "shut the door on effective prosecution."[62] This data is information that law enforcement could previously obtain through its own skill but now no longer can.[63] Loss of this

56. *Id.* at 601.
57. *Id.*
58. 406 U.S. 441 (1972).
59. *Id.* at 443.
60. *See id.* at 462 (analogizing to Fifth Amendment coerced confession doctrine).
61. *See* Amar & Lettow, *supra* note 46, at 872–73 (observing that where applying the privilege "would make it difficult, and in some cases . . . almost impossible[] to prosecute[,] . . . the Court zigs, zags, and balances, ad hoc" and "holds that the privilege does not apply at all."); *see also* Allen & Mace, *supra* note 26, at 292 (asserting that Self-Incrimination Clause doctrine will be guided by the "felt necessities of the times" (quoting OLIVER WENDELL HOLMES, JR., THE COMMON LAW 1 (1881))); Ungberg, *supra* note 4, at 542, 552–55 ("[T]he Court became more willing to interpret the Fifth Amendment to accommodate the needs of law enforcement.").
62. Larkin, *supra* note 4, at 258.
63. David Stoll, Comment, *A Comment on the Encryption Debate*, 1998 STAN. TECH. L. REV. 1; Ungberg, *supra* note 4, at 548; *see also* OFFICE OF LEGAL EDUC., EXEC. OFFICE FOR U.S. ATTORNEYS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 72–75 (2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (explaining process of obtaining warrant for information stored

information could be devastating, as "computers have become an increasingly important source of evidence," and searching them is more and more "an essential step in the investigation."[64] In turn, a fair balance requires giving the state additional latitude in confronting these technological roadblocks.[65]

This incredible state need for compulsion makes Supreme Court dicta on safe combinations unpersuasive in this context. With safe combinations, the government does not *need* to compel the combination's production to access the safe's contents. It can realistically crack the safe on its own.[66] Thus, the balancing favors the accused because there is no real state interest in compelling production.

* * *

Let's review this Essay's main points so far. The Supreme Court often seeks a fair state-individual balance when interpreting the Fifth Amendment. This may even be why the Court developed the key-combination dichotomy: It would be unfair to force the accused to create evidence against himself (by memorializing the combination) when the state can easily crack the safe on its own. The same cannot be said of encrypted hard drives. The government cannot realistically crack them, so it has a significant interest in compelling the decrypted data's production.

These principles serve as guideposts in interpreting Fifth Amendment doctrine. If the doctrine can be interpreted in a manner both permitting compulsion and avoiding compelled creation, courts should adopt that interpretation. This interpretation is possible.[67] Producing documents may be compelled where it requires little mental cognition, which is why the government can compel the production of keys. Compelling a key's production comprises three acts, only one of which cognitive: remembering the key's location, retrieving it, and producing it. Producing a decrypted hard drive involves essentially the same acts and cognition: remembering the password, entering it, and producing the decrypted drive. Note that the immediate results of these two productions differ; one produces the key to the storage device, the other the unlocked device itself. This difference should

on a computer); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 537–38 (2005) (explaining how law enforcement searches computers for evidence).

64. *See* Kerr, *supra* note 63, at 532.

65. Michael Smith, Comment, *The Fourth Amendment, Password-Protected Computer Files and Third Party Consent Searches: The Tenth Circuit Broadens the Scope of Warrantless Searches*, 85 DENV. U. L. REV. 701, 724 (2008); *see also* Larkin, *supra* note 4, at 256.

66. *See* Mary McNamara, *In Safe Hands*, L.A. TIMES, July 15, 2002, http://articles.latimes.com/2002/jul/15/news/lv-safecracker15 (profiling elite safecracker).

67. *See, e.g.*, Larkin, *supra* note 4, at 275.

not matter. The results are functionally the same, with the state obtaining the device's contents either way.[68]

This is not how the Eleventh Circuit analyzed the issue. That court found the mental cognition from producing decrypted data more demanding because it is "more akin to requiring the production of a combination."[69] But this rationale proves too much. The reason combinations cannot be compulsively produced is not because of cognitive concerns but because of compelled creation concerns. So the similarities between compelling the production of combinations and of passwords are immaterial to analyzing the cognitive efforts.

The conclusion that courts should allow the compelled production of decrypted data carries a caveat. So far, this Essay has assumed there will always be a real state need for compelling this production. But sometimes there will not be. Occasionally, the password may be realistically obtained through means that do not touch on the Fifth Amendment. Maybe a simple password can be easily cracked;[70] maybe the password is written somewhere and easily found; maybe even others know the password and they readily produce it.[71] The point is that sometimes reasonable investigatory effort will yield the password without requiring compulsion upon the defendant.

Interest balancing must vary with the effort required to obtain the password through investigatory means. With passwords discoverable through minimal or reasonable effort, the state's interest in compelled production is little to none. Contrast that with passwords that are not discoverable, reasonably or otherwise, where the state's need for compulsion remains incredible.

If we take interest balancing seriously and use it to favor doctrinal interpretations permitting compulsion, as this Essay does, then we should also consider what happens where there is little state need for compulsion. One option is that the result remains the same—the decrypted data can still be compelled—on the

68. *See id.*; *see also In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1, *3–4 (D. Vt. Feb. 19, 2009) (upholding subpoena seeking the production of an encrypted version of a computer drive).

69. *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012).

70. *See* Criminal Complaint at 4–5, United States v. Feldman, No. 13-892M (NJ) (E.D. Wis. filed Aug. 13, 2013), ECF No. 1, *available at* http://www.wired.com/images_blogs/threatlevel/2013/08/Crim-Comp.-13MJ892-8-13-13.pdf (containing affidavit of Federal Bureau of Investigation special agent swearing that government agents were able to decrypt the contents of encrypted drives, but not explaining how they were able to); *see also* Order Denying Application to Compel Decryption, *supra* note 3, at 2–3.

71. *See* Carl Hessler Jr., *UPDATE: Former North Penn Vice Principal Charles Hurst Cell Phone Password Obtained*, MONTGOMERY NEWS (Mar. 4, 2011), http://www.montgomerynews.com/articles/2011/03/04/north_penn_life/news/doc4d6fa74747db3944451459.txt; *see also* Larkin, *supra* note 4, at 258.

same grounds already highlighted. Because fair balancing was only a reason for adopting that interpretation, it does not necessarily add fair balancing to the testimonial calculus.

Alternatively, courts could explicitly incorporate interest balancing into the calculus. So the decrypted data could be compelled only if there is a significant state need for compulsion. Drawing this line in practice would not be difficult. Imagine the government subpoenas the accused for the production of decrypted data and the accused moves to quash on Fifth Amendment grounds. Under this approach, the motion would be denied if the government shows it could not realistically obtain the data through investigatory effort. This procedure would not be uncommon, as similar iterations exist elsewhere in criminal procedure. Obtaining a search warrant, for example, requires the government first show the existence of probable cause,[72] and a later determination that cause was deficient may result in excluding any evidence obtained under the warrant.[73]

CONCLUSION

So far, analysis of the Fifth Amendment's application to encrypted data has largely been limited to whether passwords are more like combinations than keys. This dichotomy is faulty and the analysis incomplete. Passwords are not like combinations: Only passwords make their contents effectively impenetrable to law enforcement. This impenetrability creates a significant state interest in permitting compelled production, and achieving a fair balance of interests often requires permitting that compulsion. Courts should therefore allow this compulsion on fair balancing grounds. Or in the very least, they should consider the state's heightened interest when ruling on this issue.

72. FED. R. CRIM. P. 41(d); *see also* U.S. CONST. amend. IV.
73. *See* United States v. Leon, 468 U.S. 897, 922–23 (1984).