Fordham Law Review

Volume 87 | Issue 1 Article 9

2018

Unlocking the Fifth Amendment: Passwords and Encrypted Devices

Laurent Sacharoff
University of Arkansas School of Law, Fayetteville

UNLOCKING THE FIFTH AMENDMENT: PASSWORDS AND ENCRYPTED DEVICES

*Laurent Sacharoff**

Each year, law enforcement seizes thousands of electronic devices—smartphones, laptops, and notebooks—that it cannot open without the suspect's password. Without this password, the information on the device sits completely scrambled behind a wall of encryption. Sometimes agents will be able to obtain the information by hacking, discovering copies of data on the cloud, or obtaining the password voluntarily from the suspects themselves. But when they cannot, may the government compel suspects to disclose or enter their password?

This Article considers the Fifth Amendment protection against compelled disclosures of passwords—a question that has split and confused courts. It measures this right against the legal right of law enforcement, armed with a warrant, to search the device that it has validly seized. Encryption cases present the unique hybrid scenario that link and entangle the Fourth and Fifth Amendments. In a sense, this Article explores whose rights should prevail.

This Article proposes a novel settlement that draws upon the best aspects of Fourth and Fifth Amendment law: the government can compel a suspect to decrypt only those files it already knows she possesses. This rule follows from existing Fifth Amendment case law and, as a corollary to the fundamental nature of strong encryption, also represents the best accommodation of law enforcement needs against individual privacy.

* Professor of Law, University of Arkansas School of Law, Fayetteville; J.D., Columbia Law School; B.A., Princeton University. The author would like to thank Orin S. Kerr, Ronald J. Allen, Andrew G. Ferguson, Brian Lee, Jocelyn Simonson, I. Bennett Capers, Christina Mulligan, Alice Ristroph, Jenia Iontcheva Turner, David Patton, Aloni Cohen, Sunoo Park, and for research assistance, Jessica Boykin.

INTRODUCTION

The U.S. Supreme Court has long pondered how the Fourth and Fifth Amendments relate during a criminal investigation. Under the hoary, nineteenth century *Boyd* doctrine, the Court once intertwined the two amendments into a majestic, overlapping bulwark of absolute protection.[1] For example, the government could not compel a suspect to produce personal papers as evidence in a criminal case. Indeed, at its apogee, the amendments together barred agents from physically seizing such papers or other evidence—even with a warrant.[2]

1. Boyd v. United States, 116 U.S. 616 (1886), *overruled by* Fisher v. United States, 425 U.S. 391 (1976).

2. Gouled v. United States, 255 U.S. 298, 309 (1921) (holding that search warrants "may not be used as a means of gaining access to a man's house or office and papers solely for the purpose of making search to secure evidence to be used against him in a criminal or penal proceeding"), *overruled by* Warden, Md. Penitentiary v. Hayden, 387 U.S. 294 (1967).

In the last fifty years, however, the Court has sought to melt this powerful alloy, separating each amendment into complementary, distinct domains. When the government compels a person to testify, the Fifth Amendment applies.[3] But when the government unilaterally seizes evidence, only the Fourth Amendment governs.[4] Scholars have similarly sought to define separate realms for each.[5] As Richard Nagareda put it, the Fifth Amendment addresses the "giving" of evidence by a suspect; the Fourth, the "taking" of evidence by law enforcement.[6]

This new direction has created a gap in coverage, however. The privacy of papers and information fell into this gap, enjoying little to no protection from either amendment. When government officers subpoenaed a person's papers, or when police seized an electronic device with a warrant, they enjoyed almost unlimited power in what they could demand and where they could search. Neither amendment imposed meaningful limits.

This result also followed in part because of the exposed nature of seized papers. Until recently, individuals had little physical power to shield the privacy of their personal information. Once government agents seized papers, whether a written journal, a photo album, an email, digital images, or a collection of magazines, all were freely visible by their very nature to government agents. The printed word was always in plain view.

But widespread electronic encryption has altered the balance of power. Now individuals can shield their private information. Most handheld devices now automatically "lock," which means not only that the device will not run, but also that the device automatically encrypts its data into an unreadable scramble.[7] Agents who seize a device with a warrant that authorizes them to search its content now find they cannot access those contents without the password. Technology has filled the gap to afford privacy protection to papers once again.

---

3. United States v. Dionisio, 410 U.S. 1, 10 (1973) (holding that a subpoena requiring a person to appear and testify does not implicate the Fourth Amendment seizure provision "once the Fifth Amendment is satisfied" (quoting Fraser v. United States, 452 F.2d 616, 620 (7th Cir. 1971))).

4. Maryland v. Andresen, 427 U.S. 463, 472–73 (1976).

5. *See generally* Robert S. Gerstein, *The Demise of* Boyd*: Self-Incrimination and Private Papers in the Burger Court*, 27 UCLA L. REV. 343 (1979); Robert Heidt, *The Fifth Amendment Privilege and Documents—Cutting* Fisher*'s Tangled Line*, 49 MO. L. REV. 439 (1984); Richard A. Nagareda, *Compulsion "To Be a Witness" and the Resurrection of* Boyd, 74 N.Y.U. L. REV. 1575 (1999); H. Richard Uviller, *Foreword:* Fisher *Goes on the Quintessential Fishing Expedition and* Hubbell *Is Off the Hook*, 91 J. CRIM. L. & CRIMINOLOGY 311 (2001). *But see generally* Bryan H. Choi, *For Whom the Data Tolls: A Reunified Theory of Fourth and Fifth Amendment Jurisprudence*, 37 CARDOZO L. REV. 185 (2015); Michael S. Pardo, *Disentangling the Fourth Amendment and the Self-Incrimination Clause*, 90 IOWA L. REV. 1857 (2005).

6. Nagareda, *supra* note 5, at 1603. Nagareda agrees with the Court that the Fourth and Fifth Amendments govern separate domains. *Id.* But unlike the Court, he would draw the line differently to include the production of documents pursuant to a subpoena under the Fifth Amendment "giving" side of the divide. *Id.* at 1658–59.

7. APPLE, IOS SECURITY 13–16 (2018), https://www.apple.com/business/docs/iOS_Security_Guide.pdf [https://perma.cc/Z5XT-ZFGT].

Indeed, in a development scholars and the courts have largely failed to note,[8] these facts on the ground by necessity reunite the Fourth and Fifth Amendments, making each apply to the same factual situation. A warrant satisfying the Fourth Amendment appears to give the agents the right to all the information on the device. Meanwhile, the Fifth appears to give the individual the right to remain silent and thereby deny agents access to that same data. Encryption thus challenges the ability to divide the Fourth and Fifth Amendments into discrete territories, and the new technology requires a new settlement. We could set the two amendments against each other or, as I propose in this Article, draw upon the values they share to harmonize them.

Consider two paradigmatic scenarios. First, federal agents suspect an individual possesses child pornography, and they obtain a warrant to seize all his devices and other storage media. Agents may recover numerous hard drives, flash drives, camera cards, and smartphones; these and other seized digital media can sometimes contain terabytes of data.[9] But they quickly learn the suspect has encrypted the devices with a password they cannot crack, and the suspect refuses to disclose it. In a second scenario, in a drug case, agents wish to search the suspect's smartphone for trophy photos—images of the suspect standing before drugs, guns, or large amounts of money.[10] They have arrested the defendant and obtained a warrant to search his smartphone, but it is locked and only he has the passcode.

Law enforcement agencies report thousands of such cases every year—cases including homicides, drugs cases, child pornography, and white-collar crime.[11] In these cases, officers have, or can get, a warrant to search a seized

8. *See, e.g.*, United States v. Apple MacPro Comput., 851 F.3d 238, 248 (3d Cir. 2017) (analyzing an order to decrypt a digital device under the Fifth Amendment, with no mention of the Fourth); *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012) (holding that the act of decrypting a hard drive was sufficiently testimonial to invoke the Fifth Amendment); *see also* Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISCOURSE 298, 308 (2014) (analyzing decryption as a Fifth Amendment question only, though balancing against law enforcement interests within a Fourth Amendment framework). *But see* Benjamin Folkinshteyn, *A Witness Against Himself: A Case for Stronger Legal Protection of Encryption*, 30 SANTA CLARA HIGH TECH. L.J. 375, 411–12 (2013) (briefly noting that Fifth Amendment protections should take account of deficiencies in Fourth Amendment protections).

9. *See, e.g.*, *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d at 1340 (describing the large volume of data seized in the case, totaling over five terabytes).

10. Lucas v. State, 698 A.2d 1145, 1155 (Md. Ct. Spec. App. 1997) (holding that the trial court did not err in admitting trophy photos and expert testimony on their "importance to mid-level drug dealers").

11. Devlin Barrett, *FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public*, WASH. POST (May 22, 2018), https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html [https://perma.cc/GQE6-SKND] (noting that investigators were locked out of 1000–2000 cellphones last year, and not 7800 as the FBI originally stated); N.Y. CTY. DIST. ATTORNEY'S OFFICE, THIRD REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 8–9 (2017), https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20

device, but the device is locked.[12] Often agents can hack in, but when they cannot, they face the fundamental question: can a court compel a suspect to disclose her password or enter it into the device?

On the one hand, law enforcement and some courts say that the warrant, coupled with the Fourth Amendment,[13] affords access to the device.[14] The Fifth Amendment should present no obstacle because the suspect will enter the password in such a way that no one sees or learns the password, no one records it, and the device itself makes no record of the password. The government has compelled a person merely to turn a key and open a box. On the other hand, many privacy advocates argue that the Fifth Amendment provides protection that is far more robust.[15] The government cannot compel a person to orally disclose her password,[16] and requiring her to type it into a device amounts to the same prohibited compulsion.

This Article answers the fundamental question bedeviling courts[17] and scholars[18]: does the Fifth Amendment protect suspects from being compelled to enter their passwords into a device?

This Article charts a sensible middle ground between authorizing law enforcement agents to search the entirety of a device and preventing them

---

on%20Smartphone%20Encryption.pdf [https://perma.cc/5NL5-J6DN] (stating that the Manhattan District Attorney's Office recovered 1283 locked devices in 2017).

12. *See supra* note 11. The Manhattan report elsewhere suggests that law enforcement ultimately unlocked most of these devices through hacking. N.Y. CTY. DIST. ATTORNEY'S OFFICE, *supra* note 11, at 8.

13. Federal and state statutes and rules authorize courts to issue search warrants, and the Fourth Amendment merely provides limits on their use and on searches without warrants. *See, e.g.*, FED. R. CRIM. P. 41; *see also* United States v. Horton, 863 F.3d 1041, 1049 (8th Cir. 2017) (holding that a warrant issued beyond the authorization of Rule 41 is no warrant at all).

14. *See* Rod J. Rosenstein, Deputy Attorney Gen., U.S. Dep't of Justice, Remarks as Prepared for Delivery at the United States Naval Academy (Oct. 10, 2017), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval [https://perma.cc/2GU9-9T4A] (noting that if law enforcement meets the Fourth Amendment's warrant and probable cause requirements, agents can access locked devices used to commit crimes); *see also* Microsoft Corp. v. United States, 829 F.3d 197, 223–24 (2d Cir. 2016) (Lynch, J., concurring) (stating that the Fourth Amendment's probable cause requirement provides sufficient protection to individual privacy), *vacated*, 138 S. Ct. 1186 (2018).

15. *See, e.g.*, Jamie Williams, *EFF to Court: Forcing Someone to Unlock and Decrypt Their Phone Violates the Constitution*, ELECTRONIC FRONTIER FOUND. (Mar. 6, 2017), https://www.eff.org/deeplinks/2017/03/eff-court-forcing-someone-unlock-and-decrypt-their-phone-violates-constitution [https://perma.cc/F5F4-M2L6].

16. *See, e.g.*, United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010); *see also* United States v. Hubbell, 530 U.S. 27, 43 (2000) (holding that an act is "testimonial" if it is "like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox").

17. *Compare In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1341 (11th Cir. 2012) (finding that the Fifth Amendment protects against compelled disclosure of passwords), *with* United States v. Apple MacPro Comput., 851 F.3d 238, 248 (3d Cir. 2017) (finding no Fifth Amendment protection on the facts before it), *and* Commonwealth v. Gelfgatt, 11 N.E.3d 605, 615 (Mass. 2014) (same).

18. *See* Aloni Cohen & Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, 32 HARV. J.L. & TECH. (forthcoming 2019) (applying the technical lessons of cryptography to Fifth Amendment case law but remaining largely neutral on the central legal debates).

from obtaining any information from a locked device whatsoever. This Article proposes that a court may compel a suspect to decrypt only those files that (1) the government already knows the person possesses, and (2) the government can describe with reasonable particularity. Once the government has identified the specific files, it may compel the defendant to decrypt *only those files*. It may not, as often happens today, require him to enter his password and walk away,[19] a requirement that affords law enforcement access to *all* of his files simply upon satisfying the rule of particularity for one or two files.

I derive this rule of particularity from the best principles of both the Fourth and Fifth Amendments. It draws upon the particularity requirement in the Fourth Amendment's Warrant Clause and existing Fifth Amendment case law—well outside the password and encryption context—on the act-of-production doctrine and its complement the foregone conclusion test.

This rule not only balances the Fourth and Fifth Amendments but *harmonizes* them. Under the Fifth Amendment, my rule limits the assistance the government can compel from a defendant in her own prosecution by requiring her to make her entire digital life available. Moreover, my rule promotes another Fifth Amendment value: a limit on government fishing expeditions.[20] By limiting the government to only those files it can identify, this rule prevents law enforcement agents from reviewing thousands of files in search of *new* crimes.

Under the Fourth Amendment, my rule of particularity enhances informational privacy[21] and limits broad government overreach, such as exploratory searches for new crimes.[22] It also provides suspects the very security the Fourth Amendment expressly protects by making clear to them the precise files the government will inspect—a value carefully enunciated in the precedent leading to the Fourth Amendment. It assures suspects that government agents will not roam at will throughout the entirety of the person's digital life.

This Article argues that we must view Fifth Amendment rights against the background of the existing Fourth Amendment deficiencies—we cannot simply view each in isolation. Instead, we must begin again to read the two

19. *See, e.g.*, *Gelfgatt*, 11 N.E.3d at 611.

20. *See infra* notes 270–81 and accompanying text.

21. *See generally* Katz v. United States, 389 U.S. 347 (1967); Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869, 873 (1985) (arguing that the Fourth Amendment historically afforded nearly absolute protection for private papers in criminal investigations).

22. *See* Schnapper, *supra* note 21, at 918. Current Fourth Amendment case law essentially allows agents, armed with a warrant, to search every file, folder, picture, video, spreadsheet, message, and document for evidence of the crime that gave rise to probable cause. *See, e.g.*, United States v. Evers, 669 F.3d 645, 653 (6th Cir. 2012); United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009) ("[T]here may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders."); *see also* Adam Gershowitz, *The Post*-Riley *Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 615 (2016) (noting and critiquing the lack of ex ante limits on search warrant execution).

amendments together. After all, *Boyd* did not say we should blindly conflate them, but rather that they "throw great light on each other."[23]

Current case law and scholarship concerning compelled decryption have not only focused too narrowly on technical Fifth Amendment considerations, such as the foregone conclusion doctrine, but have also misconstrued that doctrine in ways that threaten to unravel its entire framework. As I discuss in depth below,[24] cases have mistakenly applied the foregone conclusion doctrine to the *password* rather than to the documents sought.

This Article falls within the larger debate concerning encryption.[25] On the one hand, many in law enforcement have complained that encryption facilitates crime and stymies investigations. Former FBI Director James Comey and many others in law enforcement have painted a dark picture of terrorists communicating and operating at will, in secret.[26] On the other hand, law enforcement can obtain the information despite encryption in most situations.[27] In these instances, the suspect may volunteer the password or open the device,[28] law enforcement may obtain data synced to a cloud from a service provider,[29] a spouse or family member may provide access, law enforcement may learn the password from other easily available sources, or law enforcement may crack the device by brute force.[30]

This Article addresses those cases in which law enforcement cannot gain access without the password, and the suspect or witness refuses to disclose

---

23. Boyd v. United States, 116 U.S. 616, 633 (1886).

24. *See infra* Part IV.D.

25. *See generally* NAT'L ACAD. OF SCI., DECRYPTING THE ENCRYPTION DEBATE: A FRAMEWORK FOR DECISION MAKERS (2018).

26. *See generally Encryption Working Group Year-End Report*, HOUSE JUDICIARY COMM. & HOUSE ENERGY & COM. COMM. (Dec. 20, 2016), https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf [https://perma.cc/WUN3-Q6BN]; HOUSE HOMELAND SEC. COMM. MAJORITY STAFF REPORT, GOING DARK, GOING FORWARD: A PRIMER ON THE ENCRYPTION DEBATE (2016), https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf [https://perma.cc/8JWD-F6L3]; Rosenstein, *supra* note 14 ("Encrypted communications that cannot be intercepted and locked devices that cannot be opened are law-free zones that permit criminals and terrorists to operate without detection.").

27. *See generally* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989 (2018); BERKMAN CTR. FOR INTERNET & SOC'Y HARVARD UNIV., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE (2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/JN6U-AKYK] (cataloging methods available to law enforcement to sidestep encryption).

28. Suspects in child pornography cases often simply confess to the possession of the information and disclose their passwords, perhaps out of deep shame. *See, e.g.*, United States v. Johnson, 652 F.3d 918, 920 (8th Cir. 2011) (describing how the suspect, after receiving *Miranda* warnings, admitted to authorities that he saved any child pornography he "stumbled upon").

29. 18 U.S.C. § 2703 (2012) (stating that electronic service providers must produce their customers' emails and other communications in response to appropriate legal process); FED. R. CRIM. P. 41(e)(2)(A)–(B).

30. Brute force access often involves trying numerous keys or passwords. *See* Kerr & Schneier, *supra* note 27, at 994; *see also* N.Y. CTY. DIST. ATTORNEY'S OFFICE, *supra* note 11, at 8 (stating that workarounds may involve "exploit[ing] a flaw in the encryption scheme").

it. These circumstances are likely to increase as encryption becomes a greater, more automatic part of our data lives.[31] Each year, major cities seize hundreds of encrypted devices they cannot decrypt, primarily investigating ordinary (nonterrorism) crimes such as narcotics, cybercrime, homicide, and sex crimes. The Manhattan District Attorney's Office reports that it seized 1283 locked devices in 2017, and other jurisdictions report similar numbers.[32]

So far, most reported court cases involve contraband images or other evidence on devices, and this Article therefore focuses on these cases. But this simple, paradigmatic case will apply directly to the range of encryption problems law enforcement will increasingly face, including encrypted cloud storage,[33] encrypted cloud computing,[34] encrypted communications, and more novel applications of passwords and encryption such as Bitcoin or other digital currency[35] and smart contract rights on blockchains.[36]

Part I summarizes the Court's changing treatment of the Fourth and Fifth Amendment protections for papers and, as applied today, digital evidence. It elaborates upon the Fifth Amendment act-of-production doctrine, and shows how the foregone conclusion doctrine leads to a suitable rule for passwords. Part II summarizes how encryption works to lock devices and scramble their contents. Part III considers the different ways law enforcement might compel a password, focusing in particular on two main categories: compelling a suspect to state her password or compelling her to enter it directly into her device. It concludes that the first category represents Fifth Amendment protected testimony, whereas the second category amounts to the quasi testimony protected by the act-of-production doctrine. Part IV applies the act-of-production doctrine and the foregone conclusion test to the paradigmatic case: a seized device that contains contraband images or other evidence. Finally, Part V considers both the Fourth and Fifth Amendments from a theoretical perspective and describes how a particularity rule furthers the goals of both amendments.

---

31. *See* N.Y. CTY. DIST. ATTORNEY'S OFFICE, *supra* note 11, at 2 (noting that the "arms race" between strong commercial encryption and law enforcement's power to crack it has "intensified"). These authorities often do not clarify, however, how many of these devices they ultimately cannot decrypt. In fact, the FBI significantly inflated the number to nearly 7800 until May 2018, when it conceded the annual number was closer to 1200. Barrett, *supra* note 11.

32. N.Y. CTY. DIST. ATTORNEY'S OFFICE, *supra* note 11, at 5.

33. *See* Wei Chen Lin, *Where Are Your Papers?: The Fourth Amendment, the Stored Communications Act, the Third-Party Doctrine, the Cloud, and Encryption*, 65 DEPAUL L. REV. 1093, 1096 (2016) (noting that the market may well soon facilitate widespread encryption of cloud storage).

34. *See* STEFAN RASS & DANIEL SLAMANIG, CRYPTOGRAPHY FOR SECURITY AND PRIVACY IN CLOUD COMPUTING 1–2 (2014).

35. *See* ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES 97 (2014) (describing the use of cryptographic private keys for digital currency wallets).

36. *See generally Ethereum Blockchain App Platform*, ETHEREUM, https://www.ethereum.org [https://perma.cc/J8BR-3YYK] (last visited Aug. 24, 2018) (describing the open blockchain, smart contract platform).

I. PAPERS AND CRIMINAL INVESTIGATIONS

When scholars and the Court speak of the relationship between the Fourth and Fifth Amendments, whether their overlap or the line dividing them, they primarily talk about suspects' papers—their bank statements, letters, diaries,[37] and, today, their emails, photos, and spreadsheets. In conducting a criminal investigation or prosecuting a criminal case, the government wants these documents because they will constitute direct evidence of guilt or lead to evidence of guilt.

Though today we speak of emails, the founding generation similarly reverenced the privacy of papers. The Fourth Amendment lists "papers" expressly,[38] and its authors relied in large part upon the English court precedent[39] affording papers nearly absolute protection.[40] These cases[41] protected the privacy of papers against government criminal investigations for reasons that today we would recognize as sounding in the Fourth and Fifth Amendments, as well as the First.[42] The court in *Entick v. Carrington*,[43] for example, held that the common law did not permit seizing, or subpoenaing in discovery, a person's papers to use them as evidence in a criminal investigation.[44] This was a question not only of seizure but also of the common law principle against self-incrimination.

The principle derived in part from an abhorrence of government tyranny—a principle naturally suited to the founding generation.[45] But the opinion contained a principle amenable to the modern era: papers taken are not just any property or chattel; they are property that contains a person's secret thoughts, and for the government to seize such papers works a greater harm than seizing other property.[46]

In 1886, the U.S. Supreme Court almost directly applied the common law principles of *Entick* in interpreting and applying the Fourth and Fifth

---

37. *See, e.g.*, Andresen v. Maryland, 427 U.S. 463, 465–68 (1976) (business records); Boyd v. United States, 116 U.S. 616, 630 (1886) ("private papers"); Nagareda, *supra* note 5, at 1642.

38. U.S. CONST. amend. IV.

39. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 773 (1994) (stating that the 1763 English *Wilkes* case "was *the* paradigm search and seizure case for Americans"); David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739, 1799 (2000).

40. Entick v. Carrington (1765) 19 Howell's State Trials 1029, 1038–39; Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1311 (2016) ("[In]dividuals' persons, papers, and effects were immune from government examination and interference."); Schnapper, *supra* note 21, at 915.

41. *See generally Entick*, 19 Howell's State Trials 1029; Wilkes v. Wood (1763) 98 Eng. Rep. 489; King v. Wilkes, (1763) 95 Eng. Rep. 737.

42. *See generally* Schnapper, *supra* note 21.

43. (1765) 19 Howell's State Trials 1029.

44. *See generally id.*

45. *See* BERNARD BAILYN, THE IDEOLOGICAL ORIGINS OF THE AMERICAN REVOLUTION 82–83 (1992). *See generally* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 602–1791 (2009).

46. *Entick*, 19 Howell's State Trials at 1066 ("[W]here private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass.").

Amendments. In *Boyd v. United States*,[47] the Court read the amendments as nearly running together to provide powerful, nearly absolute protection for a person's papers against law enforcement's efforts to obtain them for criminal prosecution.[48]

The *Boyd* holding was premised upon legal principles that would strike the modern lawyer as nearly absurd. First, it held that the search and seizure provision protected not only against literal physical seizures of papers but also against compelled production such as by a subpoena.[49] Merely requiring a person to produce the papers *himself* counted, in the Court's view, as a seizure. Today, the Fourth Amendment affords only a residue of protection against a subpoena—so scant that it is often ignored.[50]

Second, the Court held that the production of papers violated the Fourth Amendment's privacy protection for papers. The Court quoted *Entick* to remind us that papers contain a person's most private, secret thoughts and that they are therefore more sacred than any ordinary property or chattel.[51]

Third, it would violate the Fifth Amendment right against self-incrimination to *introduce* these papers in court against a criminal defendant. The papers in *Boyd* were business invoices—nothing particularly personal or private[52]—yet the Court afforded even these mundane papers protection.[53] The Court's principle veered near holding that the Fifth Amendment protects a defendant not only against testifying against himself but also from having to *give or furnish* any evidence against himself, even if this meant merely surrendering that evidence.[54] In the Court's view, the Fifth Amendment protected a person from having to assist in her own undoing. For much of the twentieth century, the Court continued to afford papers nearly absolute protection in criminal cases.[55]

But in a series of cases in the 1960s, the Court held that the Fourth Amendment only applied to subpoenas in a highly watered-down form because they are not literally physical seizures;[56] rather, they are orders that the suspect or defendant produce the documents themselves. The once-sacred privacy represented by a person's papers now yielded immediately to the needs of government investigations. For our purposes, in compelling a password, the Fourth Amendment would therefore impose no meaningful limits under these cases.

---

47. 116 U.S. 616 (1886).
48. *Id.* at 630, 633.
49. The government did not use a subpoena in *Boyd*, but the court deemed the procedure to be a compelled production and therefore a seizure. *Id.* at 634–35.
50. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 140 (2007).
51. *Boyd*, 116 U.S. at 627.
52. *Id.* at 618.
53. *Id.* at 634–35.
54. *Id.* at 637.
55. Schnapper, *supra* note 21, at 869.
56. SLOBOGIN, *supra* note 50, at 148–49.

But even more important, the Court in *Fisher v. United States*[57] held that the Fifth Amendment does not protect the contents of papers against compelled production, even if used against a person at trial in a criminal case.[58] The Fifth Amendment does not protect these *preexisting* documents because the government did not compel their content when created; the individual author created them voluntarily.[59] Now, in issuing a subpoena, the government merely seeks their physical surrender.[60] Except as discussed below, the witness producing the papers has not been compelled to "testify" under the Fifth Amendment.

Fisher marked the Court's shift from the originalist, and majestic, approach in *Boyd* to a more delineated, textualist approach.[61] The Court focused on the prohibition against compelling a person to be a "witness" against himself and equated this language with "testimony."[62] Unless the government compelled "testimony," it had not violated the self-incrimination clause.[63] Merely assisting the government in its prosecution by surrendering the incriminating documents no longer sufficed.

We can conclude that the Court has accomplished two main results in undoing *Boyd*. First, it has unbundled the two amendments so that they are no longer read together. Rather, they each govern isolated territories. Second, the Court has greatly curtailed what these amendments, now read in isolation, protect. As for papers, *neither* amendment affords much protection against their compelled production; they enjoy little privacy protection under the Fourth and little protection against self-incrimination under the Fifth.[64] Papers, once the sacred repository of private thoughts, have fallen on hard times. Whereas *Boyd* emphasized that papers are not ordinary chattel simply to be physically handed over, the Court in the twentieth century treated papers as just that, ordinary property to be "surrendered."

When we apply the foregoing to electronic devices, we will initially observe a strict division between the Fourth and Fifth Amendments to highlight how current doctrine applies. Part I.A considers the Fourth Amendment and its deficiencies under current case law, and the Fifth Amendment is similarly analyzed in Part I.B. The end of this Article shows how we can reunite them; indeed, the facts on the ground, a warrant to search a password-protected device, requires us to consider the two amendments together.

57. 425 U.S. 391 (1976).
58. *Id.* at 414.
59. *Id.* at 403–04.
60. *Id.* at 411 ("The question is not of testimony but of surrender." (quoting *In re* Harris, 221 U.S. 274, 279 (1911))).
61. *Id.* at 409 (stating that *Boyd* was a "rule searching for a rationale").
62. *Id.*
63. *Id.* at 410.
64. *See infra* Part I.A–B.

A. Fourth Amendment Deficiencies

In this section, we assume police have a warrant to search an *unlocked* device so we can focus on the Fourth Amendment alone and bracket the Fifth Amendment for now. For context, we can identify many ways in which the Fourth Amendment fails to protect privacy because it allows searches without a warrant, or even probable cause, under various exceptions. But we deal here with an often-unnoticed problem: Fourth Amendment case law affords too little protection to electronic devices even when government agents do ask a magistrate for a warrant.

First, it is not hard to get a warrant based upon probable cause. We assume the government already has arrested the suspect and therefore has probable cause to believe he has committed a crime. In this context, the police only need the additional margin of probable cause that the government will find some evidence of the crime on the suspect's smartphone or laptop. As Paul Ohm has pointed out, they will almost always have such probable cause.[65]

For example, in a drug investigation, law enforcement can likely meet this standard because drug dealers often use their phones to communicate with buyers and coconspirators, whether by text, email, or phone call.[66] Similarly, white-collar criminals will often have financial information on their smartphones or laptops, whether in the form of communications, banking applications, or spreadsheets.[67] Smartphones will often reveal location data too.[68] In a child pornography case, the same evidence leading to arrest will often show the suspect has images on his devices—for example, evidence that the suspect downloaded an image or reports from a spouse or other family member who saw a contraband image on a device.[69]

Second, once officers obtain a warrant, the Fourth Amendment's warrant clause imposes few limits. Law enforcement agents may seize a device, take it back to the lab, and conduct an exhaustive search in every nook and cranny by using advanced forensic software to guarantee nothing evades their notice.[70]

True, the warrant clause of the Fourth Amendment contains a particularity clause that requires the government to state with particularity the places to be searched and the things to be seized.[71] But numerous courts have held that the particular-place requirement is no more specific than the device itself, the type of device, or sometimes even just the residence in which the

---

65. Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1515 (2010).

66. *See, e.g.*, United States v. Alston, No. 15-CR-435, 2016 WL 2609521, at *1 (S.D.N.Y. Apr. 29, 2016).

67. *See, e.g.*, United States v. Makeeff, No. 4:14–cr–00081–SMR–CF, 2015 WL 13284966, at *1 n.4 (S.D. Iowa Feb. 6, 2015).

68. *See, e.g.*, *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 137 (E.D.N.Y. 2013).

69. *See, e.g.*, United States v. Grauer, 701 F.3d 318, 321 (8th Cir. 2012).

70. *See* FED. R. CRIM. P. 41(e)(2)(B) (permitting two-step search warrant execution, where law enforcement can conduct an off-site search of electronic material).

71. U.S. CONST. amend. IV.

device might be found.[72] Thus, a warrant need only list computers, memory media generally, or even simply a certain address.[73] As for the "things to be seized," a warrant might only need to recite the crime for which the police are seeking evidence on the device.[74] It is enough to say they seek evidence of child pornography, for example, or tax evasion.[75]

In conducting the search, courts often refuse to limit the police beforehand.[76] In most jurisdictions, law enforcement may essentially search the entire device to find evidence of the crime for which it has probable cause.[77] On the theory that a person could hide evidence in any deceptively labeled folder or file, law enforcement may look in every folder and file.[78] And, of course, if law enforcement agents run across evidence of another crime, they may immediately obtain a fresh warrant to continue searching for evidence of that newly discovered crime.

As a consequence, law enforcement will typically search information detailing a person's entire life. In a drug case, for example, agents will review photographs and videos for evidence of guns, money, or drugs in pictures[79] inevitably also seeing family photos, videos, and other very personal images. Agents will review financial files such as excel spreadsheets for evidence of financial dealings[80]—again, likely learning innocent but very private information. Agents can review emails, messages, and other communications for incriminating statements and to develop leads to other suspects.[81] They can also use the device to enter other online accounts to further search for photos, communications, and financial

72. *See* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 6–7 (2015).

73. *See id.*

74. *See* United States v. Deppish, 994 F. Supp. 2d 1211, 1221 (D. Kan. 2014).

75. Kerr, *supra* note 72, at 15–17.

76. *See id.* at 8 (noting that no circuit court has "required *ex ante* restrictions for computer warrants"). *But see, e.g.*, *In re* Search Warrant, 71 A.3d 1158, 1168 (Vt. 2012) (summarizing the debate on whether to impose ex ante restrictions or rely on ex post judicial review and approving ex ante limits).

77. *See* Kerr, *supra* note 72, at 8. *See generally* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241 (2010).

78. The Ninth Circuit has repeatedly held, for example, that even a single image or video of child pornography justifies agents' search of every computer device, every folder, and every file. *See* United States v. Schesso, 730 F.3d 1040, 1046 (9th Cir. 2013) ("The government had no way of knowing which or how many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner."); United States v. Krupa, 658 F.3d 1174, 1178 (9th Cir. 2011) (approving a search of fifteen computers based on one image); United States v. Brobst, 558 F.3d 982, 988, 993–94 (9th Cir. 2009) (finding that the search of "computers, compact disks, floppy disks, hard drives, memory cards, printers, and other portable digital devices, DVDs, and video tapes," based on a witness's observation of one illicit photograph in the defendant's home, to be reasonable).

79. *See, e.g.*, United States v. Burgess, 576 F.3d 1078, 1084 (10th Cir. 2009) (describing an agent's search for "trophy photos").

80. *See, e.g.*, United States v. Bustamonte-Conchas, No. 13-2028, 2014 WL 12697272, at *3 (D.N.M. July 8, 2014) (approving a search for drug activity including bank statements, records of distribution, and contacts with conspirators).

81. *See, e.g.*, United States v. Archibald, No. 2015-0041, 2016 WL 7469717, at *1 (D.V.I. Dec. 28, 2016).

documents, and to enter bank or travel accounts that can lead to obtaining bank records, hotel records, and flight information.[82]

Courts have generally refused to impose limits beforehand and stated that a warrant supplies agents with the authorization to look for relevant evidence wherever it might be found.[83] The Tenth Circuit, for example, held that agents may search for evidence of drug crimes in whatever form that might take, from financial documents to "trophy pictures," and look for them in any type of file, such as Word, WordPerfect, Adobe, Outlook, Lotus, Excel, Quicken, Access, or Paradox.[84] The court there drew a conclusion typical among other circuit courts: in the end, there may be no practical substitute for actually looking in many, or perhaps all, folders and sometimes at the documents contained within those folders.[85] Numerous scholars and courts have identified and attacked this broad search power, but they have struggled to announce workable solutions.[86]

The Fourth Amendment thus imposes few real restrictions on the search of electronic devices. If a suspect must surrender her password in the face of government compulsion, law enforcement will immediately obtain access to the entirety of her online life. Thus, much hinges on whether the government can compel this password under the Fifth Amendment.

The foregoing reflects the Court's sharp withdrawal from the protection of papers and electronic files and the privacy of their contents under both the Fourth and Fifth Amendments, but the twenty-first century has brought two promising developments. First, the Court in *Riley v. California*[87] erected a new Fourth Amendment principle with respect to electronic data.[88] *Riley* addressed an exception to the warrant requirement, but its general thrust could reinvigorate efforts to limit the scope of execution of warrants on electronic devices.

Second, the Court in *Fisher* left open an exception to its principle that the Fifth Amendment does not protect the content of papers—the act-of-production doctrine.[89] In the years since, the Supreme Court[90] and lower courts[91] have enlarged this exception to provide a surprisingly wide avenue for the protection of papers against compelled production. The Court has

82. *See* Riley v. California, 134 S. Ct. 2473, 2490 (2014) (describing the range of information available on mobile phone applications).

83. *See, e.g.*, *Burgess*, 576 F.3d at 1094. *But see* Kerr, *supra* note 77, at 1248–60 (describing ex ante restrictions imposed by some courts).

84. *Burgess*, 576 F.3d at 1093.

85. *See id.* at 1094.

86. *See generally* Gershowitz, *supra* note 22; Kerr, *supra* note 72.

87. 134 S. Ct. 2473 (2014).

88. *Id*. at 2478 (stating that "[a]bsent more precise guidance from the founding era," the Court would perform a balancing test for cases involving electronic data).

89. Fisher v. United States, 425 U.S. 391, 410 (1976) ("The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced.").

90. *See generally* United States v. Hubbell, 530 U.S. 27 (2000).

91. *See generally, e.g.*, United States v. Greenfield, 831 F.3d 106 (2d Cir. 2016); United States v. Ponds, 454 F.3d 313 (D.C. Cir. 2006).

also noted that the roots of the Fifth Amendment lie, in part, on principles opposed to government fishing expeditions and that it would interpret the act-of-production doctrine liberally, when necessary to enforce this norm.[92] This act-of-production doctrine, therefore, will form the backbone for developing a rule for the protection of passwords.

B. Fifth Amendment Protections: The Act-of-Production Doctrine

The Court in *Fisher* refused to accord Fifth Amendment protection to the content of papers, but, at the same time, it announced an exception. The Fifth Amendment does protect against the compelled production of papers when the act of production itself would be testimonial.[93] That is, "testimony" protected by the Fifth Amendment is not the content of the papers, but rather the physical act of production to the extent that the act itself communicates incriminating information.[94]

For example, if the government orders a suspected felon-in-possession to produce any firearms and he does so, he has communicated the fact that he possessed a firearm by the act of producing it.[95] He could only physically hand it over, after all, if he possessed it. Because possession is an element of the crime, the defendant, by physically handing over the gun, has implicitly admitted to incriminating facts about the suspected crime. At trial, the prosecutor could point to the defendant's production as strong evidence that he possessed the gun—and that he "knowingly" possessed as well.

To take another example, if a person ordered to produce all sources of income provides a bank statement, he has implicitly provided some evidence that the bank statement is authentic. After all, it came from his file, so possession here tends to authenticate the document as *his* bank statement. More significantly, since he produced it in response to a question about his income, *he* thinks it is responsive, and this inference from his belief also tends to authenticate it.[96]

Thus, *Fisher* held that the act of production *can* be testimonial and therefore protected by the Fifth Amendment if it discloses any of three categories of testimony: the "existence," "possession," or "authenticity" of the documents produced.[97] One might challenge whether we should count such an act as "testimonial" at all; after all, a suspect reveals this information inadvertently as a necessary byproduct of handing over the documents. He does not intend to communicate this information; he simply cannot help but

92. *Hubbell*, 530 U.S. at 32.
93. *Fisher*, 425 U.S. at 410.
94. *Id.* at 410–11.
95. *See* Commonwealth v. Hughes, 404 N.E.2d 1239, 1244 (Mass. 1980) ("If the defendant should produce the revolver, he would be making implicitly a statement about its existence, location and control to which the Commonwealth says it would allude at trial to show he had possession and control at some point after the alleged crime.").
96. *See, e.g.*, *Fisher*, 425 U.S. at 410 (stating that the defendant's turning over of documents expresses "[his] belief that the papers are those described in the subpoena," but there, he was not the author, nor was he able to authenticate them).
97. *Id.* at 410, 428–29; *see also Hubbell*, 530 U.S. at 36.

lead an observer to draw the natural inference. *Fisher* does not address this problem or explain why such inadvertent byproduct communications should count as testimony. We must therefore accept that such acts count as testimonial, though I will refer to this type of testimony as "quasi testimony" for much of this Article.[98]

Another problem arises with inadvertent communication testimony. By the Court's definition,[99] *every* act of producing documents will be testimonial. After all, every such act of production will communicate some information concerning the existence, possession, and authenticity of the documents. Without some limit, the act-of-production doctrine would swallow the rule that the Fifth Amendment does not protect against the compelled production of documents.

Perhaps with this breadth in mind, the Court in *Fisher* imposed two limits to the act-of-production doctrine—limits to what would count as "testimonial" in this context. First, the testimonial aspect of the production must be "sufficiently testimonial."[100] Second, the act of production will not count as testimonial if it is a "foregone conclusion" that the government already knows that the document exists, the person possesses it, and it is authentic.[101]

The Court in *Fisher* did not explain what principle it would use to measure how testimony will be sufficiently testimonial. Later cases do not readily illuminate the concept. Instead, in cases where the government seeks to use directly at trial the evidence produced, courts seem willing to find the defendant's act of producing such evidence sufficiently testimonial.[102] For example, if the government compels the production of child pornography from a defendant's laptop, the court will not make a separate inquiry into whether this production would be sufficiently testimonial. The production immediately admits two central elements of the crime: that the defendant possessed the contraband and likely did so knowingly.[103] As a consequence, at least in child pornography cases, we can assume the sufficiently testimonial requirement is always met.

The Court in *Fisher* also imposed a second limit to this act-of-production exception—an exception to the exception—called the "foregone conclusion doctrine."[104] If the information disclosed by the act of production is a foregone conclusion, meaning the government already knows it, then this act of production does *not* count as testimonial. Under this doctrine, if the

98. "Quasi testimony" shows that this inadvertent communication does not entirely resemble ordinary speech, in which a person does intend the words to communicate and not merely as abstract sounds or grunts. The term also reminds us that the Court affords act-of-production testimony less protection under the Fifth Amendment than it does to full-fledged oral or written testimony.

99. *See supra* note 97 and accompanying text.

100. *Fisher*, 425 U.S. at 411.

101. *Id.*

102. *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1346–49 (11th Cir. 2012).

103. *Id.* at 1346.

104. *Fisher*, 425 U.S. at 411; *see also* United States v. Hubbell, 530 U.S. 27, 44 (2000).

government knows the suspect possesses a particular document that it can describe with reasonable particularity then the suspect's act of production adds little to the government's overall knowledge. That production, therefore, would not count as testimonial.[105] If agents see an image of child pornography on a device before the defendant closes and locks it, those agents have likely also met the test.[106]

We might be tempted to say that the foregone conclusion doctrine measures whether, or to what degree, the testimony is incriminating. If the government already knows the person possesses the document, their production will not be highly incriminating, or at least its marginal value will not be. But *Fisher*, other courts, and scholars have correctly noted that the foregone conclusion doctrine rests not with whether the facts communicated are additionally incriminating, but rather with the threshold question of whether the court will count the act of production as testimony at all.[107]

In elaborating upon this foregone conclusion test, it is useful to divide between existence and possession on the one hand, and authenticity on the other. For existence and possession, the Second Circuit, the D.C. Circuit, and others have held that the government cannot merely infer the suspect possesses the demanded document; rather, it must know.[108] For example, the court in *United States v. Greenfield*[109] held that it is not enough that business people often possess certain documents or that it is customary for them to do so.[110] But if the government can identify particular bank accounts, it can usually establish that it knows that monthly statements for that account exist and that the defendant possesses them.[111]

For authenticity under the foregone conclusion doctrine, the government must show it can *independently* authenticate the required document at trial under the rules of evidence.[112] For a bank account statement, the government can establish this requirement by pointing to an available bank employee who could testify that the account statement is what it purports to be.[113]

Below, we apply the authenticity prong to encrypted devices and see that it amounts to our proposed rule of particularity: the government must know

105. *Fisher*, 425 U.S. at 411.

106. *See In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *3 (D. Vt. Feb. 19, 2009).

107. *See Hubbell*, 530 U.S. at 29; *Fisher*, 425 U.S. at 411; Minerva Pinto, *The Future of the Foregone Conclusion Doctrine and Compelled Decryption in the Age of Cloud Computing*, 25 TEMP. POL. & C.R. L. REV. 223, 223 (2016).

108. *See* United States v. Ponds, 454 F.3d 313, 324–26 (D.C. Cir. 2006); *see also* United States v. Greenfield, 831 F.3d 106, 118–19 (2d Cir. 2016); United States v. Fox, 721 F.2d 32, 37 (2d Cir. 1983); *In re Boucher*, 2009 WL 424718, at *3.

109. 831 F.3d 106 (2d Cir. 2016).

110. *Cf. id.* at 118, 122.

111. *Id.* at 119; *see also* United States v. Bright, 596 F.3d 683, 692–94 (9th Cir. 2010); United States v. Norwood, 420 F.3d 888, 895 (8th Cir. 2005).

112. *Greenfield*, 831 F.3d at 120.

113. *Id.* But if the bank is foreign, sometimes the government cannot make this showing because foreign banks will sometimes refuse to supply a witness to authenticate a client's bank account statements. *Id.*

the defendant possesses the document and be able to describe it with reasonable particularity.

II. ENCRYPTED DEVICES

When we say a device such as a laptop or smartphone is "locked" with a password, we mean not only that the device will not operate but that its storage memory is encrypted.[114] This Part first considers the scope of this encryption and, second, describes how encryption works.

A. Scope of Encryption

This Article focuses on encrypted devices that law enforcement has validly seized—data "at rest." But Apple and other communication platforms, such as WhatsApp and Facebook, have made end-to-end encryption standard for messages.[115] Similarly, internet web browsing and transactions are increasingly encrypted as they travel from host to server.[116] This means law enforcement agents cannot readily gain access to electronic communications—whether in real time or historically—from the intermediary service providers, as they once easily could. Now, law enforcement must seize a suspect's device and obtain any communications directly from the party to the communication. In other words, even communications have become, from a law enforcement viewpoint, data at rest. These communications are encrypted on the device and, like everything else, inaccessible to law enforcement without the password or some workaround.[117]

One of these workarounds, of course, is for law enforcement to obtain the data from the cloud.[118] But, even on the cloud, providers will increasingly encrypt both backups and other cloud storage in such a way that the provider

114. Many smartphones encrypt by default; however, users often must still enable encryption for laptops. *See* Whitson Gordon, *The One Thing That Protects a Laptop After It's Been Stolen*, N.Y. TIMES (Mar. 13, 2018), https://www.nytimes.com/2018/03/13/smarter-living/how-to-encrypt-your-computers-data.html [https://perma.cc/V3FQ-BE99]; Joe Miller, *Google and Apple to Introduce Default Encryption*, BBC (Sept. 19, 2014), https://www.bbc.com/news/technology-29276955 [https://perma.cc/5B8J-M878].

115. *See End-to-End Encryption*, WHATSAPP, https://faq.whatsapp.com/en/android/28030015/ [https://perma.cc/Y6PG-2Z3R] (last visited Aug. 24, 2018) (stating that end-to-end encryption is automatically implemented if both parties use an updated version of the WhatsApp application); *Privacy*, APPLE, https://www.apple.com/privacy/approach-to-privacy/ [https://perma.cc/795D-BL7F] (last visited Aug. 24, 2018); *see also* Andy Greenberg, *You Can All Finally Encrypt Facebook Messenger, So Do It*, WIRED MAG. (Oct. 4, 2016), https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/ [https://perma.cc/Y8H8-YN8N] (describing how a Facebook Messenger user must opt in to such encryption).

116. Albeit a leader, Google encrypted 95 percent of its internet traffic as of June 2018. *Transparency Report*, GOOGLE, https://www.google.com/transparencyreport/https/?hl=en [https://perma.cc/8WX8-X7W4] (last visited Aug. 24, 2018).

117. *See generally* Kerr & Schneier, *supra* note 27 (canvassing possible workarounds).

118. *Id.* at 1010.

itself will be unable to decrypt them.[119] The cloud too, therefore, will come to resemble an encrypted device.

Finally, law enforcement will need an individual's passwords to conduct other types of investigations. New technology such as Bitcoin and other cryptocurrencies, and new legal instruments such as smart contracts, all depend upon a person keeping safe and secret passwords. Often, no centralized institution will have that password, so law enforcement will be able to access the Bitcoin, for example, only by compelling a person to reveal their password.[120] Consequently, what goes for the encrypted device will similarly apply to a vast array of investigative areas.

B. How Encryption Works

When we say a password locks a device, we refer to a few related protections based upon strong cryptography. Let us first consider smartphones such as the iPhone. First, when a person enters a password, the device verifies the password so that it will operate. The device verifies the password to release a longer, stronger encryption key, which, in turn, unlocks another series of encryption keys down a hierarchy ultimately allowing the device to work and access all the data kept on storage memory.[121]

Second, the smartphone decrypts the storage memory so that the device and user can access the messages, documents, photos, and other files and data on the device. This means that if law enforcement simply removes the storage media from the device—its hard drive or hybrid flash drive—and accesses the drive directly with laboratory equipment, investigators will face an encrypted scramble. Without the password, it is nearly impossible to decrypt the hard drive. For smartphones, the password will only work to decrypt the hard drive if the drive remains within the device, because decryption depends upon a chain of encryption keys, some of which are within the hard circuitry of the device itself.[122]

The above applies to nearly all smartphones because most automatically encrypt their contents.[123] Every time its owner enters her passcode or password and "unlocks" the phone, she also decrypts its contents, or at least makes them available to be decrypted.[124] Laptops and desktops may not encrypt their hard drives or other persistent storage as thoroughly or

119. *See iCloud Security Overview*, APPLE, https://support.apple.com/en-us/ht202303 [https://perma.cc/46G9-2M6T] (last visited Aug. 24, 2018).

120. A person ultimately controls their Bitcoin or other cryptocurrency by way of a much longer private key. Usually a person accesses that key by way of a shorter password or, more often, passphrase. *See infra* notes 226–28 and accompanying text. Either way, the government will need to compel this content from the individual herself.

121. *See* APPLE, *supra* note 7, at 13–16.

122. *Id.*

123. *Id.* (noting that each device has a unique ID number burned into its hardware to power the AES 256 encryption engine).

124. iPhones build a hierarchy of encryption keys upon the hardware key in order to encrypt and decrypt files as they are added or read. *Id.*

automatically as does a smartphone. But, individuals can take deliberate steps to encrypt even these devices[125] as well as their cloud data.[126]

1. Passwords, Passcodes, and Keys

This Article focuses on a suspect's password or passcode, often as short as four or six digits. For simplicity's sake, we will proceed as if a password or passcode directly encrypts and decrypts the device and a court order directs a person to enter this password or passcode.

But the password or passcode does not, itself, encrypt or decrypt the device.[127] Rather, when a user enters a password, the device verifies it without recording it long term. Once it verifies the password, the device can access the actual encryption key or keys and use this separate, far longer key to encrypt and decrypt the device. Nothing in the argument below depends upon this difference—the only important point is that the device, through the magic of encryption technology, can verify the user's password without recording it.

2. Deniability

More advanced encryption affords users "deniability" by giving them *two* passwords. One password decrypts the encrypted drive correctly to its real documents. The other password decrypts at least part of the drive to realistic, but dummy, documents that the user supplies, leaving the real files encrypted. The suspect can thus supply the fake password that will decrypt the drive, or a portion of it, to innocent documents in a way that appears to truly decrypt the drive.[128]

III. CATEGORIES OF COMPULSION

We can now turn more directly to the law of encrypted devices, but we cannot properly evaluate a claimed Fifth Amendment privilege without first deciding how to characterize and categorize the compulsion itself. Courts and scholars have not comprehensively categorized the different scenarios

125. *See Use FileVault to Encrypt the Startup Disk on Your Mac*, APPLE, https://support.apple.com/en-us/HT204837 [https://perma.cc/6LWB-94QW] (last visited Aug. 24, 2018). Numerous established security outfits provide rigorous disk encryption software such as VeraCrypt and Symantec. *See* Neil J. Rubenking, *The Best Encryption Software of 2018*, PC MAG. (July 17, 2018, 1:01 PM), https://www.pcmag.com/article/347066/the-best-encryption-software-of-2016 [https://perma.cc/C65M-JARB].

126. RASS & SLAMANIG, *supra* note 34, at 1 ("Cloud computing is one of these new areas, where cryptography is expected to unveil its power by bringing striking new features to the cloud.").

127. *See* Brief of *Amicus Curiae* Professor David W. Opderbeck et al. at 6, Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014).

128. *Gelfgatt*, 11 N.E.3d at 616–17 (holding that the defendant could be ordered to enter the real password and not the secondary password).

pertaining to encrypted devices nor provided a theoretical foundation for those scenarios.[129] This Part therefore fills this gap.

First, this Part considers scenarios where law enforcement compels a defendant to state his password orally or write it down. This is an important scenario because it forms the foundation for understanding, by contrast, how to characterize merely entering a password. Second, this Part briefly considers whether the government may subpoena documents in which the suspect has written down her password, such as the sticky note posted to the edge of the computer screen or a written list naming accounts or devices with their respective passwords. Third, this Part then considers the compulsion to enter a password such that no one observes the password and the device does not record it. Finally, this Part considers thumbprints and facial recognition used to open a device.

A. Compulsion of Passwords Directly

The government may require a defendant, subject, or witness to provide her passcode in a number of ways. In some cases, the government simply orders the defendant to state her password.[130] In others, the government might use a subpoena ad testificandum to order the defendant to appear to testify and then ask her for the password or order her to write it down.[131] If the witness refuses to comply, law enforcement may seek a court order compelling her to comply on pain of contempt and potentially face jail time.[132] Or police officers may take a suspect into custody and request the passcode before they provide the *Miranda* warnings—such a request would likely constitute interrogation and therefore compelled testimony under *Miranda*.

These methods of compelling a password directly involve testimony in its purest form and therefore should trigger direct Fifth Amendment protections. As the Supreme Court has said on numerous occasions, compelled oral statements of facts will usually be considered testimonial,[133] and this case should be no exception. In such instances, the Court has held that "the vast majority of verbal statements thus will be testimonial" because they likely "convey information or assert facts."[134] The Court has repeatedly connected testimony to true or false statements—particularly instances in which a person could lie—in part because of the history of the Fifth Amendment.

---

129. *But see generally* Cohen & Park, *supra* note 18 (drawing different categories from those sketched here and focusing on the difference between compelling entering a password versus compelling production of decrypted versions of the files).

130. *See generally, e.g.*, Commonwealth v. Baust, 89 Va. Cir. 267 (2014). Though far from clear, the government in that case appeared simply to compel the defendant to state his passcode. *See id.* Ultimately, the court held that the defendant could be compelled to produce his fingerprint but could not be compelled to produce his passcode. *See id.*

131. *See, e.g.*, United States v. Kirschner, 823 F. Supp. 2d 665, 666 (E.D. Mich. 2010).

132. FED. R. CRIM. P. 17(g) (stating that a court can hold a witness "who disobeys a subpoena issued by a federal court" in contempt).

133. *See, e.g.*, Pennsylvania v. Muniz, 496 U.S. 582, 589 (1990).

134. *Id.* at 597 (quoting Doe v. United States, 487 U.S. 201, 213 (1988)).

One of the Court's chief objectives is to prevent the government from placing a suspect in the "cruel trilemma" by forcing him to decide whether to tell the truth and incriminate himself, lie and perjure himself, or refuse to answer and face contempt and jail.[135]

Put another way, when a person discloses her password orally or in writing to agents for the specific device the police have seized, she likely is *also* disclosing her password to other, innocent devices, as well as to many of her online accounts including social media, bank, and email accounts. The *content* of the password thus provides law enforcement agents with information they can use to access these other portions of the suspect's life.

For these numerous reasons, courts and scholars agree that the Fifth Amendment, at its core, protects statements that are true or false, and stating a password to authorities falls within this core protection.[136] The words and letters the suspect utters are either the password to this device or they are not.

This situation does not fall into the narrow class of cases in which verbal statements might not count as testimony, as occurred in *Pennsylvania v. Muniz*.[137] There, officers asked a drunk suspect to state his name, his age, and other facts.[138] He stumbled over the answers because he was drunk.[139] The Court held these statements were not testimonial.[140] Although the decision was fractured, we can interpret the case as holding that the government did not rely upon the truth or falsity of the statement to incriminate the defendant, but rather the *manner* in which he delivered the answers.[141]

In compelling a password, by contrast, the government does not rely upon the manner in which the suspect states the password—whether she hesitates, struggles to remember it, or states it immediately. Rather, the government relies upon the truth or falsity of the password to decrypt the documents.

Although we might wonder whether the government can give the suspect immunity and then compel her to disclose her password orally, this method does not provide a solution. Under *Kastigar v. United States*,[142] any immunity the government affords in exchange for disclosure of the password will also protect any fruits or derivative use.[143] This means that the immunity will likewise protect the documents the password decrypts, as well as any information contained within those documents. Similarly, the immunity will protect any information derived from the documents. Immunizing oral disclosure of the password will effectively immunize everything. This strong

135. *Id.* at 596.

136. *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1346 (11th Cir. 2012); *Kirschner*, 823 F. Supp. 2d at 669.

137. 496 U.S. 582 (1990).

138. *Id.* at 590.

139. *Id.*

140. *Id.* at 600.

141. *Id.* at 592; Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and Its Future Predicted*, 94 J. CRIM. L. & CRIMINOLOGY 243, 273–74 (2004).

142. 406 U.S. 441 (1972).

143. *Id.* at 444–45.

Kastigar immunity arises from the nature of stating a password as ordinary, oral testimony enjoying full Fifth Amendment protection and stands in contrast to the more limited effect of granting act-of-production immunity.

B. Sticky Notes

In a different scenario, law enforcement subpoenas the suspect to produce any *documents* that contain the password, such as a sticky note on a desk at home. Under *Fisher*, such compulsion does not directly violate the Fifth Amendment because the person voluntarily created the document before the subpoena and has thus not been compelled.[144] But the Fifth Amendment may protect against such compulsion if the *act* of producing documents with the password would, itself, be testimonial.

Producing a written password admits that the person has written it down and that they possess the password, but this fact is neither incriminatory nor does it lead to incriminatory evidence. Possession of a password is not a crime. True, the content of the password shows that a person has access to a particular device, but under *Fisher*, the contents of documents are not protected.[145]

But when we consider authentication, we see why a person might enjoy act-of-production protection over a sticky note with a password. If the subpoena demands the password for a particular device, in producing the sticky note, a suspect implicitly testifies that the number written there *is* a password and that it is a password for *this* device.[146] In other words, she authenticates the content by producing it. But, if the sticky note says "iPhone: 1234," then the note is likely self-authenticating, and her act of producing it would not be sufficiently testimonial to warrant protection.

C. Entering a Password into the Device

We now come to the central, paradigmatic scenario: an order requiring the defendant to enter his password into the device to allow the government to access decrypted versions of the files on the drive. No one observes the password entered, and the device itself makes no record of the password.

On its surface, the government is not compelling testimony but a mere physical act; however, this section suggests three analogies to characterize

144. *See supra* notes 57–60 and accompanying text; *cf.* United States v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982, at *54 (N.D.N.Y. May 24, 2006) ("Defendant more than likely reduced the password to writing. Production of this voluntarily created writing would not, the Government argues, constitute compulsion. Defendant has not responded to this argument.").

145. *See* United States v. Ponds, 454 F.3d 313, 323 (D.C. Cir. 2006) ("[T]he contents of the documents are irrelevant for constitutional purposes because their preparation was not 'compelled.' . . . Therefore, to determine whether an act of production implicates the Fifth Amendment, the court looks only to the communicative aspects of the act of production itself." (quoting Fisher v. United States, 425 U.S. 391, 409–10 (1976))). However, under *Hubbell*, when considering the existence prong, it is possible that the content of documents can count as the source of incrimination. *See* United States v. Hubbell, 530 U.S. 27, 31 (2000).

146. *See supra* notes 93–96 and accompanying text.

the compelled act of entering a password[147]—oral testimony, a physical act, or an act of producing documents.

As for legal process, the government may serve upon the suspect a document subpoena requiring he produce decrypted versions of the encrypted files.[148] This subpoena, of course, is a legal fiction: the government already controls the device and actually requires that the defendant enter his password. Alternatively, the government may obtain an All Writs Act order requiring the defendant assist in the execution of the underlying search warrant by entering his password, or a "decryption order."[149] These processes all require precisely the same act by the suspect: enter a correct password into the device—and then walk away.[150]

1. Oral Testimony

We could consider entering a password into the device as analogous to compelling the defendant to state the password orally to law enforcement agents. If so, the Fifth Amendment would prohibit compelling a defendant to enter his password for the reasons discussed above.[151] This section will canvas the similarities and differences between entering a password and oral testimony.

First, typing a password seems quite similar to stating it or writing it down. But this similarity largely evaporates when we consider that no agent observes the typing or records the password and, perhaps more important, the device itself can verify the password is correct without keeping a record of it.[152] This compulsion thus resembles an order for a suspect to go into a room and whisper something to himself—a secret act that is oral but does not really resemble testimony.

Second, one could argue that entering a password, just like disclosing it to law enforcement, has the same end result: agents get access to the device. But this result alone cannot decide the issue because the same is true of a true

147. Some may wish to analogize compelling a person to enter a password to the government compelling a person to secretly enter a combination to a safe so law enforcement agents may access the files within. This is a precise analogy, but it does not help because the Supreme Court has not addressed the safe scenario either. In other words, our analysis must answer both scenarios.

148. *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1339, 1349–50 (11th Cir. 2012) (holding that the government may only compel this production if it also grants the subpoena recipient immunity).

149. *See, e.g.*, United States v. Apple MacPro Comput., 851 F.3d 238, 243 (3d Cir. 2017).

150. In contrast, this Article proposes a rule of particularity that would require that the defendant decrypt only those files that meet the test. *See infra* Part IV.C.

151. *See supra* Part III.A. This inquiry focuses not on whether the act of entering a password is testimonial, but rather whether it is tantamount to *oral* testimony. This Article concludes that the act of entering the password is "testimonial" as the Court uses that phrase, but only the weaker, quasi testimony that arises under the act-of-production cases. *See infra* Part IV. In other words, entering a password *is* testimonial, but it is more like act-of-production testimony than oral testimony.

152. *See* Kerr & Schneier, *supra* note 27, at 994–95.

key. If the suspect has been ordered simply to turn a key, that act would likely not constitute full-fledged testimony even though it has the same result.

A third argument presents a powerful case: compelling a person to enter a password, even secretly, requires him to use the contents of his mind to further the prosecution's case. The Court has often considered, as a shorthand method to measure whether an act counts as testimony, whether the compulsion requires the suspect to use the contents of his mind.[153] One could elaborate upon this argument by saying the use of the mind does not involve simply the entering of a password, an act that may come almost as second nature, but all the mental energy that has gone into creating, memorizing, and maintaining the password.

In response to this third argument, we may say that the suspect does not communicate these mental steps to any outsider. That is, even if we were to accept the view that an act might be testimonial because it incorporates antecedent mental activity, that still does not seem to make the resulting act itself similar to *oral* testimony. Indeed, the Court uses this test, the use of the contents of the mind, merely to determine whether an act counts as "testimony" at all, not whether it is tantamount to full, oral testimony.[154]

Finally, compelling a person to enter her password may place her in the position of the cruel trilemma.[155] She may decide to enter the correct password and potentially incriminate herself, to lie by entering the wrong password,[156] or refuse to enter anything and face contempt.

Here too, this cruel trilemma argument helps us see that the act of entering the password is testimonial, but more like act-of-production testimony than full, oral testimony. This follows because agents will immediately know if the suspect has entered the wrong password—the device will not open and will indicate that the wrong password has been entered by vibrating, for example. As a result, this lie—or false entry—is not material and therefore not perjury.[157] No one relies on its truth in any way and the lie is of no consequence to the action because agents immediately and certainly know the password is wrong.[158]

One niche case arising out of sophisticated encryption schemes *may* implicate the cruel trilemma in a manner that seems analogous to oral testimony. These programs will supply a user with *two* passwords: one is the real password that decrypts the disk to the original contents, but the

153. *See, e.g.*, United States v. Hubbell, 530 U.S. 27, 43 (2000) (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)); *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1345–46 (11th Cir. 2012).

154. *Hubbell*, 530 U.S. at 43.

155. *See supra* note 135 and accompanying text.

156. If she does so ten times with an iPhone, she knows this will potentially lock the phone forever. *See* APPLE, *supra* note 7.

157. *See* United States v. Martinez, 855 F.2d 621, 623 (9th Cir. 1988) ("A false statement is not perjurious unless material."); *see also* 18 U.S.C. § 1623(a) (2012) (criminalizing the act of making a "false material declaration" to a court or grand jury).

158. United States v. Cromitie, 727 F.3d 194, 221–22 (2d Cir. 2013) ("[P]erjury is 'material' if there is any 'reasonable likelihood that the false testimony could have affected the judgment of the jury.'" (quoting United States v. Agurs, 427 U.S. 97, 103 (1976))).

second one is a dummy password that works but "decrypts" at least part of the disk to files that are not the real files.[159] They are plausible in that they appear to be real files, but they are not the originals.[160] This feature of encryption is called deniability. Thus, this suspect faces a true temptation to lie and enter her dummy password. And if she enters the dummy password, agents will not immediately realize it and may rely on what appears on the disk—a disk that contains innocent files only.

For now, at least, we can put aside this niche case because deniable encryption remains rare. But as encryption develops, we may need to take this problem more seriously. When we do, however, we might conclude that supplying a false password still resembles act-of-production testimony more than oral testimony. After all, a person producing documents can produce false, innocent documents; his act of producing them will implicitly communicate that the documents are authentic when he knows that they are not. Despite this possibility, we still deem the act-of-production testimony to be on a lesser plane than oral testimony.

Few cases expressly consider this question,[161] and those that do find that typing in a password, or opening a combination lock, counts as testimony, but not necessarily testimony on the level of ordinary, oral testimony. Rather, the courts suggest that entering a password counts as quasi testimony akin to an act of production.[162]

2. Pure Physical Act

At the other end of the spectrum, we could treat the act of entering the password as a pure physical act deserving no protection whatsoever under the Fifth Amendment—not even the quasi-testimonial act-of-production protection. The main precedent concerning compelled, incriminatory acts arise from a long series of "physical characteristic" cases. In these cases, the government has compelled the suspect or defendant to perform a physical act that will potentially incriminate him. In the leading Supreme Court cases, the government required the defendants to wear a shirt found at the scene of the crime so the jury could see whether it fits,[163] to display his face,[164] to provide a handwriting sample,[165] and to supply a voice exemplar.[166]

---

159. *See* Timothy A. Wiseman, *Encryption, Forced Decryption, and the Constitution*, 11 I/S 525, 570–72 (2015).

160. *Id.*

161. *See* Reply Brief of Appellant at 11–12, United States v. Apple MacPro Comput., 851 F.3d 238 (3d Cir. 2017); *cf.* United States v. Green, 272 F.3d 748, 753–54 (5th Cir. 2001).

162. *See Apple MacPro Comput.*, 851 F.3d at 247–48.

163. Holt v. United States, 218 U.S. 245, 252–53 (1910).

164. United States v. Wade, 388 U.S. 218, 222 (1967).

165. Gilbert v. California, 388 U.S. 263, 265–67 (1967) (discussing the requirement for the defendant to provide a handwriting sample to see if his handwriting matched that of the robbery note).

166. United States v. Dionisio, 410 U.S. 1, 5–6 (1973).

In every case the compelled act may incriminate, but the Court repeatedly held that the Fifth Amendment did not apply at all.[167] The acts merely displayed physical characteristics of the defendant, and the defendant enjoyed no privilege to hide these.[168] Even a handwriting or voice exemplar, which veer closest to testimony, do not enjoy protection because they are physical characteristics.[169] Additionally, the government compels them not for their truth but for their manner; it does not matter what the person writes, but merely how he forms the letters.[170]

Compelling a person to enter a password differs. First, it is not a physical characteristic to distinguish or identify a person. Put another way, the government does not compel the act to weigh the manner in which it is done. Rather, it compels the act because its communicative content will open the device. Compelling a person to enter a password thus does not resemble the physical characteristic cases for us to determine that such an act does not enjoy Fifth Amendment protection.

3. Production of Documents

The third analogy, the one upon which we settle, as have most courts,[171] is that entering a password bears the closest resemblance to the act of producing documents. In both cases, the government seeks documents and the act produces them. But more importantly, the testimonial nature of each act bears striking similarities that help us understand how the Fifth Amendment relates to the act of entering a password. As noted above, the act of producing a document or item communicates in a few ways.[172] If the government compels a person to produce any guns, by producing a gun the person communicates that he possesses the gun, that he knows he possesses the gun, and that it is, in fact, a gun (because it shows he believes it is a gun).

When a person opens a device by entering a password, that act similarly communicates that he controls the device and therefore possesses the documents on it. It communicates that he likely possesses those documents knowingly. Finally, he authenticates the documents. The subpoena seeks decrypted versions of the encrypted files, and by entering his password and unlocking the device, he has demonstrated that the now decrypted files match the encrypted files previously on the drive.

Finally, in both cases the government will use the evidence in similar ways at trial. If the defendant produces the gun, the government would like to use that act as evidence at trial that he possessed the gun. In fact, it may well be the *only* evidence showing such possession. Similarly, the government

167. *Id.* at 7; *Gilbert*, 388 U.S. at 266; *Wade*, 388 U.S. at 222–23; *Holt*, 218 U.S. at 252–53.

168. *See* cases cited *supra* note 167

169. *Dionisio*, 410 U.S. at 6.

170. *Gilbert*, 388 U.S. at 266.

171. *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1342–46 (11th Cir. 2012); Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614–15 (Mass. 2014).

172. *See supra* Part I.C.

would like to use the fact that the defendant entered the password to establish that the files it introduces at trial were previously in the defendant's possession, he knew he possessed them, and that they are the same images as the encrypted files originally on his drive when seized.

One could object and argue that ordering a defendant to enter his password differs from a document subpoena. In an ordinary document subpoena, the government seeks documents that already exist, and *Fisher* held the Fifth Amendment does not protect against producing documents precisely because they already exist.[173] But when a person enters his password, the decrypted version of the documents do *not* already exist; that is precisely the government's problem. Rather than requiring the suspect to produce existing documents, it has required him to *create* documents—leading us to wonder whether the Fifth Amendment might protect them for this reason.

This argument sounds more appealing than it really is.[174] When a person decrypts a document, he does not really create a new document in the relevant sense. After all, he originally created the document in plaintext, so the document is preexisting in this sense. When he closes his computer, the software encrypts the drive so that the plaintext document becomes scrambled into an encrypted jumble of bits.[175] But asking him to decrypt it again merely asks him to restore the original document he created. In other words, he has not been compelled to create new content but merely to restore old content.

Furthermore, when a person decrypts, he does not read the encrypted version and translate it using his cognitive powers. Entering or uttering the password itself may constitute testimony,[176] but that does not mean he has *created* new documents merely by decrypting them.

IV. COMPELLING DECRYPTED VERSIONS

We have concluded that entering a password resembles the act of production, but this doctrine includes a proliferation of tests, exceptions, and variations. Testimony falls into three categories: existence, possession, and authenticity. The testimony must be sufficiently testimonial, by some mysterious measure.[177] For existence cases, at least, the Court requires that the defendant make extensive use of the contents of his mind to count as sufficiently testimonial. But for possession and authenticity cases, it seems enough that the document produced would be used at trial. Finally, the government can still compel testimony if it satisfies the foregone conclusion doctrine. This Part discusses the categories of act-of-production cases and applies the doctrine to encrypted devices.

173. Fisher v. United States, 425 U.S. 391, 411 (1976).
174. *See generally* Cohen & Park, *supra* note 18.
175. *See id.* (manuscript at 7).
176. *See supra* Part III.C.1.
177. *See supra* notes 100–03 and accompanying text.

A. The Three Prongs and a Rule of Particularity

The "existence" prong captures the idea that if government agents know that the suspect possesses the file, they also know that suspect knows it exists. In this respect, the suspect does not make "extensive use of 'the contents of his mind'"[178] in entering a password, so the test for whether something is sufficiently testimonial for the existence prong might not be met anyway. Therefore, this analysis would perform no additional work beyond the other two prongs—possession and authenticity.

Under the possession prong,[179] it is not difficult to see why the act of production in a possession-crime case will count as sufficiently testimonial because the act of entering a password communicates several incriminating facts. First, it almost conclusively demonstrates that the suspect possessed the images. Second, this fact, possession, is highly material because it is an element of some crimes, including possession of child pornography[180] and receipt of such images.[181] Similarly, his act of entering the password is probative to another fact: knowledge. The fact that the images appear on a device he is able to open increases the probability that he *knowingly* possessed the images—another element of certain crimes.[182] Finally, at least with individual devices such as smartphones, the very fact that it is locked makes it more likely that whoever can open it is the only person who can do so. The moment the suspect opens it, in this context, makes it more likely the child pornography is his and not someone else's.

The authentication prong provides the most support for the rule of particularity that this Article proposes, in part because it arises from the scientific nature of strong encryption, but also because the principles flow naturally from the ordinary nonencryption cases.

The rules of evidence require that the prosecutor authenticate any files she introduces at trial,[183] and the foregone conclusion doctrine requires that she be able to do so *independent* of the suspect's act of production—in our case, entering the password. In *Greenfield*, for example, the government subpoenaed foreign bank account statements from the defendant.[184] If the

178. United States v. Hubbell, 530 U.S. 27, 43 (2000) (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)).

179. The test proposed in this Article is essentially the test for the possession prong; therefore this Article's proposed framework is not a simplification of this concept, at least in cases where possession is at issue. As noted above, in possession crimes, such as child pornography, courts *always* treat the act of production as sufficiently testimonial. *See supra* notes 102–03 and accompanying text. As a result, in possession-crime cases, the foregone conclusion test become the sole test.

180. *See, e.g.*, 18 U.S.C. §§ 2252, 2252A (2012).

181. *Id.*; United States v. Benoit, 713 F.3d 1, 6–7 (10th Cir. 2013) (holding that possession is a lesser included offense of receipt of child pornography).

182. *See* 18 U.S.C. §§ 2252, 2252A; *cf.* United States v. X-Citement Video, Inc., 513 U.S. 64, 68–79 (1994); United States v. Grauer, 701 F.3d 318, 324 (8th Cir. 2012) (holding that the wife's testimony that the defendant alone used the laptop regularly was sufficient to establish that he knowingly possessed the child pornography on it).

183. *E.g.*, FED. R. EVID. 901.

184. United States v. Greenfield, 831 F.3d 106, 112–13 (2d Cir. 2016).

defendant produced these statements in response to the subpoena, that act of producing them *from his own files* would authenticate them as *his* bank records.[185] Therefore, the Second Circuit held that the government could not compel this production unless it had the means to show they were his bank records independently.[186]

Normally, a prosecutor would subpoena a bank employee to review the records and authenticate them as those of the defendant, but in *Greenfield*, the foreign banks at issue refused to make any employee available to authenticate the bank records or provide the underlying account statements in the first place.[187] As a result, the government could not authenticate the bank statements independently of the defendant's act of production, and the government failed to meet the requirements of the foregone conclusion doctrine.[188] The Fifth Amendment therefore protected Greenfield from having to produce those bank statements.

When we apply these principles to encryption, we see that the government must show it can authenticate the files independently of the defendant's act of entering the password. That is, it must be able to show that the decrypted file it shows the jury came from the defendant's hard drive and that it belongs to the defendant.[189] In other words, it must show that the file in evidence matches the encrypted file that the police originally seized from the defendant.

We can compare this situation to a party's burden when presenting the translation of a document from a foreign language into English for the jury. The party must show that the English translation really is an accurate translation of the original document. To do so, it must show that the person who performed the translation speaks both languages and that this person can affirm that the English version is indeed an accurate translation from the foreign language.[190]

If we think of the computer forensic expert as the "translator" in the above cases, one might believe she could compare the decrypted file with the encrypted file and show, through some kind of math, that the one is a decryption of the other—just as a translator can compare the original Spanish version with its English translation. But this belief is wrong. The entire point of strong encryption systems is to prevent someone from comparing the digital files alone and showing they match. Instead, a secure encryption system is defined to mean that given a particular decrypted file, any other file

185. *Id.* at 118.
186. *Id.* at 122.
187. *Id.*
188. *Id.*
189. In this context, authenticate does not mean a showing that the image actually depicts a minor and that the other elements of child pornography are met. Rather, authenticate here means that the document or image is what the government claims it to be: an accurate decryption of the encrypted file seized from the defendant.
190. FED. R. EVID. 604 ("An interpreter must be qualified and must give an oath or affirmation to make a true translation."); Kassim v. City of Schenectady, 415 F.3d 246, 251 (2d Cir. 2005).

is just as likely to represent the encrypted version as the one presented.[191] Only the key, or the password leading to the key, can show that the two files match.

Instead, the "translator" in this case is the defendant. When the defendant enters his key, he translates the encrypted version to the decrypted version. But the Fifth Amendment prohibits the prosecutor from pointing to the fact that the defendant entered his key to decrypt the files; the foregone conclusion doctrine requires that the prosecutor authenticate the files independently of the defendant's act of production. The government cannot avoid this result by compelling the defendant to state his password and then having government agents enter it themselves. This course would avoid the authentication problem, but it would amount to ordinary compulsion of oral testimony, which violates the Fifth Amendment.[192]

Finally, immunity provides no solution here. If we grant immunity to a defendant who then states his password to an agent, then *Kastigar* applies and the government cannot even use the contents of the files recovered.[193] Even if the government immunizes the suspect's *act* of entering his password, it is still stuck because it will be unable to show that the decrypted version introduced at trial matches the encrypted version found on the defendant without introducing to the jury the fact that the defendant entered his password. Because the fact of this action is precisely what the government has immunized, it therefore cannot use that act against him at trial.

We can now show how the authentication prong boils down the rule of particularity proposed in this Article. As described in this Part, the government cannot authenticate any files it obtains from a locked device by technological or mathematical measures; rather, it must rely on a human witness to authenticate it. Such a witness might be a spouse or investigator who saw the image on the device. If so, that person would testify in court that the image the prosecutor has shown to the jury matches the one the witness saw on the defendant's device when it was not locked.

In order to authenticate this information under the Federal Rules of Evidence, this witness must (1) have firsthand knowledge that the defendant possessed the image on the device,[194] and (2) be able to describe it well enough to persuade a jury that the two images are the same.[195] This test aligns with this Article's rule of particularity. If we assume the witness is working with law enforcement, then law enforcement will know the suspect

191. *See generally* JONATHAN KATZ & YEHUDA LINDELL, INTRODUCTION TO MODERN CRYPTOGRAPHY (2d ed. 2015) (discussing how strong encryption withstands known plaintext attacks and more determined ones as well).

192. *See supra* Part III.C.

193. *See supra* notes 142–43 and accompanying text.

194. *See* FED. R. EVID. 602 (requiring "personal knowledge"); *id.* r. 701(a) (requiring "witness's perception" for lay opinions); *id.* r. 901(b)(1) (providing that a "witness with knowledge" may authenticate evidence).

195. *Id.* r. 901 (stating that testimony must be "sufficient to support a finding that the item is what the proponent claims it is"—in this case, the same as the one seen on the device).

possesses the file on the device and will be able to describe it with reasonable particularity. The reasonable-particularity test closely parallels the federal evidentiary requirement that the testimony be sufficient to show the files are the same.

B. Application of the Rule of Particularity to Locked Devices

We can now apply the rule of particularity to locked devices under the foregone conclusion test. When the police arrest a person with a locked device, do they know whether he possesses certain documents that they can describe with reasonable particularity? In some cases, they will not. If the police arrest a person for drug dealing, they will have probable cause to believe there is some kind of evidence on his phone, but nothing in particular. They will not be able to describe particular messages, images, or spreadsheets.

On the other hand, in many child pornography cases, the government will meet the test. This follows because the government likely developed probable cause in the first place because an agent, spouse, or other individual saw a particular image on the defendant's device,[196] or the authorities may have forensic evidence that the defendant downloaded certain files, usually by comparing the hash value of the file downloaded with the hash value of known contraband images.[197]

For example, in *In re Boucher*,[198] police saw particular images on the defendant's computer before he closed it.[199] Thereafter, they could not access the computer files without a password.[200] The grand jury demanded that he produce the unencrypted versions of the files on the hard drive.[201]

The defendant argued that requiring him to produce the unencrypted versions would require an act of production which, itself, would be testimonial.[202] The court disagreed and enforced the subpoena.[203] It concluded that the government had satisfied the foregone conclusion doctrine because it could identify the documents sought with reasonable particularity—law enforcement had already seen them.[204]

---

196. *See, e.g.*, *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1–2 (D. Vt. Feb. 19, 2009). How particularly must this witness describe the image? Courts can develop guidelines, but commonsense factors can be used to identify an image: the setting and lighting of the image (indoors, outdoors), the apparent age of the child, the number of persons depicted, their clothes, hair color, and conduct.

197. Internet service providers regularly report when they detect contraband images crossing their networks, again based on hash values. *See, e.g.*, United States v. Keith, 980 F. Supp. 2d 33, 36 (D. Mass. 2013). Agents may have downloaded files from the defendant's computer as part of a peer-to-peer sharing network. *See, e.g.*, Hamilton v. State, 387 P.3d 903, 905 (Okla. Crim. App. 2016).

198. No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

199. *Id.* at *2.

200. Law enforcement mirrored the defendant's hard drive pursuant to a warrant but could not open the mirrored drive without a password; its entirety was encrypted. *Id.*

201. *Id.*

202. *Id.* at *3–4.

203. *Id.*

204. *Id.* at *4.

This is the right result, but the court went too far when it required that he produce *all* the documents on his hard drive. After all, the government had not shown it knew the defendant possessed images beyond those identified.[205]

C. Logistics

In most cases, if law enforcement wins, the suspect must enter his password to the device and walk away.[206] Law enforcement agents gain access to and may search the entirety of the device. But under the rule proposed in this Article, a court may compel a suspect to enter his password in order to produce only those files the government already knows he possesses and can describe with reasonable particularity.

Several options present themselves to address how this would function in practice. First, we could treat this as an ordinary document production. Law enforcement will give the suspect the device under the supervision of counsel. Agents will supply a list of documents to produce, ones they know the defendant possesses and can describe with reasonable particularity. The suspect will enter his password to decrypt the device. The suspect will either print the documents or, more likely, burn copies to a flash drive and supply that flash drive to law enforcement. The defendant will then close the device and return it to law enforcement in its encrypted condition.

If law enforcement can show that the suspect cannot be trusted, even with counsel, to carry out this task, it could ask the court to appoint a special master to oversee the process. In cases in which the defendant continues to insist, for example, that the requested files are not on the drive, the special master could search the drive herself for the itemized files. This latter solution resembles protocol suggested by the Ninth Circuit for conducting electronic searches with Fourth Amendment limits in mind.[207]

D. Mistaken Application of the Foregone Conclusion Doctrine

Some courts have misapplied the foregone conclusion doctrine by asking whether it is a foregone conclusion that the suspect knows his own password.[208] Since this is nearly always true, such a misapplication would swallow the rule and allow the government to compel the entry of a password in any case in which law enforcement can show the defendant owns the

---

205. *Id.* at *1–2.

206. *See, e.g.*, *supra* note 19 and accompanying text.

207. *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1180 (9th Cir. 2010) (Kozinski, J., concurring) (suggesting that specialized or independent third parties should segregate and redact electronic data and only disclose information "which is the target of the warrant" to investigators).

208. *See* United States v. Apple MacPro Comput., 851 F.3d 238, 241 (3d Cir. 2017); United States v. Gavegnano, 305 F. App'x 954, 957–58 (4th Cir. 2009); United States v. Spencer, No. 17-CR-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018); State v. Stahl, 206 So.3d 124, 135–36 (Fla. Dist. Ct. App. 2016); *see also* Kerr & Schneier, *supra* note 27, at 1002 (noting the uncertainty among courts). *But see* Commonwealth v. Baust, 89 Va. Cir. 267 (Va. Cir. Ct. 2014) (critiquing this view).

device. At least one court has applied the doctrine to oral disclosures of passwords.[209]

It is a mistake to apply the foregone conclusion doctrine to the oral disclosure of a password. The Supreme Court has never hinted that the foregone conclusion test applies to oral testimony—it applies only to an *act*, namely, the act of producing documents.[210] The entire premise of *Fisher* says that the compelled production of documents does not initially violate the Fifth Amendment because the statements in those documents are preexisting and were created in a written form voluntarily.[211] Compelling a person to state her password does not compel production of existing documents but compels disclosure of what is in her mind.

But when we consider an order to compel a person to enter her password, can we apply the foregone conclusion doctrine to the password only and ask whether the government can show that it knows the defendant knows her own password? The Third Circuit and other courts hint that we can.[212] But this view also misconstrues the doctrine.

The foregone conclusion doctrine assesses whether the act of production communicates (new) facts to the government concerning the existence, possession, or authenticity of documents. We can only assess the facts communicated about these documents with reference to the content of the documents. True, the contents of the documents are not protected, but we need those contents to *identify* the documents. For the government to say a suspect possesses a certain bank statement, it must describe the bank statement with reasonable particularity to make clear it is that exact bank statement the suspect possesses and not another statement or document entirely. The government likely must name the bank, the account, and the month. Otherwise, it is not a foregone conclusion that *that* document exists, is possessed by the suspect, and is authentic.[213]

Applied to passwords, the facts communicated by entering the password are not simply that the person knows the password but also that the documents revealed by decryption exist,[214] are possessed by the defendant, and are authentic. In seeking to meet the foregone conclusion test, the government must reference the contents of the documents and not simply the password—that is, it must show it knows that the person possesses the documents. If the government cannot identify any documents on the device, the suspect's compelled act—entering the password—will communicate to

209. *Stahl*, 206 So.3d at 134. The court spoke of requiring the defendant to "provide" the password, though it also spoke of requiring him to "produce" it. *Id.* at 128. While not clear, the court appears to envision compelling the defendant to state the password and not simply to enter it.

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

211. *See supra* notes 57–60 and accompanying text.

212. *Apple MacPro Comput.*, 851 F.3d at 241; *Spencer*, 2018 WL 1964588, at *3; Commonwealth v. Gelfgatt, 11 N.E.3d 605, 615 (Mass. 2014).

213. *See* United States v. Greenfield, 831 F.3d 106, 121–22 (2d Cir. 2016).

214. If the password reveals that the device contains no documents at all, then the act of production will not even be incriminating and the Fifth Amendment will not apply for this separate reason.

the government the person's possession of the documents and their authenticity, facts the government did not know previously.

We may illustrate the mistake by remembering precisely how the analogy to the act of production works. The *act* of entering the password is analogous to the act of physically handing over documents in the physical world. In neither instance does the foregone conclusion doctrine apply solely to that act; rather, it applies to the papers produced. In the physical world, the court asks whether it is a foregone conclusion that the papers produced exist and are in the defendant's possession, *not* whether the defendant is physically capable of producing the documents.

In the password context, the password is not being produced. Indeed, our entire premise rests upon the fact that the password is never produced to anyone and we are treating entering the password as an act. Instead, the *act* of entering the password, like the act of physically handing over documents, produces the underlying documents on the device. We must therefore ask, in both cases, whether it is a foregone conclusion that those documents on the device exist.

Some courts insist that if we know the person possesses the device, it is a foregone conclusion that the person possesses the items on the device, whatever they turn out to be.[215] But the government must show *before* the production that the person possesses the particular documents because, otherwise, it is the very production that shows possession. To return to the physical world, the government could subpoena all the documents a person possesses in his home. Upon production, it would be a foregone conclusion that the suspect possessed any documents he happened to produce because they all came from his home. But a court would never apply the foregone conclusion doctrine in this manner because the government must establish, before and independent of production, that the defendant possesses particular documents.

Applying the foregone conclusion doctrine to the password also runs afoul of the very principle of *Fisher*. In *Fisher*, the Court refused to provide Fifth Amendment protection to the content of documents because they already exist; when the person created them at some earlier date, they did so voluntarily and not under government compulsion.[216] But the password is not a preexisting document in this scenario; rather, it resides solely in the suspect's mind. To treat the password as the thing produced would mean it is the testimony compelled and it would therefore enjoy full Fifth Amendment protection just like any other compelled oral statement.

E. Nonpossessory Crimes

In some cases, the government will not use any file recovered from the suspect's device at trial. Rather, it will use information recovered from the device to locate other evidence to use at trial. It might use the defendant's

215. *See, e.g.*, *Spencer*, 2018 WL 1964588, at *3.
216. *See* Fisher v. United States, 425 U.S. 391, 409 (1976).

bank statements, for example, to get the original checks that represent the actual income. In these cases, possession and authenticity play a far smaller role. The prosecutor will never need to show the defendant possessed this bank statement or authenticate it at trial.

Courts have ruled inconsistently in this area of the law. The Court in *United States v. Hubbell*[217] treated these as existence cases.[218] It found the production there sufficiently testimonial because the defendant had made "extensive use of the contents of his mind" in producing the documents.[219] But *Hubbell* did not say this test was a required showing, rather that it sufficed to show the production was testimonial.[220]

Indeed, several leading lower court decisions seem to have treated even existence cases as resting entirely on the foregone conclusion test, largely skipping any measure of whether the production was sufficiently testimonial because it made extensive use of the mind.[221] One such leading case is *United States v. Ponds*.[222] There, the government sought documents to use the information as leads and would not introduce the documents at trial. Possession and authenticity thus seem far less relevant. Nevertheless, the D.C. Circuit did not appear to require the defendant to show he made extensive use of the contents of his mind in responding to the subpoena.[223] Rather, it appeared to jump straight to the foregone conclusion test and held that the government had failed to show it knew of the documents in advance and could describe them with reasonable particularity.[224] The Second Circuit in *Greenfield* took a similar approach.[225]

If we apply these cases to passwords, we can come to one of two conclusions. If we require evidence that the defendant made extensive use of the contents of his mind, entering a password does not cross that threshold; we never reach the foregone conclusion test, and thus the government is permitted to compel the password. But if we follow many lower court decisions and jump straight to the foregone conclusion test—in other words, applying this Article's rule of particularity—the government *will* have to demonstrate it knows of the documents and can describe them. Only then will we allow compulsion. This Article chooses the second course and proposes requiring the rule of particularity even for existence cases, not based upon the act-of-production cases themselves, but rather the broader Fourth and Fifth Amendment principles discussed in Part V below.

217. 530 U.S. 27 (2000).
218. *Id.* at 42–44.
219. *Id.* at 43 (quoting Curcio v. United States, 354 U.S. 118, 128 (1957)).
220. *Id.* at 41.
221. *See id.*; United States v. Ponds, 454 F.3d 313, 318–20 (D.C. Cir. 2006).
222. 454 F.3d 313 (2006).
223. *Id.* at 324.
224. *Id.*
225. *See generally* United States v. Greenfield, 831 F.3d 106 (2d Cir. 2016).

F. Bitcoin and Other Cryptocurrency

These principles will apply to cases outside the realm of contraband images, including Bitcoin and other cryptocurrencies, but in novel ways. A person who owns or possesses Bitcoin controls it with a long, complex encryption key.[226] Often, they will not memorize the key itself but encrypt the key on a flash drive they can open with a shorter password or passphrase that they have memorized.[227] Or they will outsource the responsibility to hold onto the keys to an institution such as Coinbase and use a password to access their Coinbase account.[228]

Whether the government can compel a person to disclose the password that would lead to the longer Bitcoin key depends on why the government wants the information. If the person has already been convicted and the government seeks forfeiture of the Bitcoin as value, then it can likely compel the password because it will not be used as evidence at trial to convict. The "incrimination" part of the Fifth Amendment is missing. But if the government seeks the key to *link* the defendant to criminal proceeds at trial, then this case resembles the cases above. And as above, if law enforcement simply sought to compel the suspect to orally (or in writing) disclose the password that would allow them access to the underlying encryption key for the Bitcoin, this compulsion would violate the Fifth Amendment directly.

Even if law enforcement officers compel a person merely to enter her password into a Bitcoin wallet, unlocking, in turn, the longer Bitcoin key, the government might fail our rule of particularity. After all, the government seeks to *link* the defendant to the Bitcoin value, but it can only do so if the defendant enters her password and it does, in fact, unlock a key associated with that particular Bitcoin. This presents precisely the authentication problem raised above with possession-crime cases: the government will never be able to link the defendant to the Bitcoin without providing the jury with evidence of the *fact* that the defendant entered his wallet password, and the foregone conclusion doctrine forbids this.

G. Objections or Other Views

Prosecutors may object that the rule proposed in this Article will prevent them from charging the appropriate offenses based on the defendant's entire conduct or that sentencing judges will lack all the information concerning the defendant. For example, in a case involving child pornography, the United States Sentencing Guidelines add points for the number of images.[229] If we limit the government to obtaining only those images it already knows the

226. *See* ANTONOPOULOS, *supra* note 35, at 63.

227. *See id.* at 235; *Where Can I Find the Private Keys for My Wallet?*, COINBASE, https://support.coinbase.com/customer/portal/articles/1526452-where-can-i-find-the-private-keys-for-my-wallet- [https://perma.cc/8UG6-FUAG] (last visited Aug. 24, 2018) (describing the option to encrypt keys on a flash drive).

228. ANTONOPOULOS, *supra* note 35, at 9.

229. U.S. SENTENCING GUIDELINES MANUAL § 2G2.2(b)(7) (U.S. SENTENCING COMM'N 2016).

defendant possesses, we may undercount by hundreds or thousands of images and put the defendant in a sentencing range two, three, four, or five points too low. Sentences in fraud cases similarly hinge on the loss; if the government cannot obtain all documents, it may fail to account for the entirety of the loss the defendant caused.

This objection has great merit. We cannot catch every criminal. For those we do catch, however, there is a sense that we should charge and sentence them according to their actual culpability.[230] On the other hand, particularly in federal cases, the fact of a conviction for possession of child pornography or fraud will often adequately condemn the defendant. In addition, the difference in sentences will not actually amount to a significant difference, and judges have the discretion to depart from the sentencing guidelines.[231]

More importantly, 97 percent of federal cases reach resolution through a plea.[232] As part of a plea, the government can certainly insist that the defendant waive his Fifth Amendment protection to his device, just as he must waive his Fifth Amendment right to enter the guilty plea itself. As a practical matter, the government will retain significant leverage to obtain the contents of the device once it has secured at least one image.

Finally, Fifth Amendment protections always bring costs, not only in whether the government can convict a person at all, but which counts it can bring and how heavy a sentence it can exact. Existing act-of-production doctrine cases impose this same rule in all criminal cases involving subpoenas of a suspect or defendant for her documents, and we tolerate this limit in those cases well enough.

One important subset of criminal investigations involves emergencies. A suspect may have left a kidnapped victim alive somewhere, and law enforcement will want to compel the person to disclose that location so they can go save her. Or, in the context of smartphones, an iPhone may contain the secret code to disarm a nuclear bomb about to detonate in a major city. Surely, one would argue, agents or courts can compel a suspect to enter her password to the device and allow law enforcement further access to disarm the bomb.

Of course, the answer is yes. A court can immunize the suspect and compel her to decrypt the drive containing the secret code, and thereby disarm the bomb and save the world.[233] Or law enforcement itself can use

230. *See* Richard S. Frase, *Punishment Purposes*, 58 STAN. L. REV. 67, 73 (2005) (describing the role of culpability in nonutilitarian sentencing principles).

231. *See* Peugh v. United States, 569 U.S. 530, 536–37 (2013). Indeed, judges may not even presume the guidelines range is reasonable and may depart if they disagree with the Sentencing Commission's view, as long as they state their "basis for [the] chosen sentence on the record." *Id.*

232. U.S. SENTENCING COMM'N, OVERVIEW OF FEDERAL CRIMINAL CASES, FISCAL YEAR 2017, at 5 (2018), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2018/FY17_Overview_Federal_Criminal_Cases.pdf [https://perma.cc/36UG-E7PY].

233. *See* United States v. Balsys, 524 U.S. 666, 682 (1998) ("[T]he government has an option to exchange the stated privilege for an immunity to prosecutorial use of any compelled inculpatory testimony.").

any lawful means of compulsion. But the government cannot then use that evidence against the suspect in a subsequent criminal trial.[234] In other words, the Fifth Amendment presents no obstacle to otherwise lawful compulsion in the face of an emergency *to stop the emergency*. But once the emergency has been averted, we can no longer point to the emergency as a justification to compel a person to testify against herself at trial. Just as in any other case, serious or minor, the Fifth Amendment protects such defendants and mandates that, at trial, such evidence is off limits.

Another objection arises when we compare entering a passcode with opening a phone with a thumbprint or facial recognition. Many phones open with a thumbprint or facial recognition.[235] These technologies present a further challenge. Courts have held that thumbprints enjoy no Fifth Amendment protection because they are essentially seizures: law enforcement can obtain a warrant and physically force a person's thumb onto the device.[236]

These courts are right. Compelling a thumbprint closely resembles the physical characteristic cases such as *Holt* and may therefore be resolved in the government's favor on this basis.[237] In addition, unlike entering a password, placing a thumb on a device involves no statement or language-like cognition at all, not even as much as remembering and entering a passcode or password.[238] But the objection asks why should the result differ so much between compelling a password versus compelling a thumbprint. The answer may not be entirely satisfying, but it depends upon how the case law ends up dividing between the Fourth and Fifth Amendments, between the taking of evidence versus requiring the suspect to produce it.

One final practical objection might run as follows: many investigations into businesses, whether criminal or civil, depend upon electronic documents that will likely be stored on locked, encrypted devices. Investigations into tax fraud, stock fraud, pollution, and many regulatory offenses involve

234. *See id.*

235. For example, Apple and Samsung phones can open with thumbprint or facial recognition. *See About Face ID Advanced Technology*, APPLE, https://support.apple.com/en-us/HT208108 [https://perma.cc/E32Y-VZQZ] (last visited Aug. 24, 2018); *About Touch ID Advanced Security Technology*, APPLE, https://support.apple.com/en-us/HT204587 [https://perma.cc/NB98-5Y7Z] (last visited Aug. 24, 2018); *How Can I Use the Fingerprint Scanner?*, SAMSUNG, https://www.samsung.com/global/galaxy/what-is/fingerprint-scanner/ [https://perma.cc/27QE-B2RQ] (last visited Aug. 24, 2018).

236. *See* Commonwealth v. Baust, 89 Va. Cir. 267 (Va. Cir. Ct. 2014).

237. *See* State v. Diamond, 905 N.W.2d 870, 874–76 (Minn. 2018) (relying on "physical characteristic" cases); *see also supra* note 163 and accompanying text.

238. A reader may complain that compelling a defendant to enter a password and compelling a thumbprint lead to the same result and should not have such different legal tests. Entering a password, an act done reflexively, resembles opening a device with a thumbprint. We may first say that this problem arises in part because current Fourth Amendment protections are wanting. We should enhance them even for those who do not use a passcode. Precisely how to enhance them goes beyond the scope of this Article, but courts should move to a more robust conception of particularity and at least consider my enhanced version limiting agents to those documents it already knows the individual possesses.

millions of documents. The simple approach is that the Fifth Amendment does not protect business entities at all.[239] The harder question will arise when the individual who possesses the password claims a personal privilege even in producing the password (which will show she has access to and knowledge of at least some of the documents). This problem arises already in many corporate contexts,[240] though encryption may magnify them. However, most businesses will give many key employees the password, and often nonbusiness IT personnel may enjoy access that will not be incriminating.

V. A PRACTICAL SETTLEMENT: HARMONIZING THE FOURTH AND FIFTH AMENDMENTS

This Part steps back to show how a more theoretical view of both the Fourth and Fifth Amendments lends support to this rule of particularity, especially in this hybrid situation where encrypted devices necessarily bring the two amendments into play.

A. Fifth Amendment Theory

Scholars have struggled to identify a single principle or collection of principles that explain current doctrine or even the value of the Fifth Amendment itself.[241] David Dolinko has comprehensively compassed the various proposed justifications for the Fifth Amendment, dividing them roughly into (1) those that draw upon the rights of the individual to dignity or privacy, and (2) those that focus on promoting the adversarial system.[242] Taken in isolation, each justification falls short. For example, the Supreme Court once insisted that the Fifth Amendment protects privacy,[243] but this is not quite true because the government can always provide a suspect or witness with immunity and compel disclosure of the same information, no matter how private.[244]

On the other hand, Professor Dolinko concedes that the Fifth Amendment plays an important role in our existing criminal justice system since so much of that system has grown up around its protections.[245] We can remove the right against self-incrimination no more safely than a Jenga plank from its

239. *See* Braswell v. United States, 487 U.S. 99, 104 (1988).

240. *See* Robert P. Mosteller, *Simplifying Subpoena Law: Taking the Fifth Amendment Seriously*, 73 VA. L. REV. 1, 58 (1987).

241. *See, e.g.*, Allen & Mace, *supra* note 141, at 293 (expressly avoiding normative views of the Fifth Amendment as hopeless and simply describing the case law instead); David Dolinko, *Is There a Rationale for the Privilege Against Self-Incrimination?*, 33 UCLA L. REV. 1063, 1064 (1985). *See generally* John Fabian Witt, *Making the Fifth: The Constitutionalization of American Self-Incrimination Doctrine, 1791–1903*, 77 TEX. L. REV. 825 (1999) (noting the shifting rationales for the Fifth Amendment throughout history).

242. Dolinko, *supra* note 241, at 1065.

243. *See* Boyd v. United States, 116 U.S. 616, 630 (1886).

244. Witt, *supra* note 241, at 844 n.60, 900 (detailing why *Boyd* moved to a privacy rationale but noting why it makes little sense).

245. Dolinko, *supra* note 241, at 1064.

precarious tower. Similarly, Dolinko has shown how the Fifth Amendment sometimes takes up the slack when other protections fail. He points to the McCarthy-era hearings in which those subpoenaed pleaded the Fifth Amendment to protect values largely falling under the First Amendment.[246] Courts had rejected a First Amendment defense, leaving the Fifth Amendment to fill in the void.[247]

Similarly, in this context, the Fifth Amendment may not protect privacy directly. Nevertheless, in our hybrid situation of encrypted devices where the Fifth Amendment already applies to some extent along with the Fourth Amendment, we may view the Fifth Amendment as protecting the privacy of papers that current Fourth Amendment case law has wrongly failed to protect.[248] Or, put another way, we can simply say that the Fifth Amendment protection for passwords furthers Fourth Amendment goals of privacy.

The second justification that Dolinko identifies, and critiques, is that the Fifth Amendment enhances an adversarial as opposed to an inquisitorial method of criminal investigation.[249] The Court regularly notes that the government must "shoulder the entire load" in its "contest with the individual."[250] It may not take shortcuts by compelling confessions, but rather it must build the case entirely on its own. Despite criticism, both courts and scholars regularly rely upon an adversarial model to some extent in interpreting the Fifth Amendment.[251] Indeed, hundreds of courts[252] have quoted approvingly the Supreme Court's premise that the government must "shoulder the entire load"—including several state supreme courts just in the last two years.[253] And while the Supreme Court has limited the personal-dignity rationale for the Fifth Amendment, it has pointed to "preventing government overreach[]" as a central principle.[254] On "anyone's view," according to the Court, this principle against government overreach "lies at the core of the Clause's purposes."[255] Those who critique the notion that the Fifth Amendment requires the government to "shoulder the entire load" have a point, but those critics reject any adversarial principle simply because the

246. *Id.* at 1064, 1089 n.140.

247. *Id.* at 1064 n.9.

248. *See supra* notes 70–80 and accompanying text.

249. *See* Dolinko, *supra* note 241, at 1076–77; *see also* Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964) (holding that the Fifth Amendment shows "our preference for an accusatorial rather than an inquisitorial system of criminal justice").

250. *See* United States v. Balsys, 524 U.S. 666, 690 (1998) (quoting *Murphy*, 378 U.S. at 55); *see also* Miranda v. Arizona, 384 U.S. 436, 475 (1966).

251. *See, e.g.*, Stephanos Bibas, *The Rehnquist Court's Fifth Amendment Incrementalism*, 74 GEO. WASH. L. REV. 1078, 1080 (2006); Heidt, *supra* note 5, at 490; *see also infra* notes 252–55 and accompanying text.

252. A Westlaw search of case law conducted in July 2018 on "shoulder the entire load" revealed 187 hits. A large sample of these hits shows the quote appears as a favorable policy behind the Fifth Amendment, sometimes as a mere platitude, but often referred to as part of the decision. *See, e.g.*, Hudec v. Superior Court, 339 P.3d 998, 1007 (Cal. 2015).

253. *See, e.g.*, *id.* at 998; State v. Diamond, 905 N.W.2d 870, 873 (Minn. 2018); Barrera v. State, 403 P.3d 1025, 1032 (Wyo. 2017) (Kautz, J., dissenting).

254. *See Balsys*, 524 U.S. at 693.

255. *Id.*

most extreme version—"the *entire* load"—makes little sense.[256] In other words, we may safely posit that the Fifth Amendment furthers the adversarial nature of our system—the question is, to what extent?

In identifying the appropriate level of protection the Fifth Amendment affords in promoting an adversarial system, we can start with a hypothetical range. At one extreme, the Fifth Amendment prohibits the government from enlisting *any* assistance whatsoever from the defendant, which would include a prohibition on compelled entering of a password, of course. At the other extreme, the government can compel any assistance that does not involve literal oral or written testimony. This view would allow the government to compel the act of entering a password since that act likely does not involve literal oral or written testimony.

The chief proponent of the no-assistance camp is Professor Nagareda. His originalist work shows that the framers intended the Fifth Amendment to prohibit the government from compelling a defendant to "furnish" evidence against himself; that is what they meant by "witness."[257] In his view, *Fisher* is simply wrong.[258] When the government subpoenas documents, it compels the defendant to assist the prosecution by furnishing evidence against himself, and this conduct violates the language, "to be a witness against himself."[259] But Nagareda notes that the Fourth Amendment always permits, as a backup, the government's power to merely *seize* any evidence, including documents.[260] In his view, the Fifth Amendment draws a line not at testimony but at compelled assistance. The government may take evidence with a warrant, but not compel the defendant to furnish it.

At the other end of the spectrum, we might simply say the Fifth Amendment protects "testimony" only. That is, testimony in its straightforward core meaning: communication through speech. A "witness," after all, recounts what she observed through language. The text supports this view, of course. The Court implicitly supported this view in *Fisher* by rejecting, at least initially, protection for a person compelled to produce documents.[261] The Fifth Amendment, under this second account, would not prohibit any other type of compelled assistance and would not, therefore, enforce the adversary system beyond this one tactic.

We can reject both extremes, for different reasons, before arriving at our middle path. As for Nagareda's argument, the first answer is that the Fifth Amendment does not say "furnish evidence"; rather, it says, "be a

256. *See* Dolinko, *supra* note 241, at 1084.
257. Nagareda, *supra* note 5, at 1606.
258. *Id.* at 1578.
259. *Id.* at 1610–11.
260. Nagareda relies upon contemporary doctrine, but at the founding, practice likely forbade the authorities from seizing papers for use in a criminal case. *See, e.g.*, Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 568 (2016). Nagareda thus seems to rely upon originalism for the Fifth Amendment but contemporary doctrine for the Fourth.
261. *See* Fisher v. United States, 425 U.S. 391, 410 (1976).

witness."[262] This is the main reason *Fisher* rejected Fifth Amendment protections for preexisting documents.[263] Plus, even Nagareda concedes the Fifth Amendment allows the government to compel the defendant's assistance in many ways, including exhibiting physical characteristics.[264]

Finally, we may reject Nagareda's view in our particular, hybrid situation of encrypted devices. Nagareda's view depends in part on the premise that the government always enjoys, as a backup to compelling assistance from the defendant, the power, with a warrant, to unilaterally seize evidence. But encrypted devices defeat this backup method: if law enforcement cannot access the device, it cannot obtain even those documents it can identify with a warrant.

We can also reject the other extreme—that the Fifth Amendment protects only testimony that resembles speech, such as oral statements, or compelled written statements. We must do so because *Fisher* and *Hubbell* have extended testimony and "witness" beyond these core examples with the act-of-production doctrine.[265] This doctrine recognizes the act of producing documents, or the act of entering a password, as testimony even though the person performing the act does not communicate through language. Indeed, the person producing the documents does not intend the act to be communicative at all.

In between these theories, this Article's rule of particularity allows some compelled assistance, such as decrypting those files the government can identify, but no more. If our test is simply a "fair" adversarial system, we might say this balance strikes many of us as fair. The government gets access to the documents it can identify in advance, but no more. Suspects must assist in some small measure in their own prosecution but only by producing documents that the government has identified. This assistance—surrendering documents the government has identified—resembles disclosing a physical characteristic, such as allowing a blood draw in a drunk driving case or producing a voice or handwriting exemplar, more than it does ordinary testimony.

This rule also furthers a more concrete principle underlying the adversarial model: antifishing. This principle draws upon both the Fourth and Fifth Amendments. Therefore, it shows that they need not stand marshalled as opposing forces: the Fourth grants the government what the Fifth denies. Instead, this antifishing principle harmonizes and unites the Fourth and Fifth Amendments around this Article's rule of particularity that law enforcement obtains only those documents it can identify with particularity in advance.

---

262. U.S. CONST. amend. V.

263. *Fisher*, 425 U.S. at 396–97.

264. *See* Nagareda, *supra* note 5, at 1627–28; *supra* notes 163–66 and accompanying text. In *Holt*, for example, the court compelled the defendant to put on the shirt the thief wore to see if it fit. *Holt v. United States*, 218 U.S. 245, 252–53 (1910). In this core example, the defendant assists the prosecution but not by communicating through language. The voice and handwriting exemplar cases challenge the proposed rule, but, even here, the defendant displays how he writes, not what he writes.

265. *See supra* Part I.C.

Two related scenarios can describe the concept of a fishing expedition. In the first, the government has no probable cause or suspicion to believe a given person has committed any crime; nevertheless, law enforcement agents attempt to gather evidence from the suspect in an effort to find one. The court in *Hubbell* viewed the special prosecutor's investigation in this light and dubbed it the "quintessential fishing expedition."[266] In the second scenario, the government has probable cause for one crime but demands from the suspect papers and other evidence to look for other, unrelated crimes.

This value against fishing expeditions captures both some notion of prior suspicion, such as probable cause, to justify the defendant's assistance and some notion as to scope regarding that assistance. The rule of particularity for passwords limiting agents to those documents it can identify answers both concerns.

The Fifth Amendment protects this antifishing principle chiefly in white collar criminal investigations involving large numbers of documents, often personal financial papers. Most recently in *Hubbell*, the court found that the government's subpoena violated the Fifth Amendment because it demanded that the defendant review his financial records and other papers for those responsive to several broad subpoena categories.[267] This process of reviewing, separating, organizing, and producing required the defendant use (and in some sense reveal) the contents of his mind in ways that amounted to Fifth Amendment testimony.[268]

But with this account of *Hubbell*, a new problem arises: any subpoena requires the defendant to use his mind in finding, organizing, and producing responsive documents. Yet *Hubbell* does not invalidate all subpoenas or overrule *Fisher*. We must therefore discern that the *Hubbell* subpoena crossed the line into compelled testimony due to its scope: the degree to which it enlisted the defendant's assistance. In other words, the subpoena went beyond mere surrender of documents because it was the "quintessential fishing expedition."[269]

Indeed, the Supreme Court has had several occasions to find in the Fifth Amendment a general principle against fishing expeditions.[270] Older

266. *See* United States v. Hubbell, 530 U.S. 27, 32 (2000) (quoting United States v. Hubbell, 11 F. Supp. 2d 25, 33–37 (D.D.C. 1998)).

267. *Id.* at 45.

268. *Id.* at 43.

269. *Id.* at 32.

270. *Id.* at 32, 34 n.8 (finding a Fifth Amendment violation, describing it as "the quintessential fishing expedition," and noting that the roots of the Fifth Amendment lie, in part, to prevent wide exploration to "uncover uncharged offenses, without evidence from another source"); Griffin v. California, 380 U.S. 609, 620 (1965) (Stewart, J., dissenting) ("When a suspect was brought before the Court of High Commission or the Star Chamber, he was commanded to answer whatever was asked of him, and subjected to a far reaching and deeply probing inquiry in an effort to ferret out some unknown and frequently unsuspected crime."). Some scholars have deemphasized this early English history in their accounts of the Fifth Amendment. *See generally* JOHN H. LANGBEIN, THE ORIGINS OF THE ADVERSARY CRIMINAL TRIAL (2003). Others have rejected the antifishing expedition principle based upon other considerations. *See generally* Akhil Reed Amar & Renee B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857 (1995).

precedents such as *Boyd* draw a closer connection between papers and self-incrimination in ways that echo this principle against government rummaging through papers in search of evidence of a crime.[271]

The Fourth Amendment also protects against fishing expeditions[272] far more explicitly than the Fifth. It guards against unreasonable searches and general warrants, two requirements that arose in part out of English precedents disapproving broad searches and seizures of a person's personal papers for use in a criminal case.[273] One influential English pamphlet excoriating such searches and seizures of papers used the term "fishing" to describe the potential government practice of scouring a person's papers to discover new crimes and linked this protection to the right against self-incrimination.[274] Some scholars point to this and other English pamphlets of the 1760s and 1770s as influencing the adoption of the search and seizure provisions of the early state constitutions, as well as that of the Fourth Amendment.[275]

Disapproval of fishing expeditions during the founding era appears to have extended to civil cases, where courts sometimes rejected any paper discovery if not supported by some independent facts justifying the discovery. One New York court in 1800 referred to such a bill as a "mere *fishing bill*" and cited authorities from England that suggest the term had already become commonplace.[276] Courts in the United States in the late nineteenth century continued to use the term "fishing expedition" to describe civil discovery practices that also required the opposing party to produce all their books and records.[277] At the time, the rule limited a party to discovery of only a narrow class of documents that they could identify and demonstrate were material. Although in civil contexts, courts pointed to the preference for adversarial rather than inquisitorial methods in limiting paper discovery.[278]

---

271. *See* Boyd v. United States, 116 U.S. 616, 633–34 (1886). *Boyd* itself relied heavily upon the English *Entick* case from a century before, which rejected the seizure and search of papers in a criminal case based in part upon the common-law prohibition against compelling a man to accuse himself. *See id.* at 626; Schnapper, *supra* note 21, at 873–74.

272. *See* United States v. Uzenski, 434 F.3d 690, 706 (4th Cir. 2006) (stating that fishing expeditions violate the particularity requirement of the Fourth Amendment); United States v. Foster, 100 F.3d 846, 852 (10th Cir. 1996) (noting that a "fishing expedition" for additional crimes violates the purpose of the Fourth Amendment's particularity requirement); Michelle Segal, *The Inadvertency Requirement and the Warrant Clause*, 63 U. COLO. L. REV. 989, 1003 n.94 (1992) (noting that the particularity requirement limits "the wide-ranging exploratory searches the Framers intended to prohibit").

273. *See* Entick v. Carrington (1765) 19 Howell's State Trials 1029, 1038–39; *see also supra* notes 40–46 and accompanying text.

274. Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 70–71 (2013).

275. *Id.*

276. *See* Newkerk v. Willett, 2 Cai. Cas. 296, 300 (N.Y. 1800).

277. *See Ex parte* Clarke, 58 P. 546, 548–49 (Cal. 1899) (rejecting a discovery bill as "a general fishing expedition").

278. The courts have greatly liberalized the civil discovery rules concerning production of documents, but even these still require production only of relevant documents. *See* FED. R. CIV. P. 26(b), 34.

The Fourth Amendment concern with broad paper searches and seizures rests upon values beyond fishing expeditions for new crimes; it relies as well on protecting privacy and security. Both the reasonableness clause and the warrant clause protect privacy by limiting searches and seizures to only those items that can be listed with particularity in the warrant.[279] This requirement will prevent officers from seizing or searching many unrelated items and therefore protect privacy. In the context of papers, this means it should prevent officers and other government officials from reading papers unrelated to the investigation that might contain personal or private information, such as letters, diaries, and family photos. A rule for encrypted devices that requires agents to list in advance with reasonable particularity the documents or files that they already know the defendant possesses will certainly further this goal better than current Fourth Amendment case law.[280]

The proposed rule of particularity also furthers the Fourth Amendment goal of security. That is, it furthers a type of Fourth Amendment security beyond mere privacy-as-secrecy from prying government eyes. It will assure a suspect that law enforcement limits its search to documents relevant to the crime by limiting it to those documents. The suspect will not have to worry that law enforcement will, having gained access to the device, scour its entirety looking at unrelated photos and videos, even if only out of curiosity. Instead, the suspect will *know* precisely which files the government has access to. It will similarly provide the suspect with an accounting of the files accessed. This will both give the suspect control and help make the people "secure in their . . . papers."[281]

Some scholars, recognizing the need for balance in the adversarial system under the Fifth Amendment, have argued for a different result from my proposal. Dan Terzian, for example, has argued that allowing any Fifth Amendment protection for a password in the face of a warrant would impose too high a burden to law enforcement, contending that the Fifth Amendment must yield.[282] But his argument seems to rely upon an all-or-nothing approach: either the person decrypts the entire device or none of it. If those are the only two options, one understands why law enforcement should obtain access. But my rule sidesteps the all-or-nothing approach, allowing law enforcement access to only those files it can identify with reasonable particularity. That represents a true balance of interests.

B. Fourth Amendment Theory

Law enforcement agents often reject any balance between the Fourth and Fifth Amendment and claim that they are entitled to everything. In their view, the Fourth Amendment already contains the relevant balance between privacy and disclosure: a warrant based upon probable cause.[283] If the

279. *See* Berger v. New York, 388 U.S. 41, 56 (1967).
280. *See supra* Part I.A.
281. U.S. CONST. amend. IV.
282. Terzian, *supra* note 8, at 309–10.
283. *See* N.Y. CTY. DIST. ATTORNEY'S OFFICE, *supra* note 11, at 1.

government has successfully seized the media pursuant to such a warrant, affording it the right to search that media, then it is entitled to those documents. Compelling a person to enter a password follows as an adjunct to executing the warrant.[284]

In response to this maximalist position, we may first point out that the Fifth Amendment enjoys equal constitutional status and, at the very least, must be taken into account. The government often enjoys the legal right or power to search a place or item that it cannot locate because of the Fifth Amendment. For example, the police cannot compel a suspect to disclose the location of a body so that the government may search for it, or seize it, even if the government has obtained a warrant to search for or seize the body.[285] It also cannot compel a person to disclose the location of bank accounts,[286] safes, or other containers even if the government otherwise has probable cause and a warrant to search them. A warrant cannot change physics; a warrant that provides a legal right cannot provide a physical *ability* to access that evidence.[287]

But the government's argument runs into a far more serious objection. As originally understood, the Fourth Amendment likely banned *any* search and seizure of personal papers in a criminal case.[288] This principle rested in part on the notion that agents *could*, in theory, seize particular incriminating documents, but they *could not* look through innocent documents to find them.[289] If the Fourth Amendment banned paper searches in criminal cases, then the government could not seize a person's electronic device at all, much less compel a person to open it. Although the Fourth Amendment no longer entirely bans such searches and seizures, law enforcement still cannot point to the Fourth Amendment to show that it supplies the relevant balance for

284. *See* Brief for Appellee at 22, United States v. Apple MacPro Comput., 851 F.3d 238 (3d Cir. 2017) (arguing that the defendant had not been required to disclose his password but to merely decrypt the device and that a court may issue an All Writs Act order requiring a defendant to decrypt a hard drive "to facilitate the execution of search warrants").

285. *See, e.g.*, Satter v. Solem, 434 N.W.2d 725, 725–27 (S.D. 1989) (holding that the sheriff violated the Fifth Amendment by asking the suspect where the body was without providing *Miranda* warnings).

286. *See, e.g.*, Doe v. United States, 487 U.S. 201, 215 (1988) (stating that the consent directive was not testimonial because it did not require the defendant to identify banks at which he held accounts and noting that the government must "locate that evidence" by its own efforts).

287. When the government says it already *has* the documents, and it merely needs to decode them, it uses a misleading analogy. With encryption, the underlying files cease to retain any meaningful existence—the software scrambles everything on the storage drive into a jumble of bits that are effectively indistinguishable from random bits. *See supra* Part II.B. Indeed, a forensic expert cannot tell whether an encrypted disk originally contained any data or was blank; both states encrypt to an equally indiscernible random scramble. *See, e.g.*, *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1340 (11th Cir. 2012).

288. *See* Donohue, *supra* note 40, at 1309–10; Dripps, *supra* note 274, at 50; Schnapper, *supra* note 21, at 869–70.

289. *See* Schnapper, *supra* note 21, at 875 ("[T]he search and seizure clause forbids the inspection of innocent private papers in the course of a search for inculpatory documents that by themselves are unprotected by the fourth amendment.").

encrypted devices because the Court has never answered that question, and the framers would have disallowed any such seizure and search. As Laura Donohue put it:

> This point is worth emphasizing in the contemporary environment, not least because the Director of the Federal Bureau of Investigation, in the context of the encryption debate, has taken to repeating a falsehood: that, with the appropriate process, the government has always had access to what people think, say, and write. It has not. For nearly two hundred years, the government could *not* obtain private papers—even with a warrant—when they were to be used as evidence of criminal activity.[290]

Of course, we have long departed from the view that papers are absolutely protected, whether under the Fourth or Fifth Amendment. The entire regulatory state would collapse without the government power to review papers,[291] as would most white-collar criminal prosecutions. But, even once we acknowledge the right of the government to seize and search papers pursuant to a warrant, we can impose limits consistent with the original prohibition and the modern view of the particularity requirement of the warrant clause, now made relevant to papers.

If the reasonableness clause prohibited the seizure of papers in part because agents cannot look through innocent papers to find the incriminating ones,[292] this rule of particularity answers this precise objection. The government may compel an individual to decrypt only those documents it can already identify, and it will not see any innocent documents.

CONCLUSION

Passwords, passcodes, and passphrases have increasingly become the personal key to our entire digital and online lives. It may seem a little thing, a four- or six-digit passcode, but this slender thread unlocks the entirety of a person's life—it is the corpus callosum between our minds and our vast repositories of personal information. This Article argues that passwords must therefore enjoy at least some robust Fifth Amendment protections—but how much? When can law enforcement, armed with a warrant, compel a person to enter her password and unlock her device, decrypt her files, and make accessible her entire digital life?

In answering this question, this Article notes a seldom-considered development: encrypted devices seized by law enforcement with a search warrant present a hybrid case that brings into play both the Fourth and Fifth Amendments. While the last 150 years have seen the Supreme Court striving to separate these two amendments into discrete territories, the encrypted device forces us to reunite them. With this overlap, we can either set them against each other or try to harmonize them. This Article tries to harmonize them and draw upon their common values to create a middle ground.

---

290. Donohue, *supra* note 260, at 568.

291. *See* William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1059 (1995).

292. *See* Schnapper, *supra* note 21, at 918.

In particular, this Article proposes a rule of particularity: when law enforcement agents have a warrant to search a locked, encrypted device, they can compel the suspect to enter her password to decrypt only those files that agents (1) know she possesses, and (2) can describe with reasonable particularity. This rule follows from a careful and technical consideration of the Supreme Court's act-of-production doctrine and its foregone conclusion test. This rule of particularity shows how lower courts have gone astray in applying this rule to passwords: even if agents have succeeded in identifying some files or documents, that does not entitle them to have the entire device unlocked for their perusal.

This rule of particularity answers the bigger, theoretical question of how we can harmonize the Fourth and Fifth Amendments. First, it considers deficiencies in current lower court Fourth Amendment case law that permit agents, armed with a warrant, to search every file, every folder, and every deleted document, with the most sophisticated forensic software. At least when a person has a passcode, the new rule limits them to those specific documents, if any, that gave rise to probable cause in the first place. Second, my rule of particularity furthers a key goal of both amendments: a principle against government fishing expeditions in which agents conduct vast, exploratory searches for unsuspected, new crimes against suspects or even nonsuspects.

As encryption spreads to all digital information, whether communications over the internet or data at rest on our devices, passwords will play an increasingly critical role in protecting our data, but it will also present an increasing obstacle to legitimate law enforcement needs. End-to-end encryption of communications, including emails and messages as well as internet browsing, means law enforcement will have to obtain data not from providers in transit but from individuals from their devices, cloud backups, or online accounts. Data in flight will become data at rest. This rule balances these concerns in ways that should help us navigate these impending battles.