Locked Out or Locked Up: The Need for New Guidelines for Compelled Decryption

Adriana Christianson*

"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."[1]

I. INTRODUCTION

The Founders of the United States were deeply concerned with government overreach into the private lives and property of citizens.[2] Witness to troubling evidence-gathering practices, the Founding Fathers conceived two strong protections against such overreach: the prohibition against unreasonable search and seizure in the Fourth Amendment, and the prohibition against self-incrimination in the Fifth Amendment.[3] Both amendments have been the subject of much litigation as courts struggle to define the boundaries of the amendments' limits on government action and keep pace with ever-changing technology and perceptions of privacy.[4]

The explosion of personal technology in the twenty-first century has highlighted the relationship between the two amendments as modern society

* J.D. Candidate, Suffolk University Law School, 2022; B.S. 2005, University of Massachusetts, Amherst. A big thank you to Professor René Reyes for his guidance, the all-star *Suffolk University Law Review* team for their countless improvements, and my eternally supportive family, especially Phil, Nora, and Calvin, for allowing me the space to think and the time to write.

1. Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 251 (2018).

2. *See* Boyd v. United States, 116 U.S. 616, 625-27 (1886) (claiming every statesman during America's formation considered Lord Camden's opinion on reasonable search); Riley v. California, 573 U.S. 373, 403 (2014) (noting British officers' unrestrained rummaging for evidence one cause of American Revolution).

3. *See* U.S. CONST. amends. IV–V; *Riley*, 573 U.S. at 403 (recognizing Fourth Amendment's original purpose to prevent unrestrained searches); *see also* Richard A. Nagareda, *Compulsion "to Be a Witness" and the Resurrection of* Boyd, 74 N.Y.U. L. REV. 1575, 1576 (1999) (describing common scenarios of governments abusing suspects and defendants).

4. *See* MICHAEL A. FOSTER, CONG. RSCH. SERV., LSB10416, CATCH ME IF YOU SCAN: CONSTITUTIONALITY OF COMPELLED DECRYPTION DIVIDES THE COURTS 1 (2020), https://www.everycrsreport.com/files/2020-03-06_LSB10416_2a8b1e8e28f39dfbd6d5e3dfe7870b10b7792c22.pdf [https://perma.cc/9PDS-2PHT] (noting many cases focus on permissible device searches under Fourth Amendment); David Rassoul Rangaviz, *Compelled Decryption & State Constitutional Protection Against Self-Incrimination*, 57 AM. CRIM. L. REV. 157, 157 (2020) (recognizing challenges involving scope of Fifth Amendment protection relating to self-incrimination challenges).

migrates intimate information onto digital devices.[5] Cell phones and computers have become ubiquitous, with over 97% of the U.S. population owning a cell phone and 77% owning a desktop or laptop computer.[6] Police are frequently interested in searching digital devices for evidence of wrongdoing because of their popularity and the private nature of their contents, but must do so without violating either amendment.[7]

The physical size of these devices belies the vast amounts of information contained within, and guidelines defining a reasonable search do not always apply to devices' contents.[8] Often listed as one item on a warrant, a device may hold terabytes of information in the form of videos, pictures, applications, activity logs, emails, messages, calendars, search history, and location data.[9] Although citizens have fought countless court battles over how readily and expansively law enforcement may search individuals' private spaces—and even public spaces where people reasonably expect privacy—expansive searches of digital devices are now the norm.[10] Courts have recently begun to recognize that

5. *See* Sacharoff, *supra* note 1, at 206 (claiming encryption challenges ability to separate Fourth and Fifth Amendments); Commonwealth v. Hughes, 404 N.E.2d 1239, 1241 (Mass. 1980) (noting subtle interaction between Fourth and Fifth Amendments where government seeks to compel incriminating statement); William Clark, Note, *Protecting the Privacies of Digital Life:* Riley v. California*, the Fourth Amendment's Particularity Requirement, and Search Protocols for Cell Phone Search Warrants*, 56 B.C. L. REV. 1981, 1981 (2015) (highlighting rising popularity of smartphone use for managing personal and sensitive data).

6. *See Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/46TE-83QW] (noting Americans increasingly connected to digital information while away from home).

7. *See* SEAN E. GOODISON ET AL., RAND CORP., DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM: IDENTIFYING TECHNOLOGY AND OTHER NEEDS TO MORE EFFECTIVELY ACQUIRE AND UTILIZE DIGITAL EVIDENCE 1, 9 (2015), https://www.rand.org/pubs/research_reports/RR890.html [https://perma.cc/F5GE-KCU2] (claiming police rely heavily on digital evidence to learn about victims and suspects); Commonwealth v. Jones, 117 N.E.3d 702, 722 n.1 (Mass. 2019) (Lenk, J., concurring) (noting lawful government seizure of encrypted devices faces challenges); Rob Lekowski, *What Lawyers Need to Know About Data Stored on Mobile Devices*, L. TECH. TODAY (Feb. 17, 2015), https://www.lawtechnologytoday.org/2015/02/data-stored-on-mobile-devices/ [https://perma.cc/A5GA-PHVW] (describing increase in mobile device collection for litigation).

8. *See* Riley v. California, 573 U.S. 373, 393 (2014) (identifying immense storage capacity distinguishes modern cell phones); GOODISON ET AL., *supra* note 7, at 9-10 (discussing different conceptions of reasonable scope for searches of seized devices). The Court highlighted that it would be impossible for someone to physically carry every piece of mail received, every picture taken, or every book or article they have read, but people easily do so with a device the size of a pack of cigarettes. *See Riley*, 573 U.S. at 393-94 (describing search limits of physical realities).

9. *See* Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 IOWA L. REV. 1643, 1648 (2020) (describing court requirement to list device, rather than specific files law enforcement viewed or copied); *see also Riley*, 573 U.S. at 394 (describing cell phone capacity and contents); N.Y. CNTY. DIST. ATT'Y'S OFF., REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 7 (2015), https://www.manhattanda.org/wp-content/themes/dany/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf [https://perma.cc/2X3C-8MZ9] (listing common data sources and their location).

10. *See* Weeks v. United States, 232 U.S. 383, 391-92 (1914) (holding Fourth Amendment limited government power and secured people, their houses, papers, and effects); Hester v. United States, 265 U.S. 57, 59 (1924) (holding Fourth Amendment protections not applicable to open fields); Katz v. United States, 389 U.S. 347, 359 (1967) (prohibiting warrantless surveillance of phonebooth conversations); Chimel v. California, 395 U.S. 752, 766 n.12 (1969) (refusing to call invasion of privacy occurring during top to bottom search of home

digital devices are more than just physical objects, but practices and procedures still lag behind; police are generally able to search an entire device with impunity as long as they have secured a search warrant.[11]

Encryption is a way to scramble information so that only authorized recipients can unscramble it.[12] Device users increasingly rely on encryption to maintain privacy, making it difficult for law enforcement to search encrypted information without compelling suspects to disclose the password or remove encryption protections.[13] Encryption is critically important to modern financial, medical, and business industries, which rely on advanced encryption to send and receive data securely.[14] There are also many personal benefits of encryption, from securing intimate conversations and family photos to keeping prying eyes out of one's search history.[15] But while encryption makes it safe to send a credit card number to a vendor over the internet, it can also make it very difficult for a detective to investigate and subsequently prove criminal activity.[16]

"minor"); Sacharoff, *supra* note 9, at 1646 (noting routine issuance of warrants authorizing limitless digital device search).

11. *See Riley*, 573 U.S. at 393 (distinguishing cell phones from other objects); Adam M. Gershowitz, *The Post*-Riley *Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 588 (2016) (noting courts issue warrants authorizing expansive searches of cell phones, even post-*Riley v. California*).

12. Aloni Cohen & Sunoo Park, Note, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, 32 HARV. J.L. & TECH. 169, 176-77 (2018) (providing brief background on encryption).

13. *See* FRED UPTON ET AL., HOUSE JUDICIARY COMM. & HOUSE ENERGY & COM. COMM., ENCRYPTION WORKING GROUP YEAR-END REPORT 2, 12 (2016), https://info.publicintelligence.net/US-HouseEncryption WorkingGroup-2016.pdf [https://perma.cc/ERA4-Z5K5] (noting increased use of strong encryption creates challenges for law enforcement's access to information).

14. *See id.* at 4 (acknowledging encryption's vital role in personal, economic, and national security). Encryption proponents assert that encryption protects millions of people from fraud and theft, strengthens individual privacy, protects free speech and human rights, and any effort to weaken encryption technology works against the national interest. *See id.* at 2, 4 (highlighting benefits of encryption and recommending Congress not weaken such vital technology); Carlos Liguori, *Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate*, 26 MICH. TECH. L. REV. 317, 319 (2020) (claiming exceptional access mechanisms would weaken encrypted systems). Additionally, proponents note that encryption is used globally and attempts to limit or compromise encryption technology in the United States could push customers to use foreign products. *See* UPTON ET AL., *supra* note 13, at 5 (acknowledging encryption's global presence).

15. *See* Jason Wareham, *Cracking the Code: The Enigma of the Self-Incrimination Clause and Compulsory Decryption of Encrypted Media*, 1 GEO. L. TECH. REV. 247, 251 (2017) (describing morning routine using multiple encryption schemes); UPTON ET AL., *supra* note 13, at 4 (acknowledging encryption's importance to personal, economic, and national security); Shira Ovide, *Police Can Open Your Phone. It's OK*, N.Y. TIMES (Oct. 21, 2020), https://www.nytimes.com/2020/10/21/technology/police-can-open-your-phone-its-ok.html?searchResultPosition=4 [https://perma.cc/3E9G-TT5U] (reporting police use code-breaking technologies to search phones in less serious investigations).

16. *See* GEORGE B. DELTA & JEFFREY H. MATSUURA, LAW OF THE INTERNET § 6.02 (4th ed. Supp. 2022) (describing encryption software for commercial credit card transactions); N.Y. CNTY. DIST. ATT'Y'S OFF., *supra* note 9, at 1 (contending criminals keep records of behavior on phones rather than file cabinets, closets, or safes); Sacharoff, *supra* note 1, at 206 (describing scenarios frustrating police efforts to recover digital evidence); *see also* KRISTIN FINKLEA, CONG. RSCH. SERV., R44481, ENCRYPTION AND THE "GOING DARK" DEBATE 9 (2016), https://fas.org/sgp/crs/misc/R44481.pdf [https://perma.cc/H8BY-3FCD] (describing difficulty law enforcement encounters when retrieving smartphone data).

Investigators have increasingly turned to the courts to compel suspects to decrypt their own devices when investigators believe evidence exists on an encrypted device but cannot access it, and some courts have been more willing than others to oblige.[17] Whether courts will support an order to compel depends on their application of decades-old case law—developed for paper documents—to encrypted data on digital devices.[18] But an encrypted digital device is not a document.[19] Unsurprisingly, a doctrine based on paper documents does not apply cleanly to the encrypted contents of a digital device, and confusion abounds when analogizing the two.[20]

Without coherent, thoughtful judicial direction, the danger is that courts will further erode the constitutional rights not to be a witness against oneself and to be free from unreasonable search and seizure.[21] New guidelines are necessary to establish and clarify the government's power to compel citizens to aid in their own incrimination by disclosing the contents of their minds.[22] Between the interests of law enforcement in a digital age, national reliance on safe and private data, and our cherished liberties and constitutional rights, too much hangs in the balance to risk getting it wrong.[23]

---

17. *See* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 768-69 (2019) (describing common self-incrimination question encountered in criminal investigations). Most courts and scholars agree that compelling a suspect to explicitly provide a password would clearly violate the right against self-incrimination. *See* Sacharoff, *supra* note 1, at 223-24 (asserting government cannot compel suspect to say or write password). The difficulty arises when the government asks a court to compel the password's entry, leaving the police with a fully accessible device. *See id.* at 207 (expressing fundamental nature of question whether courts can compel password entry). Compelled decryption is less clearly testimonial than providing a password, and thus has drawn comparisons to compelled document production. *See id.* at 216-17 (specifying testimonial nature of document production).

18. *See* Fisher v. United States, 425 U.S. 391, 411 (1976) (holding government may compel paper business documents); Seo v. State, 148 N.E.3d 952, 962 (Ind. 2020) (refusing to extend *Fisher* to compelled decryption); State v. Andrews, 234 A.3d 1254, 1274 (N.J. 2020) (applying *Fisher* to compel phone's passcode).

19. *See Seo*, 148 N.E.3d at 959 (reasoning compelled production of unlocked phone unlike compelled production of business documents); Riley v. California, 573 U.S. 373, 393 (2014) (noting cell phones do more than make calls; function like cameras, rolodexes, recorders, televisions, maps).

20. *See* Jeffrey Kiok, Article, *Missing the Metaphor: Compulsory Decryption and the Fifth Amendment*, 24 B.U. PUB. INT. L.J. 53, 76 (2015) (noting attempts to analogize modern encryption and older technologies stretch too far and lose usefulness); Cohen & Park, *supra* note 12, at 179 (asserting analogies hide technical details and cannot convey subtleties).

21. *See Seo*, 148 N.E.3d at 962 (concluding allowance of compelled decryption would result in seismic erosion of right against self-incrimination); Commonwealth v. Jones, 117 N.E.3d 702, 724 (Mass. 2019) (Lenk, J., concurring) (calling majority's decision death knell for protection against self-incrimination in technology era); Nicholas Soares, *The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age*, 49 AM. CRIM. L. REV. 2001, 2017 (2012) (highlighting risk self-incrimination privilege will become "little more than a technicality" with narrow doctrinal interpretation); Nagareda, *supra* note 3, at 1577 (suggesting citizens maintain less protection against compelled self-incrimination this century than eighteenth or nineteenth centuries); Sacharoff, *supra* note 9, at 1646 (claiming diminished procedural protections against unlawful search and seizure).

22. *See* Wareham, *supra* note 15, at 257 (noting lack of guidance from Supreme Court on foregone conclusion doctrine).

23. *See* Riana Pfefferkorn, *The Earn It Act: How to Ban End-to-End Encryption Without Actually Banning It*, STAN. L. SCH.: THE CTR. FOR INTERNET & SOC'Y (Jan. 30, 2020, 12:42 PM),

This Note evaluates the current compelled decryption doctrine.[24] This Note examines the origins of the Fifth Amendment's act-of-production doctrine, its primary exception, the foregone conclusion doctrine, and their application to compelled decryption.[25] This Note also summarizes the Fourth Amendment's particularity requirement and the challenges it poses to compelled decryption.[26] This Note provides an overview of court decisions that highlight the split regarding the application of the doctrines to compelled decryption.[27] Then, this Note analyzes the shortcomings of the existing self-incrimination doctrine in the case of digital devices and argues that the contents of devices are testimonial communications, as is the compelled act of decrypting them.[28] Finally, this Note identifies alternatives to compelled decryption, whereby law enforcement can acquire the evidence they need through means less violative of constitutional protections.[29]

II. HISTORY

A. The Fifth Amendment Right Against Self-Incrimination

Within the U.S. Constitution's Fifth Amendment, the Self-Incrimination Clause enshrines citizens' inherent freedom from being forced to bear witness against themselves.[30] The Self-Incrimination Clause originated from English

---

http://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it [https://perma.cc/W7PC-V98K] (describing balance between law enforcement, network security, privacy, civil liberties, and technological innovation). In addition to judicial guidance on the limits of fundamental rights, many countries are exploring legislative action. *See* Lizzie O'Shea, Opinion, *Australia Wants to Take Government Surveillance to the Next Level*, N.Y. TIMES (Sept. 4, 2018), https://www.nytimes.com/2018/09/04/opinion/australia-encryption-surveillance-bill.html [https://perma.cc/4B6V-SGM5] (describing Australia's proposed law requiring communications providers to assist law enforcement in bypassing encryption). The Telecommunications and Other Legislation Amendment (Assistance and Access) Act allows law enforcement to compel communications providers to assist in national security matters, introduces a new covert computer access warrant, and strengthens existing search and seizure powers under warrant. *See* Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) 4 (Austl.), https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6195_ems_1139bfde-17f3-4538-b2b2-5875f5881239/upload_pdf/685255.pdf;fileType=application%2Fpdf [https://perma.cc/6L7A-3FR6] (describing new, graduated approach to industry assistance). *See generally Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (Austl.) (amending law relating to telecommunications, computer access warrants, and search warrants).

24. *See infra* Sections II.D-E (applying foregone conclusion and particularity doctrines to encrypted digital devices).

25. *See infra* Sections II.A, II.D (detailing history of Self-Incrimination Clause and application to compelled decryption).

26. *See infra* Sections II.B, II.E (providing overview of Fourth Amendment particularity requirement and application to compelled decryption).

27. *See infra* Sections II.D-E (reviewing cases applying act-of-production and foregone conclusion doctrines to compelled decryption).

28. *See infra* Sections III.A-B (analyzing courts' missteps in applying Fourth and Fifth Amendment doctrines to compelled decryption cases).

29. *See infra* Section III.C (suggesting alternatives available to law enforcement).

30. *See* U.S. CONST. amend. V (forbidding compulsion to bear witness against oneself).

common law, where it served as a broad principle against forced testimony that would bring legal peril, infamy, or even disgrace to the witness.[31] The initial concept of the now-familiar right against self-incrimination was to forbid the government from forcing the self-production of adverse evidence.[32] Early state bills of rights first used the language of being a witness against oneself, which was elevated to a constitutional right when the Fifth Amendment was adopted in 1791.[33] Today, a violation of the Self-Incrimination Clause requires elements of compulsion, incrimination, and testimony—the last of which has been the source of abundant litigation.[34]

Commonly considered the Supreme Court's first tango with the privilege against self-incrimination, *Boyd v. United States* outlined the broad initial

---

31. *See* LEONARD W. LEVY, ORIGINS OF THE FIFTH AMENDMENT: THE RIGHT AGAINST SELF-INCRIMINATION 405-06 (1968) (describing common law self-incrimination rights prior to inclusion in U.S. Constitution).

32. *See id.* at 406 (describing wider principles of right against self-incrimination); State v. Andrews, 234 A.3d 1254, 1290 (N.J. 2020) (LaVecchia, J., dissenting) (tracing protection against self-incrimination to Founders' repugnance of compelling cooperation in securing one's own conviction).

33. *See* LEVY, *supra* note 31, at 409, 424-25 (comparing language in early bills of rights and noting amendment's adoption). Virginia was the first to include the sentiment in its Declaration of Rights, with the edict "nor can he be compelled to give evidence against himself." *See id.* at 406 (noting Section 8 of Virginia Declaration of Rights). Prior to inclusion in the Virginia Declaration of Rights, the common law provided broad protections against compelled incriminating testimony and even testimony that would reveal infamy or disgrace. *See id.* (describing broader common-law protections in place prior to Declaration of Rights). Eight states followed suit and included the same privilege in some form in their separate bills of rights. *See id.* at 409 (describing minor changes to wording or placement made by some states). Every state that adopted a bill of rights protected the right against self-incrimination, which cannot be said for the freedom of speech, freedom of press, or other dearly held rights. *See id.* at 412 (highlighting importance of right against self-incrimination considering other omissions). Ultimately, the drafters of the U.S. Bill of Rights included the right in the Fifth Amendment, but it is difficult to determine the scope they intended. *See id.* at 429-30 (admitting too few clues left to know Framers' intended scope). Nevertheless, it is likely they thought a statement of the bare principle would be sufficient to cement a deeply accepted principle: that respect for the individual demanded that guilt be determined by just means, and that no man can be obligated to furnish evidence in his own conviction. *See id.* at 431-32 (describing principles of Constitution and Fifth Amendment). The somewhat ambiguous term "witness" left open questions about its scope, but modern courts and legal scholars generally agree that the Self-Incrimination Clause prevents government use of threats, force, or intimidation to obtain confessions or evidence. *See id.* at 405 (claiming right against self-incrimination enshrined in ambiguous way); Michael S. Pardo, *Disentangling the Fourth Amendment and the Self-Incrimination Clause*, 90 IOWA L. REV. 1857, 1869 (2005) (explaining modern conception of compelled testimony).

34. *See* Pardo, *supra* note 33, at 1868 (describing limits on government attempts to gather information and confusion stemming from testimonial requirement); *see also* Fisher v. United States, 425 U.S. 391, 408 (1976) (specifying when Fifth Amendment applies). Compulsion means impermissible conduct meant to trigger a suspect's statements; some types of pressure are allowed, such as favorable plea agreements, but the court insists on the suspect's free will. *See* Pardo, *supra* note 33, at 1868-69 (describing compulsion requirement). Incrimination is defined broadly; a statement is considered incriminating if it might be used in a criminal prosecution or could even lead to other such evidence. *See id.* at 1869 (describing incrimination requirement). Testimony is the trickiest requirement of the three, and it generally requires communicating one's knowledge or beliefs through words or nonverbal conduct. *See id.* at 1870 (describing testimony requirement). Because the Self-Incrimination Clause uses the word "witness," courts have applied it only to testimonial communications—what a witness would provide in a court setting. *See* United States v. Hubbell, 530 U.S. 27, 34 (2000) (describing limiting effect of word "witness").

boundaries of the Self-Incrimination Clause.[35] In 1884, a New York District Attorney charged Boyd with fraudulently importing plate glass without paying the required taxes.[36] Using a court order authorized by federal statute, the District Attorney compelled Boyd to produce the invoice for the glass, believing the invoice would prove the fraud.[37] Boyd claimed the law that authorized this type of order was unconstitutional because the government could not lawfully compel evidence from a defendant.[38]

The Court agreed, calling the compelled production an unreasonable search and seizure under the Fourth Amendment.[39] The Court reasoned that the

35. *See* Boyd v. United States, 116 U.S. 616, 633-35 (1886) (discussing meaning and scope of Self-Incrimination Clause); Soares, *supra* note 21, at 2007 (stating *Boyd* first case to interpret Self-Incrimination Clause); Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27, 31 (1986) (claiming *Boyd* beginning of Supreme Court's effort to apply self-incrimination to document subpoenas); *Hubbell*, 530 U.S. at 55 (Thomas, J., dissenting) (noting significance of *Boyd* case for self-incrimination protections). *But see* Nagareda, *supra* note 3, at 1584 (identifying equation of document production with furnishing evidence against oneself first occurred in *United States v. Reyburn*). Nagareda begins his analysis with *Reyburn*, where the court stated in dicta that a witness, even if he could be found, could not be compelled to produce a document because it would have proved highly incriminating. *See* Nagareda, *supra* note 3, at 1584-85 (commenting on lack of citation for stating compelled production included bearing witness against oneself). Since this statement was dicta, most modern accounts begin with *Boyd*. *See id.* at 1585 (noting first explicit ruling stating compelled production violated Fifth Amendment came in *Boyd*).

36. *See Boyd*, 116 U.S. at 617-18 (describing charge against Boyd).

37. *See id.* at 618 (summarizing origins of compelled production order). The federal act authorized the government to go to great lengths to secure duties on imported products and allowed the government to fine offenders $50–$5,000, imprison them for up to two years, and confiscate the offending merchandise. *See id.* at 617 (describing act charging offenders); 19 U.S.C. § 535 (allowing United States attorneys prosecuting civil revenue cases to compel document production), *invalidated by* Boyd v. United States, 116 U.S. 616 (1886). The Court highlighted that Congress passed the law during a "period of great national excitement, when the powers of the government were subjected to a severe strain to protect the national existence." *Boyd*, 116 U.S. at 621. In addition to holding the order to compel unconstitutional, the Court further held the statute unconstitutional. *See id.* at 638 (holding order and law unconstitutional and void).

38. *See Boyd*, 116 U.S. at 618 (describing Boyd's objection to invoice's introduction into evidence). Boyd obeyed the notice from the trial court and produced the invoice, but he objected to the order and the law authorizing it, claiming that the government could not compel evidence from a suspect. *Id.* (describing Boyd's objections). The trial court admitted the evidence and a jury found for the government, forcing Boyd to forfeit the plate glass. *Id.* (describing case posture).

39. *See id.* at 635 (holding compulsory production of private books and papers unreasonable search and seizure under Fourth Amendment); Alito, *supra* note 35, at 35 (stating Court's decision more complicated than required). Alito asserts that the Court could have used Fifth Amendment privilege to strike down the law and forbid the compelled production of private papers. *See* Alito, *supra* note 35, at 35 (criticizing Court's approach); *see also* Nagareda, *supra* note 3, at 1586 (hypothesizing Court focused on Fourth Amendment following legislative history of statute authorizing court order). Nagareda traced the Court's rationale for invoking the Fourth Amendment to previous, unpopular legislative authorization for federal agents to enter any premises and search for invoices, books, or papers associated with illegally imported merchandise. *See* Nagareda, *supra* note 3, at 1586 (noting Justice Bradley's attention to reasoning behind provision). While less severe, the statute that authorized Boyd's court-ordered compulsion had replaced earlier federal authorization—which may explain the Court's inclusion of the Fourth Amendment in the *Boyd* analysis—where there was merely a compelled production. *See id.* at 1586-87 (noting compelled production of documents alternative option to their seizure). The Court's Fourth Amendment analysis did not stand the test of time. *See Fisher*, 425 U.S. at 407-08 (listing cases overturning aspects of *Boyd's* holdings); Nagareda, *supra* note 3, at 1593 (reiterating Court's observation modern Fourth Amendment decisions undercut *Boyd*).

compelled production had the same effect and purpose as a search and seizure, and it was unreasonable because it went further than the writs of assistance.[40] Justice Bradley, writing for the majority, then stretched his reasoning to conclude that the compelled production also violated the Fifth Amendment, holding "a compulsory production of the private books and papers of the owner . . . is compelling him to be a witness against himself, within the meaning of the Fifth Amendment of the Constitution."[41] With this proclamation, the Court cemented the notion that the government could neither seize private books and papers under the Fourth Amendment nor compel them under the Fifth Amendment.[42] Over the next century, however, the Court struggled with Justice Bradley's conflation of the two amendments; the Court eventually teased them apart again by distinguishing between testimonial evidence that the Fifth Amendment protects and other types of more physical evidence that the Fourth Amendment protects.[43]

1. The Act-of-Production Doctrine

One hundred years after *Boyd*, in *Fisher v. United States*, the Court repudiated *Boyd*'s analysis and introduced a new framework with which to consider the

40. *See Boyd*, 116 U.S. at 622-23, 634-35 (holding compelled production of papers to establish criminal charge within scope of Fourth Amendment). The Court noted that common law or legal rationale would have made this compulsion reasonable and distinguished search and seizure of goods subject to unpaid tax from search and seizure of personal papers for information. *See id.* at 623 (noting long history of search and seizure of goods subject to tax and illegal items).

41. *See* Boyd v. United States, 116 U.S. 616, 634-35 (1886) (holding compulsory production of private papers makes owner witness against himself). The Court acknowledged that compelling the papers was "the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure." *Id.* at 635.

42. *See* Soares, *supra* note 21, at 2007 (noting *Boyd* protected defendants against compelled production of books and papers).

43. *See* Nagareda, *supra* note 3, at 1591 (summarizing Court's distinction between testimonial communication and other forms of incriminating evidence); *see also* Sacharoff, *supra* note 1, at 213 (claiming undoing *Boyd* unbundled Fourth and Fifth Amendments). Because the Self-Incrimination Clause does not forbid all compelled, incriminating evidence, but only compelled, incriminating, *testimonial* communications, the definition of testimonial has taken on great significance. *See* United States v. Hubbell, 530 U.S. 27, 34 (2000) (describing effect of word "witness" in Fifth Amendment). Unlike sworn communications, an individuals' physical characteristics, even if compelled and incriminating, neither expressly nor impliedly *assert* a fact. *See id.* at 35. For example, taking blood from a person suspected of driving under the influence does not violate the Self-Incrimination Clause because the blood does not provide the state communicative or testimonial evidence. *See* Schmerber v. California, 384 U.S. 757, 761 (1966) (excluding blood analysis from Fifth Amendment protection because of physical rather than testimonial nature). Likewise, compelling a suspect to try on certain clothing to appear in a lineup does not violate the Self-Incrimination Clause. *See* Holt v. United States, 218 U.S. 245, 252-53 (1910) (calling objection to suspect trying on blouse "an extravagant extension" of Fifth Amendment). Compelling a suspect to give a voice sample is not testimonial. *See* United States v. Wade, 388 U.S. 218, 222 (1967) (analogizing compulsion to speak to *Schmerber v. California*'s compulsion to provide blood sample). Compelling a suspect to provide a handwriting sample to compare to a note used in a burglary is not self-incrimination because the sample identifies a physical characteristic. *See* Gilbert v. California, 388 U.S. 263, 266-67 (1967) (distinguishing means of communication from compelled communication).

compelled production of documents: the act-of-production doctrine.[44] Fisher was under IRS investigation for tax liability when the government subpoenaed an income and expense report that his accountant had prepared.[45] Claiming the documents were privileged under the Fourth and Fifth Amendments, Fisher's attorney declined to comply with the summons.[46]

The *Fisher* Court held that the right against self-incrimination does not protect physical contents of already existing and possibly incriminating documents because their creation was voluntary—the government did not compel their creation.[47] Furthermore, Fisher neither created the papers in question nor made testimonial declarations in them.[48] Nevertheless, the Court reasoned that while the contents were not testimonial and thus not protected by the Fifth Amendment, the *act* of producing them required a separate analysis.[49] Specifically, the Court held that Fisher's act of production implicitly communicated to the government that the papers existed, they were in Fisher's control, and he believed they were

44. *See* Fisher v. United States, 425 U.S. 391, 401 (1976) (stating Fifth Amendment protects against compelled self-incrimination, not disclosure of private information without testimony); Alito, *supra* note 35, at 29 (summarizing effect of *Fisher* on *Boyd*); *see also* Nagareda, *supra* note 3, at 1590 (highlighting *Fisher* ended Fifth Amendment protections against compelled production).

45. *See Fisher*, 425 U.S. at 391 (summarizing case posture). Although the subpoena in question described tax documents, the government can also subpoena tangible objects; the *Fisher* analysis remains the same in both scenarios. *See* FED. R. CRIM. P. 17(c)(1) (outlining federal rules for document or object subpoenas); WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 8.13(e) (4th ed. 2020) (noting self-incrimination privilege applicable to defendant ordered to produce gun).

46. *See Fisher*, 425 U.S. at 395 (summarizing attorney's response to summons). Although Fisher's attorneys possessed the documents, the Court addressed whether the documents could have been compelled from Fisher. *See id.* at 405 (outlining effect of attorney-client privilege on self-incrimination privilege). The Court reasoned that if the government could not summon the documents from Fisher, then the government could not summon them from his attorney due to attorney-client privilege. *See id.* (acknowledging Fisher provided documents to attorney for legal advice).

47. *See id.* at 409-10 (highlighting voluntary preparation of papers); Sacharoff, *supra* note 1, at 213 (clarifying Fifth Amendment does not protect preexisting documents). The Court specified, "[w]e cannot cut the Fifth Amendment completely loose from the moorings of its language, and make it serve as a general protector of privacy a word not mentioned in its text and a concept directly addressed in the Fourth Amendment." *See Fisher*, 425 U.S. at 401.

48. *See Fisher*, 425 U.S. at 409 (highlighting documents created by accountant contained no testimonial declarations).

49. *See id.* at 410 (reasoning act of producing evidence communicative); Sacharoff, *supra* note 1, at 217 (describing exception to refusal to accord Fifth Amendment protection to papers' contents). The Court in *Fisher* stated:

> 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. Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena.

Fisher, 425 U.S. at 410.

the documents sought.[50] The Court then had to address whether these implicit communications were testimonial.[51]

2. The Foregone Conclusion Exception

The *Fisher* Court defined a new exception to what is considered testimonial, holding that because the government already knew the communication implied by the act, the act itself added nothing to the sum total of the case, and therefore it did not rise to the level of testimony.[52] The Court acknowledged that producing the financial reports was implicitly communicative and thus normally protected by the Fifth Amendment, but it created a narrow exception allowing this instance of compelled production.[53] The foregone conclusion exception—as it has come to be known—allows compelled production that communicates facts if the government already knows those facts.[54]

The *Fisher* holding set the course for future constitutional determinations of compelled acts in three ways.[55] First, it divorced the documents' contents from the act of producing them, removing the documents' contents from the Fifth

50. *See* Fisher v. United States, 425 U.S. 391, 410 (1976) (identifying tacit concessions associated with subpoena compliance).

51. *See id.* (noting difficult issue of whether tacit concessions testimonial for purposes of Fifth Amendment).

52. *See id.* at 411 (denying implicit communication rose to level of testimony under Fifth Amendment). The Court explained that although the "tacit averments" were present, they did not qualify as testimonial because the documents were common tax documents. *See id.* at 410-11 (reasoning production of standard documents not testimonial). Furthermore, the government did not rely on Fisher's truth-telling to prove the documents' existence or his access to them, and the documents' location and existence were a foregone conclusion because the government already knew the attorney possessed the prepared documents. *See id.* at 411 (explaining basis of foregone conclusion reasoning). Because Fisher had not been compelled to give testimony, neither in the papers nor by producing them, his Fifth Amendment rights had not been violated. *See id.* at 414 (holding compliance with summons involved no incriminating testimony protected by Fifth Amendment).

53. *See id.* at 410-11 (holding act of production did not involve testimonial self-incrimination). No such exception exists for oral testimony; a witness is still a witness even if the government knows the answers to the questions posed. *See* Nagareda, *supra* note 3, at 1597-98 (claiming government's preexisting knowledge does not impact witness status). The government's level of knowledge is irrelevant to whether the government may compel an oral statement by force or threat. *See id.* (recognizing courts do not consider government's preexisting knowledge when determining whether to compel oral testimony).

54. *See Fisher*, 425 U.S. at 411 (holding existence and location of documents amounted to foregone conclusion); Sacharoff, *supra* note 1, at 218 (describing function of foregone conclusion doctrine to make compelled production nontestimonial when government knows information); *Compelled Decryption Primer*, FOURTH AMENDMENT CTR., NAT'L ASS'N OF CRIM. DEF. LAWS. (2019), https://www.nacdl.org/Nacdl/media/image_library/Elements/Advertisements/CompelledDecryptionPrimer_1.pdf [https://perma.cc/RU2L-LRXF] (describing foregone conclusion exception). The level of government knowledge cannot be too general; knowing only the type of documents that a certain type of people usually keep is not specific enough, but it does not have to be as specific as knowing the exact contents of the documents. *See* United States v. Hubbell, 530 U.S. 27, 44 (2000) (rejecting government's claim of foregone conclusion because businessmen always possess such business records).

55. *See* Nagareda, *supra* note 3, at 1593 (stating *Fisher* overturned *Boyd* where Fifth Amendment bars compelled production of incriminating documents); Sacharoff, *supra* note 1, at 217-18 (specifying Fifth Amendment protects against compelled production for testimonial acts but not if testimony known).

Amendment's protection.[56] Second, it hinged Fifth Amendment protection of a compelled act on whether the act was sufficiently testimonial, which in turn hinges on the subjective interpretation of what one communicates with an act.[57] Third, it exempted some testimonial acts from protection of the Fifth Amendment if the government could prove it already knew of the communication implied by the act.[58] All three features of the *Fisher* holding greatly reduced the protections the Fifth Amendment provides and have created division and confusion as courts attempt to apply these doctrines to encrypted digital devices.[59]

3. Compelled Production of Other Evidence

Under *Fisher*, the government may compel existing, voluntarily created papers, but courts have typically drawn the line at compelling incriminating objects from suspects.[60] Case law has established that compelling a weapon from a suspect violates the Fifth Amendment right against self-incrimination.[61] The Massachusetts Supreme Judicial Court (SJC) stated:

---

56. *See* Nagareda, *supra* note 3, at 1593-94 (decoupling document's content from its production); Sacharoff, *supra* note 1, at 205 (describing gap in coverage between Fourth and Fifth Amendments over privacy of papers and information). The holding in *Fisher* related to tax documents, not personal and private papers. *See* Fisher v. United States, 425 U.S. 391, 391 (1976) (summarizing investigation). In a footnote, however, the Court identified that the circumstances did not involve privacy problems unique to a subpoena of a personal diary. *See id.* at 401 n.7 (noting summons narrowly focused and relevant to tax investigation).

57. *See Fisher*, 425 U.S. at 409 (asking what incriminating testimony compelled by document summons); Laurent Sacharoff, Response, *What Am I Really Saying when I Open My Smartphone? A Response to Orin S. Kerr*, 97 TEX. L. REV. ONLINE 63, 67 (2019), https://texaslawreview.org/wp-content/uploads/2019/04/Sacharoff-TLRO-V97.pdf [https://perma.cc/Z932-HPLW] (describing nearly impossible task required in compelled decryption cases: determining implicit communication of acts); *see also* Alito, *supra* note 35, at 46 (calling act-of-production theory abstract and difficult to apply).

58. *See* Wareham, *supra* note 15, at 256 (explaining government can overcome Fifth Amendment protections with independent knowledge of evidence); William F. Bloomer, *18th Century Constitutional Principles Meet 21st Century Technology: Compelling Individuals to Enter Passwords into Electronic Devices Under* Commonwealth v. Gelfgatt*, 468 Mass. 512 (2014) and* Commonwealth v. Jones*, 481 Mass. 540 (2019)*, 101 MASS. L. REV. 65, 68 (2020) (highlighting foregone conclusion exception can render testimonial acts nontestimonial).

59. *See* Kerr, *supra* note 17, at 768-69 (asserting courts disagreed on when to uphold data decryption court orders); Alito, *supra* note 35, at 51 (describing new, uncertain, and ambiguous course *Fisher* set for Fifth Amendment).

60. *See* LAFAVE ET AL., *supra* note 45, § 8.13(e) (noting act-of-production doctrine applies to physical evidence unless testimonial and incriminating).

61. *See* Commonwealth v. Hughes, 404 N.E.2d 1239, 1244 (Mass. 1980) (holding production of revolver would implicitly communicate its existence, location, and control). Police accused Hughes of firing a gun into a vehicle with two people in it. *See id.* at 1240 (summarizing facts of case). Hughes had a registered weapon that matched the bullet recovered from the crime scene, and he had not reported the gun lost or stolen. *See id.* at 1240-41. The court ordered him to produce it, but he refused, citing his Fifth Amendment rights. *See id.* at 1240. The court looked primarily to *Schmerber* and *Fisher* and held that the act would implicitly communicate facts which were not a foregone conclusion. *See id.* at 1242, 1244 (describing source of precedent and implicit statements in producing revolver).

> A search warrant has proved futile. Apparently the Commonwealth does not know whether the gun exists or, if it does, where it is being kept; it has only some evidence to base a suspicion that the defendant may be able to produce it, if he will. In the language of the cases, the Commonwealth is seeking to be relieved of its ignorance or uncertainty by trying to get itself "informed of knowledge the defendant possesses."[62]

B. The Fourth Amendment Particularity Requirement

The Fourth Amendment's particularity requirement, which prohibits unreasonable searches and seizures, provides a second constitutional right limiting law enforcement's evidence-gathering powers.[63] Acquiring a warrant—the default method for ensuring a reasonable search or seizure—is feasible only when law enforcement convinces a neutral magistrate that there is probable cause to believe that a search or seizure will provide evidence of a criminal act.[64] The particularity requirement ensures warrants "particularly describ[e] the place to be searched, and the persons or things to be seized."[65] For example, a search for a fifty-inch television does not authorize police to look in the microwave.[66] The original intent behind the particularity requirement, as understood by the

---

62. *Id.* at 1244 (quoting People *ex rel.* Bowman v. Woodward, 349 N.E.2d 57, 60 (Ill. 1976)).

63. *See* U.S. CONST. amend. IV; Pardo, *supra* note 33, at 1867 (claiming Fourth Amendment limits government access and use of information). The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV. Constitutionality under the Fourth Amendment requires a two-part analysis: Was there a search or seizure, and if so, was it reasonable? *See, e.g.*, Marron v. United States, 275 U.S. 192, 195 (1927) (holding general searches unconstitutional); Groh v. Ramirez, 540 U.S. 551, 557 (2004) (holding warrant invalid for failing to list seized persons or things).

64. *See* Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance*, 90 NEB. L. REV. 971, 972 (2012) (describing Fourth Amendment requirements); *see also* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.6(a) (6th ed. 2020) (claiming many objects constitute fruits of criminal activity, thus warrants may issue for any item).

65. *See* U.S. CONST. amend. IV (defining particularity requirement). One recent test for the sufficiency of warrant particularity asks, "whether the warrant's description of items to be searched would enable the searcher to reasonably ascertain and identify the things authorized to be seized." *See* United States v. Dunn, 719 F. App'x. 746, 748 (10th Cir. 2017) (per curiam). Law enforcement searched Dunn's apartment under a very broad warrant secured after tracking a stabbing suspect to the apartment. *See id.* (describing facts of case). The warrant prefaced items to be searched with the catch-all phrase, "include but are not limited to." *See id.* (noting catch-all phrases may widen scope of warrant too far). Police found two firearms during the search, which caused police to file felony firearm possession charges. *See id.* (describing procedural history). The court held that the added catch-all phrase unlawfully allowed officers to search "for any item for any reason." *See id.* at 749-50 (holding language did not render warrant sufficiently particular).

66. *See* Gershowitz, *supra* note 11, at 638 (highlighting example of physical search restrictions particularity requirement imposes).

Supreme Court, was to prohibit the despised general warrants and writs of assistance common in the colonial era that enabled "British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[67]

Securing a warrant does not guarantee a constitutional search; courts occasionally find warrants, and the searches they authorize, unconstitutional.[68] For instance, a federal district court in *United States v. Wey*[69] granted a motion to suppress all seized evidence after the FBI raided Wey's home and offices in search of evidence of suspected financial fraud and market manipulation.[70] The FBI seized 4,500 pages of documentation and twenty-four pieces of computer or other electronic equipment from his office, as well as 4,000 hard-copy documents and twenty-five devices or pieces of equipment from his home.[71] The court held that the warrants lacked particularity, were overbroad, and were executed in blatant disregard of the Fourth Amendment.[72] The warrants did not describe suspected criminal conduct or cite criminal statutes and authorized the

67. *See* Riley v. California, 573 U.S. 373, 403 (2014) (recognizing original purpose of Fourth Amendment). The question the Court addressed in *Riley* was whether the search of a cell phone incident to arrest was constitutional without a warrant. *See id.* at 378 (summarizing issue). Police stopped Riley for driving with expired registration stickers and arrested him when they found concealed, loaded firearms in the vehicle. *See id.* The police then searched a phone found in Riley's pocket, located a picture of him with a car that had been involved in a shooting a few weeks earlier, and charged him with multiple crimes associated with that shooting. *See id.* at 378-79 (summarizing facts of case). The Court held that police must secure a warrant before searching a cell phone incident to arrest, acknowledging that while this requirement would restrict law enforcement's ability to combat crime, individual privacy was worth that cost. *See id.* at 401, 403 (describing holding and its implications).

68. *See* Friess, *supra* note 64, at 972 (noting warrant must have probable cause and particularly describe place searched and things seized); United States v. Alberts, 721 F.2d 636, 639-40 (8th Cir. 1983) (holding improper search at residence different than address specified on warrant).

69. 256 F. Supp. 3d 355 (S.D.N.Y. 2017).

70. *See id.* at 362-63, 409-10 (holding warrant lacked particularity and describing warrant's affidavit).

71. *See id.* at 370, 372-73 (describing both searches). The financial and personal documents seized included materials unrelated to the investigation, such as drug prescriptions; data about medical appointments; family members' x-rays; Wey's will; Wey's health care directives; family sports schedules; high school, college, and law school mementos and photographs; Wey's children's grades and test scores; divorce papers from Wey's first marriage; Wey family passports; and family photographs. *See id.* at 372-73 (describing documents seized). The electronic devices that were seized or copied included cell phones, personal computers, laptops, and flash drives. *See id.* at 373 (describing electronics seized or copied). The court noted:

> During the course of the Apartment Search, the search team did not review every document that it encountered. Instead, the searching agents would "flip through" any given box or other container to see if it contained at least a "subset" or "sampl[e]" of relevant documents, and, if so, they would seize the entire container.

Id. at 372.

72. *See id.* at 410 (inferring lack of good faith from indiscriminate physical search and later mining for further evidence).

government to seize expansive categories of documents without linking them to suspected criminal activity.[73]

C. Encryption Overview

Encryption—although not a new concept—poses new challenges for law enforcement and courts in both Fourth and Fifth Amendment jurisprudence.[74] Cryptography is the millennia-old science of transmitting messages that are unreadable until the recipient can translate them into readable text.[75] The word loosely translates from the Greek words *kryptos* and *graphein*, which mean "hidden" and "to write," respectively.[76] Cryptography is an ancient practice, but it was revolutionized with the advent of computers in the twentieth century.[77] In the modern practice of cryptography, encryption refers to the process of converting readable data, often called plaintext, into scrambled data, often called cyphertext, using an encryption algorithm and a password, often called a key.[78] The software on an encryption-enabled device scrambles the data on the device when locked, and only the user's password will unlock the device and unscramble the data.[79]

Once a technology primarily reserved for war generals and state secrets, encryption software is now a basic feature on most smart phones and readily available for computers.[80] While this feature increases the privacy of digital communications, it complicates law enforcement officials' attempts to access evidence of crime stored on those devices.[81] Law enforcement organizations

---

73. *See Wey*, 256 F. Supp. 3d at 384-85 (listing warrant shortcomings). The only restriction the warrant imposed was that the documents must relate to the owner of the searched premises. *See id.* at 387 (claiming warrants gave unfettered discretion to executing officers).

74. *See* Cohen & Park, *supra* note 12, at 172 (highlighting challenges encryption poses to law enforcement); FINKLEA, *supra* note 16, at 1 (calling strong end-to-end encryption hurdle for law enforcement).

75. *See* ROBERT CIESLA, ENCRYPTION FOR ORGANIZATIONS AND INDIVIDUALS 1-2 (2020) (defining and outlining history of cryptography).

76. *See id.* at 1 (characterizing etymology of cryptography).

77. *See id.* at 2, 8 (recalling earliest uses of cryptography and explaining impact of digital encryption on cryptography).

78. *See* Cohen & Park, *supra* note 12, at 176 (giving brief background of encryption). Encryption abilities are standard on most modern computers. *See* Kiok, *supra* note 20, at 56.

79. *See* Sacharoff, *supra* note 1, at 220 (explaining meaning of locking device); Carissa A. Uresk, Comment, *Compelling Suspects to Unlock Their Phones: Recommendations for Prosecutors and Law Enforcement*, 46 BYU L. REV. 601, 604-05 (2021) (explaining difference between locking device with and without encryption).

80. *See* Wareham, *supra* note 15, at 247 (describing growing sphere of encryption); N.Y. CNTY. DIST. ATT'Y'S OFF., *supra* note 9, at 1 (summarizing Apple and Google's decisions to place encryption on their phones).

81. *See* N.Y. CNTY. DIST. ATT'Y'S OFF., *supra* note 9, at 1 (explaining how encryption prevents law enforcement from accessing evidence even with warrant). The New York County District Attorney's Office objected to default encryption because it allowed criminals to keep their data from law enforcement, even when police wished to search the device lawfully. *See id.* (describing law enforcement's response to default encryption). Before encryption, police could search anywhere, provided they had a warrant. *See* Dan Terzian, *Forced Decryption as Equilibrium—Why It's Constitutional and How* Riley *Matters*, 109 NW. UNIV. L. REV.

have reported a trend they refer to as "going dark," where prosecution of criminals is increasingly difficult because securing evidence of their misdeeds is more challenging.[82] Ironically, this reduced access to potential evidence comes in the midst of what civil rights proponents claim is a "golden age of surveillance," where the police have an abundance of digital information at their fingertips.[83] Some theorize that encryption emerged to alter the balance of power, once again giving individuals the ability to protect their private information.[84]

D. Applicability of the Foregone Conclusion Doctrine to Encrypted Digital Devices

The Supreme Court has not yet ruled on a case involving compelled decryption of a digital device.[85] The three cases where the Court applied the act-of-production and foregone conclusion doctrines involved paper business documents.[86] Nevertheless, defendants are raising the question of whether

---

ONLINE 56, 62 (Sept. 5, 2014), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1010&context=nulr_online [https://perma.cc/U4JQ-8H6Z] (noting before encryption government obtained data with warrant).

82. *See* FINKLEA, *supra* note 16, at 1 (outlining history and trajectory of debate around "going dark").

83. *See id.* (describing "golden age of surveillance"); O'Shea, *supra* note 23 (claiming state's capacity to spy on citizens growing exponentially because of technology); Jack Nicas, *The Police Can Probably Break into Your Phone*, N.Y. TIMES (Oct. 21, 2020), https://www.nytimes.com/2020/10/21/technology/iphone-encryption-police.html [https://perma.cc/8FMJ-ZL2S] (noting police routinely get past smartphone encryption). *But see* N.Y. CNTY. DIST. ATT'Y'S OFF., *supra* note 9, at 6 (claiming "golden age of surveillance" unconvincing because much important data only resides on encrypted devices). In its 2015 report, the New York County District Attorney's Office acknowledged that although some information can be lawfully obtained from cloud storage or phone service providers, a significant portion of evidentiary data is unavailable because it remains encrypted on the device. *See* N.Y. CNTY. DIST. ATT'Y'S OFF., *supra* note 9, at 8 (noting cloud and phone companies do not possess same information on devices). Even if a suspect sets a device to back up to a more accessible location, such as cloud storage, law enforcement may not be able to find the location, the data may not have been backed up yet, or it may have been deleted. *See id.* (describing data available on device and reasons cloud storage poor substitute).

84. *See* Sacharoff, *supra* note 1, at 205 (suggesting encryption filled gap into which private papers fell unprotected by Fourth or Fifth Amendments).

85. *See* Commonwealth v. Davis, 220 A.3d 534, 543 (Pa. 2019) (noting Supreme Court did not address whether compelled password disclosure testimonial); State v. Andrews, 234 A.3d 1254, 1286 (N.J. 2020) (LaVecchia, J., dissenting) (stating Supreme Court did not address split over applicability of act-of-production doctrine to encrypted devices).

86. *See Davis*, 220 A.3d at 549 (noting Supreme Court limited foregone conclusion doctrine's application to compulsion of financial or business documents). *Fisher* was the only Supreme Court case that held the foregone conclusion doctrine allowed document compulsion. *See id.* (noting Court never applied foregone conclusion beyond business or financial documents). In *United States v. Doe*, a grand jury investigating corruption in municipal contracts served Doe with five subpoenas compelling nearly every document associated with his businesses over a period of four years, including ledgers, bank statements, and paid bills. *See* United States v. Doe, 465 U.S. 605, 606-07 (1984) (describing government subpoenas Doe had moved to quash). The Court held that the contents of the documents were not privileged but the compelled act was, relying on the lower courts' agreement that the act would have involved testimonial self-incrimination. *Id.* at 612-14 (holding act, but not contents, protected). In *United States v. Hubbell*, the Court again applied *Fisher* to the analysis of a document subpoena. *See* United States v. Hubbell, 530 U.S. 27, 44-46 (2000) (distinguishing facts in *Hubbell* from *Fisher*

compelled decryption is constitutional more frequently, and a definitive split has developed among state and circuit courts.[87] Interestingly, there is no clear trend, and both federal and state courts are evenly divided.[88] Most courts have determined that entry of a password conveys some testimonial information; where they diverge is on the question of whether that information is a foregone conclusion.[89]

1. The Argument that Compelled Decryption Violates the Fifth Amendment

Multiple courts have expressly held that compelling a suspect to decrypt a device violates the Fifth Amendment.[90] Some of these courts have reasoned that the act of unlocking a device communicates a breadth of information, including the suspect's knowledge of the password, the information's existence on the device, and the suspect's possession or control of that information.[91] Other courts have also noted that disclosing or entering a password requires using "the

and dismissing indictment). Hubbell initially pled guilty to mail fraud and tax evasion and agreed to cooperate in a wider investigation. *See id.* at 30 (describing procedural history of case). The government served him with a subpoena for eleven categories of business records, and although he initially claimed a Fifth Amendment privilege, he complied with a court order and produced 13,120 pages of documents. *See id.* at 31 (describing response to commands of subpoena). Following a review of the documents, the prosecution brought ten new charges against Hubbell. *See id.* (describing second prosecution based on search of compelled documents). The Court held that the production violated the constitutional privilege against self-incrimination because its testimonial nature was the first step in an evidence chain leading to further prosecution. *See id.* at 42-43 (highlighting first step in chain of evidence and summarizing self-incrimination protections). The Court dismissed the new indictments, stressing that the government had no prior knowledge of the documents' existence or location. *See id.* at 45-46 (rejecting argument government knew about documents because businesspeople always have certain types of documents).

87. *See* Kerr, *supra* note 17, at 769 (describing courts' disagreement on power to compel decryption); *Andrews*, 234 A.3d at 1269 (noting courts have diverged after grappling with foregone conclusion doctrine's applicability beyond document production).

88. *See* Uresk, *supra* note 79, at 635-36 (discussing current trends regarding split).

89. *See* FOSTER, *supra* note 4, at 2 (summarizing where courts agree and disagree regarding compelled decryption). The degree to which courts protect encrypted communications may depend on the analogy they apply to the concept of encryption. *See id.* at 2-3 (describing Court's reasoning in *Hubbell*); Ryan Calo, *Robots as Legal Metaphors*, 30 HARV. J.L. & TECH. 209, 212 (2016) (asserting judges rely on analogies when applying reason to new technologies). One analogy likens the decryption of a device to handing over a combination to a wall safe, which could be testimonial, and another describes it as giving up the key to a strongbox, which is not testimonial. *See* FOSTER, *supra* note 4, at 2 (describing potential analogies).

90. *See* Garcia v. State, 302 So. 3d 1051, 1057 (Fla. Dist. Ct. App. 2020) (holding compelled password disclosure testimonial and foregone conclusion doctrine not applicable to compelled oral testimony); Seo v. State, 148 N.E.3d 952, 958 (Ind. 2020) (holding Fifth Amendment prohibits compelled self-incrimination); People v. Spicer, 125 N.E.3d 1286, 1292 (Ill. App. Ct. 2019) (holding password compulsion implicated Fifth Amendment and foregone conclusion doctrine did not apply); *Davis*, 220 A.3d at 550 (holding compelled decryption testimonial thus protected, and foregone conclusion doctrine inapplicable to compelled decryption); United States v. Doe (*In re* Grand Jury Subpoena *Duces Tecum* Dated Mar. 25, 2011), 670 F.3d 1335, 1349 (11th Cir. 2012) (holding Fifth Amendment did not allow compelled decryption because government could not show foregone conclusion).

91. *See Seo*, 148 N.E.3d at 955 (holding decryption conveys breadth of factual information); *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d at 1346 (concluding decryption communicates knowledge of existence, possession, access to and control of incriminating evidence).

contents of one's mind," which renders the act testimonial—and when it provides incriminating evidence, compelling the act violates the Self-Incrimination Clause.[92] To apply the foregone conclusion doctrine, these courts have held that the police must demonstrate that they had particular knowledge of the exact evidence they were searching for.[93]

For example, in *Seo v. State*, the Indiana Supreme Court held that the act of unlocking a smartphone communicates more than simply knowledge of the password; it communicates the existence of the files on the phone and the suspect's possession of those files.[94] The *Fisher* court describes these communications as tacit averments: facts the act demonstrates.[95] Because the State admittedly did not know exactly what evidence it was looking for on the device, the *Seo* court held the State did not have the specificity of information required to satisfy the foregone conclusion doctrine.[96] Thus, the act of unlocking the phone was testimonial and could not be compelled, and the court reversed Seo's contempt order for refusing to decrypt her phone.[97]

---

92. *See Garcia*, 302 So. 3d at 1055 (holding revelation of passcode verbally communicates contents of suspect's mind); *Spicer*, 125 N.E.3d at 1290 (citing *Hubbell* definition of testimonial when government compels defendant to use contents of mind). The court in *State v. Garcia* recognized that its holding conflicted with the Second District Court of Appeal's decision in *State v. Stahl* and certified the questions of constitutionality and whether the foregone conclusion doctrine applies to compelled decryption to the Florida Supreme Court. *See Garcia*, 302 So. 3d at 1057 (recognizing conflict with Second District Court of Appeal and certifying questions).

93. *See Spicer*, 135 N.E.3d at 1291 (holding proper focus not on passcode but on evidence passcode protects). *But see In re* Grand Jury Subpoena to Boucher, No. 06-MJ-91, 2009 WL 424718, at *1-2 (D. Vt. Feb. 19, 2009) (holding foregone conclusion doctrine applied because government knew about files it sought); United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (concluding government knew of existence and location of computer's files). In both *In re Boucher* and *United States v. Fricosu*, although the foregone conclusion analysis focused on the evidence on the device, the courts held the compelled decryption was constitutional because the government had seen the files on the devices before they were encrypted. *See In re Boucher*, 2009 WL 424718, at *3-4 (holding Boucher could not claim privilege and must decrypt computer); *Fricosu*, 841 F. Supp. 2d at 1237 (indicating Fifth Amendment not implicated by compelled production).

94. *See Seo*, 148 N.E.3d at 955 (holding production of unlocked smartphone communicates breadth of information).

95. *See* Fisher v. United States, 425 U.S. 391, 410 (1976) (describing communicative aspects of producing evidence). The Court did not go into a detailed description of how it determined what an act admits, instead it focused on whether the admissions were testimonial. *See id.* (claiming difficult question whether tacit admissions both testimonial and incriminating). Sacharoff notes that all facts gleaned through acts are inferences, but none are entirely certain. *See* Sacharoff, *supra* note 57, at 70 (discussing how acts communicate facts).

96. *See* Seo v. State, 148 N.E.3d 952, 958 (Ind. 2020) (holding foregone conclusion exception not applicable). The detective investigating the stalking and harassment at issue in the case obtained a warrant to search the device for "incriminating evidence." *See id.* at 954 (describing warrant authorizing search of cell phone). The court took issue with the detective's testimony, which confirmed he was on a fishing expedition for information that he did not previously know. *See id.* at 958 (highlighting State failed to show existence of particular files). The detective testified in part:

> [T]here's probably some that I'm not even aware of, numerous entities out there like Google Voice and Pinger and Text Now and Text Me, and I don't know, I don't have an all-encompassing list of them, however if I had the phone I could see which ones she had accessed through Google.

Id. (demonstrating detective did not know what to look for on phone).

97. *See id.* at 962 (holding compelled decryption violates Fifth Amendment).

The court further disparaged the foregone conclusion doctrine, calling it a narrow exception and concluding that not only did it not apply to the facts at hand, but that it was generally unsuitable for the compelled production of a decrypted cell phone.[98] The court highlighted three concerns with extending the foregone conclusion doctrine: An unlocked cell phone is unlike specific business documents, there is no limit to the information available when producing a decrypted cell phone, and the Supreme Court has refused to extend other established doctrines to cell phones.[99]

2. The Argument that Compelled Decryption Is a Foregone Conclusion

On the other hand, several courts have allowed compelled decryption by shifting the focus of the foregone conclusion from the evidence sought on the device to the password protecting the device.[100] These courts have determined that the only assertion implicit in the act of decrypting a phone is that the actor knows the password, rather than an incriminating admission regarding the existence and possession of the files, or a testimonial act using the contents of the actor's mind.[101] In these cases, the foregone conclusion applies because the government seeks only the password.[102]

---

98. *See id.* at 958-59 (outlining three concerns with using foregone conclusion exception to compel decrypted device).

99. *See id.* at 958-62 (detailing concerns with extending limited exception). The court noted the ubiquity and capacity of smartphones, difficulty limiting access to information once the device is unlocked, and the recent Supreme Court precedent hesitating to extend existing doctrines to new technology. *See id.* at 958-61.

100. *See* State v. Andrews, 234 A.3d 1254, 1275 (N.J. 2020) (holding compelled production of password falls within foregone conclusion exception); United States v. Spencer, No. 17-CR-00259-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018) (holding government proved Spencer knew passwords and thus may compel him to decrypt); United States v. Apple MacPro Comput., 851 F.3d 238, 249 (3d Cir. 2017) (affirming district court order of contempt for not decrypting computer); State v. Stahl, 206 So. 3d 124, 136-37 (Fla. Dist. Ct. App. 2016) (focusing foregone conclusion on knowledge of passcode, claiming State did not request contents). A handful of courts have not shifted the focus of the foregone conclusion but have allowed compelled decryption because the government demonstrated that the government knew the evidence sought—the file, picture, or message on the device. *See* United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (holding government knew of files' existence and location); *In re* Grand Jury Subpoena to Boucher, No. 06-MJ-91, 2009 WL 424718, at *2 (D. Vt. Feb. 19, 2009) (holding government knew of existence and location of Z drive and its files).

101. *See* Commonwealth v. Jones, 117 N.E.3d 702, 710 (Mass. 2019) (holding compelled decryption conveys only defendant's knowledge of password and access to device). The court further clarified that entering a password into an encrypted device does not convey ownership of the device or contents, or control of its contents. *See id.* at 710 n.8 (clarifying holding from *Commonwealth v. Gelfgatt*). The court hypothesized a family member might know the password to another family member's cell phone but neither own nor control the cell phone. *See id.* (sharing examples of password entry not conveying ownership or control).

102. *See* Commonwealth v. Gelfgatt, 11 N.E.3d 605, 615-16 n.14 (Mass. 2014) (distinguishing entering encryption key from selecting and producing documents); *Jones*, 117 N.E.3d at 713 (requiring Commonwealth to prove defendant knows password beyond reasonable doubt before applying foregone conclusion doctrine); *Andrews*, 234 A.3d at 1274 (reasoning production of passcode compelled act thus foregone conclusion doctrine overcomes Fifth Amendment protection); *Stahl*, 206 So. 3d at 136 (holding State only requested passcode so passcode proper focus of foregone conclusion doctrine). These decisions do not address the evidence that law enforcement will no doubt find once they have an unlocked device. *See* Sacharoff, *supra* note 1, at 236 (calling application of foregone conclusion doctrine to passwords mistaken).

For example, in *Commonwealth v. Jones*, the SJC held that when the Commonwealth can establish that a defendant knows the password, the knowledge of the password is a foregone conclusion; therefore, the password can be constitutionally compelled.[103] Police arrested Jones for sex trafficking and found an LG phone on his person.[104] A judge denied the Commonwealth's initial motion to compel Jones to decrypt the LG phone; the SJC reversed, reasoning that police had demonstrated Jones knew the password and thus it was a foregone conclusion.[105] The SJC further clarified in a footnote "that the evidence at issue . . . is the password itself, not the contents of the phone."[106]

E. Applicability of Particularity Doctrine to Encrypted Digital Devices

Courts have similarly struggled to apply the Fourth Amendment particularity requirement to searches of digital devices.[107] Following *Fisher*, the Fourth Amendment no longer protects individuals against forced production of incriminating content in existing documents, however, it still theoretically forms the basis of protection against overbroad searches.[108] Unfortunately, few practical limits exist on what the government can search within a device, and once law enforcement officers have an accessible device in their possession, they frequently execute a thorough search of the entire device.[109]

Rule 41 of the Federal Rules of Criminal Procedure allows both the seizure of an entire device listed in the warrant and a later search of the copied data from

---

103. *See Jones*, 117 N.E.3d at 710 (applying foregone conclusion doctrine to compelled decryption).

104. *See id.* at 706 (reviewing background of case).

105. *See id.* at 706-07 (reviewing background of case and reversal of lower court's denial).

106. *See id.* at 711 n.10 (clarifying evidence at issue). The court acknowledged it was unclear in its prior analysis in *Gelfgatt*, where it concluded police demonstrated they knew the suspect knew the password, *and* they knew of files on the suspect's computers. *See id.* (acknowledging confusion around meaning of evidence); *Gelfgatt*, 11 N.E.3d at 615 (describing facts demonstrating foregone conclusion).

107. *See* Friess, *supra* note 64, at 975 n.21 (noting courts have struggled with uncertainty when applying Fourth Amendment to email searches); Bihter Ozedirne, Note, *Fourth Amendment Particularity in the Cloud*, 33 BERKELEY TECH. L.J. 1223, 1228 (2018) (claiming courts struggle to balance particularity and thoroughness regarding overcollection resulting from digital device seizure).

108. *See* Sacharoff, *supra* note 1, at 213 (noting *Fisher's* result: neither Fourth nor Fifth Amendment significantly protects against compelled production); Friess, *supra* note 64, at 991 (describing role of courts to consider probable cause and limit searches to suspected criminal activity).

109. *See* Gershowitz, *supra* note 11, at 600, 629 (claiming judges issuing warrants do not restrict where or how police may search device); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 7 (2015) (describing typical case where agents run forensic software on copy of device). Without limits, a warrant to search all data on a digital device resembles the general warrants the Framers intended the Fourth Amendment to prevent. *See* Gershowitz, *supra* note 11, at 601 (noting warrants authorizing search of "any and all data" on phone lack limits); Kerr, *supra*, at 1 (warning digital search process risks similarities to general warrants). A warrant may even allow police to search beyond the limits of the device by using saved passwords to log in to cloud accounts. *See* Seo v. State, 148 N.E.3d 952, 960-61 (Ind. 2020) (highlighting questions unbridled access to smartphones raise). Even warrants that restrict the types of data to be searched will include data types likely unrelated to the crime. *See* Gershowitz, *supra* note 11, at 589-90 (noting example of warrants for photographs in drug cases).

that seized device consistent with the warrant.[110] If officers have probable cause and a supporting warrant for one piece of incriminating information stored on a device, courts often will allow police the latitude to search every file on that device.[111] Understanding that a device can hold millions of files, photographs, apps, call logs, location logs, and provide a comprehensive record of a device owner's life makes it clear that unfettered government search capabilities have significant privacy implications, but courts have been reluctant to overturn such overbroad search warrants.[112]

In recent years, scholars have recognized that digital data storage exceeds anything the Founders could have imagined.[113] Existing doctrines, such as the third-party doctrine and the search-incident-to-arrest warrant exception, have failed to cover digital data, and the Court has recognized that in many cases, it needs a new approach to digital data protection.[114] For example, a modern cell phone holds more information about its owner's intimate moments, deepest insecurities, health, wealth, daily practices, and beliefs than any hoard of private papers the government could hope to find in an office or diary.[115] While limited in many cases by precedent, the Court does have the power to forge a new path when required, and it has been willing to do so when the privacy interests are

110. FED. R. CRIM. P. 41(e)(2)(B).

111. *See* Sacharoff, *supra* note 9, at 1646 (claiming current deviation from procedural safeguards).

112. *See* Stuart A. Thompson & Charlie Warzel, Opinion, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES: THE PRIVACY PROJECT (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/U9SM-932P] (describing what information location data provides); Riley v. California, 573 U.S. 373, 394 (2014) (claiming sixteen gigabytes translates to millions of pages of text and describing consequences for privacy); Gershowitz, *supra* note 11, at 600-14 (describing overbroad search warrants incorrectly upheld). Cell phones hold many distinct types of information that reveal more when viewed in aggregate than when viewed in isolation. *See Riley*, 573 U.S. at 394 (noting variety of information held in cell phones). Even one type of information—photographic, for example—may appear in such volume that it can allow law enforcement to reconstruct an individual's life. *See id.* (highlighting breadth of information held in cell phones). Furthermore, this information is collected over the life of the device, or longer, allowing the reconstruction of the past and present. *See id.* (noting continuous collection of information held in cell phones).

113. *See* Rangaviz, *supra* note 4, at 199 (noting password compulsion unimaginable from originalist perspective).

114. *See* Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 678 (2016) (claiming Fourth Amendment frameworks fail to cover privacy interests in digital world); Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018) (considering cell site location information (CSLI) unique kind of business record). The *Carpenter v. United States* opinion recalled that the Court has cautiously avoided "uncritically extend[ing] existing precedents" to new digital technology concerns. *See Carpenter*, 138 S. Ct. at 2222; *Riley*, 573 U.S. at 403 (holding search-incident-to-arrest exception to warrant requirement inapplicable to arrestees' cell phones); Kyllo v. United States, 533 U.S. 27, 36 (2001) (reasoning Court must address sophisticated technology in new rule). Justice Scalia, writing for the majority in *Kyllo*, asked the oft-cited question of "what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34.

115. *See Carpenter*, 138 S. Ct. at 2218 (emphasizing privacy risk of CSLI when owner brings phone into private spaces); Erik Sofge, *What Personal Data Stays on a Phone?*, CONSUMER REPS. (Mar. 23, 2016), https://www.consumerreports.org/cell-phones-services/what-personal-data-stays-on-your-phone-/ [https://perma.cc/39VW-9CTY] (noting level of detail of geographic data stored on smartphones); *see also* Rangaviz, *supra* note 4, at 199 (claiming data from phones never existed together, or at all, in founding era).

great.[116] Nevertheless, the Supreme Court has not yet defined what particularity means for electronic devices.[117] Cases like *Riley v. California* and *Carpenter v. United States* established new Fourth Amendment barriers to warrantless searches, but once police have obtained a warrant and a decrypted device, the particularity requirement is of little help to the device owner's privacy, as the entire device is open to legal search.[118]

III. ANALYSIS

A. Compelling a Suspect to Produce a Decrypted Electronic Device Violates the Fifth Amendment

1. Digital Device Contents Are Testimonial

Information extracted from a digital device cannot be considered the functional equivalent of traditional business documents, or even many boxes of business documents, because the digital device's contents are significantly more testimonial than the types of documents courts have previously considered.[119] The *Fisher* Court, in its decision to leave Fisher's tax documents unprotected and thus available to law enforcement, stressed that the papers contained no testimonial declaration from Fisher, and were even created by someone else—Fisher's accountant.[120] In contrast, a digital device can and often does hold "the privacies of life," similar to a diary, which the *Fisher* Court purposefully

116. *See* Rangaviz, *supra* note 4, at 204 (claiming Court put new limitations on old doctrines in *Riley* and *Carpenter*).

117. *See* Clark, *supra* note 5, at 2010 (noting Supreme Court has not defined particularity for cell phone searches).

118. *See* Riley v. California, 573 U.S. 373, 374 (2014) (holding government search of cell phone seized incident to arrest requires warrant); *Carpenter*, 138 S. Ct. at 2223 (holding government acquisition of CSLI requires warrant); Sacharoff, *supra* note 1, at 216 (claiming *Riley* established new Fourth Amendment principle for electronic data); Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 IOWA L. REV. 1125, 1128 (2011) (concluding, three years before *Riley*, password protection offered minimal legal protection); Brief for the American Civil Liberties Union Foundation of Massachusetts et al. as Amici Curiae in Support of the Defendant-Appellee at 37-38, Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014) (No. SJC-11358), 2013 WL 6002864, at *37-38 [hereinafter Amicus Curiae Brief] (arguing decryption of device also decrypts all files on device).

119. *See* Sacharoff, *supra* note 1, at 212 (noting papers in *Boyd* not personal or private). The cases that have applied the act-of-production doctrine have stated that incriminating contents of the documents are not protected under the Fourth Amendment. *See* United States v. Hubbell, 530 U.S. 27, 36 (2000) (clarifying Hubbell could not avoid compliance simply because documents incriminated him). The contents of a phone, however, rise to a new level of testimonial content beyond what courts in previous decisions have considered possible in a set of papers. *See* Fisher v. United States, 425 U.S. 391, 401 n.7 (1976) (noting subpoena of personal diary may raise issues of privacy where tax documents did not). Although the *Boyd* Court's reasoning regarding the Fourth Amendment has not stood the test of time, the Court felt at the time that the Fifth Amendment barred the compelled production of all private books and papers. *See* Boyd v. United States, 116 U.S. 616, 634-35 (1886) (declaring compulsion of books and papers equals compulsion to bear witness under Fifth Amendment).

120. *See Fisher*, 425 U.S. at 409 (stating Fisher neither prepared papers nor did they contain his testimonial declarations).

excluded from its holding.[121] Digital devices hold messages and emails, which often contain the owner's innermost private thoughts, memories, wishes, and beliefs.[122] Additionally, location tracking can provide a thorough mapping of the device owner's movements.[123] The contents of a cell phone or a personal laptop cannot be described as documents: They are utterly testimonial.[124]

Furthermore, the *Fisher* Court reasoned that the preparation of the tax documents in question was "wholly voluntary."[125] The same cannot be said of data on a cell phone or computer.[126] Voluminous logs are created as someone moves about their day, calls the doctor, pays a bill, or buys a cup of coffee.[127] Software and apps create many files automatically without the user's knowledge, such as location tags on pictures and location records that identify which cell phone towers the device connected to that day.[128] The device owner does not intend for the creation of vast stores of information, much less for the compulsion and use of such information against them in a court of law.[129] When law

121. *See Riley*, 573 U.S. at 403 (claiming modern cell phones hold privacies of life); Seo v. State, 148 N.E.3d 952, 959 (Ind. 2020) (noting smartphones pervasive and contain large amounts of information); *Fisher*, 425 U.S. at 401 n.7 (noting issues of privacy presented by subpoena of diary not presented by subpoena of tax documents). The *Riley* Court distinguished cell phones from a normal technological convenience because of all they may contain and reveal, noting that the small size and portability of the data did "not make the information any less worthy of the protection for which the Founders fought." *See Riley*, 573 U.S. at 403.

122. *See Riley*, 573 U.S. at 395-96 (distinguishing cell phone data from physical records); Friess, *supra* note 64, at 972 (noting similarity between innermost secrets and private conversations).

123. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (distinguishing between limited personal information previously considered and CSLI). In *Carpenter*, the Court declined to extend the third-party doctrine—an important search and seizure doctrine—to apply to CSLI, citing the different type of personal information provided by "the exhaustive chronicle of location information casually collected by wireless carriers today." *See id.* (reasoning reduced expectation of privacy in information shared with others did not apply to CSLI). The Court noted that mechanical application of the third-party doctrine failed to appreciate the revealing nature of CSLI. *See id.* (distinguishing checks and pen registers from CSLI in level of information revealed). The Court compared the third-party wireless carriers that collected the CSLI to a typical witness, such as a nosy neighbor. *See id.* (highlighting digital technology's seismic shift enabling detailed and ongoing location tracking). The Court stated wireless carriers are like a hyper-vigilant witness because "they are ever alert, and their memory is nearly infallible." *See id.* (noting exhaustive chronical of information available on cell phones).

124. *See* Nagareda, *supra* note 3, at 1642 n.254 (noting Supreme Court did not address Fifth Amendment status of very personal content like diaries); Commonwealth v. Davis, 220 A.3d 534, 549 (Pa. 2019) (noting Supreme Court did not address foregone conclusion doctrine beyond financial or business records).

125. *See* Fisher v. United States, 425 U.S. 391, 409 (1976) (stating record demonstrated documents created voluntarily).

126. *See Carpenter*, 138 S. Ct. at 2220 (asserting location information generated automatically and not voluntarily turned over to third party). Cell phones and their services are pervasive and owning a cell phone is required for participation in modern society. *See id.* (reasoning CSLI not shared in common meaning of term). Logs are created by default when the device is on, without any affirmative act from the user, who has no way to avoid creating this data without disconnecting from the network. *See id.* (noting user does not voluntarily assume risk).

127. *See* Donohue, *supra* note 114, at 554 (noting footprint individuals create in daily life); Thompson & Warzel, *supra* note 112 (describing movement logging using cell phones).

128. *See* Lekowski, *supra* note 7 (describing location information found on mobile devices); Sofge, *supra* note 115 (noting using maps, sending messages, uploading photos generates personal data).

129. *See* Donohue, *supra* note 114, at 647 (noting no meaningful choice whether or not to leave trail of data in today's world).

enforcement compels a device's decryption, they compel the vast stores of data within.[130] This data is not all voluntarily created, further distinguishing device decryption from the production analyzed in *Fisher*.[131]

Although the *Fisher* Court overturned *Boyd*'s protections of the contents of private papers, and *United States v. Doe* and *United States v. Hubbell* followed suit, all three of these cases only considered business or financial documents.[132] As the Court has indicated in other doctrinal areas, digital devices hold more personal and private content than papers ever could and are accordingly worth separate consideration.[133]

2. Decrypting a Digital Device Is a Testimonial Act

Even if the Court determines that the *contents* of a digital device are not sufficiently testimonial and thus never protected by the Self-Incrimination Clause, the *act* of decrypting a digital device is implicitly testimonial and should be protected under the Fifth Amendment.[134] The act of recalling and entering or disclosing a password requires use of the contents of an individual's mind.[135] Further, it implicitly communicates similar statements of fact as physical production, namely that the contents of the device exist, they are in the individual's control, and they are the evidence sought.[136]

---

130. *See* Amicus Curiae Brief, *supra* note 118, at 37 (claiming compelled decryption of drive equivalent to production of decrypted files).

131. *Cf.* United States v. Hubbell, 530 U.S. 27, 35-36 (2000) (holding voluntary creation of compelled documents not within meaning of privilege).

132. *See* Fisher v. United States, 425 U.S. 391, 391 (1976) (describing documents relating to tax return preparation); United States v. Doe, 465 U.S. 605, 608, 614 (1984) (questioning Fifth Amendment's application to business records); *Hubbell*, 530 U.S. at 45 (comparing to *Doe* subpoenas, which also sought business records); *see also* Commonwealth v. Davis, 220 A.3d 534, 549 (Pa. 2019) (highlighting limited application of foregone conclusion to financial or business documents).

133. *See* Riley v. California, 573 U.S. 373, 375 (2014) (distinguishing phone from isolated records).

134. *See Davis*, 220 A.3d at 548 (concluding act of revealing computer password not merely physical); Amicus Curiae Brief, *supra* note 118, at 23, (noting both federal and state case law equate decryption to testimony); Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614 (Mass. 2014) (claiming federal and Massachusetts law indicate decryption of device testimonial); Wareham, *supra* note 15, at 259 (claiming act of decrypting hard drive testimonial).

135. *See* Wareham, *supra* note 15, at 259 (noting attempt to force accused to disclose contents of his mind implicates Self-Incrimination Clause).

136. *See* United States v. Doe (*In re* Grand Jury Subpoena *Duces Tecum* Dated Mar. 25, 2011), 670 F.3d 1335, 1346 (11th Cir. 2012) (equating decryption to communication of knowledge and location of possibly incriminating files); Seo v. State, 148 N.E.3d 952, 955 (Ind. 2020) (holding production of unlocked cell phone communicates knowledge of password, existence, and possession of files). The *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011* court concluded "the decryption and production of the hard drives would require the use of the contents of Doe's mind and could not be fairly characterized as a physical act that would be nontestimonial in nature." *See In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d at 1346.

In *Fisher*, *Doe*, and *Hubbell*, the Court extensively discussed the implicit statements of fact that physical production of documents communicates.[137] Many commentators have maligned the difficulty of definitively determining what an act communicates.[138] They point out that because production is an act and not an oral statement, the actor is not intending to communicate; any consequential inferences are just that: inferences.[139] Nonetheless, the *Fisher* Court labeled three inferences resulting from the act of production as "tacit averments."[140] That the suspect is decrypting a phone rather than producing physical documents does not change the inferences about the relationship between the suspect and the evidence; the majority of scenarios will link the suspect to the evidence.[141]

3. A Digital Device Is Better Likened to a Tool or Weapon than Papers

Assuming the Court can overlook the privacy implications of compelling a suspect's phone and does not think the act of decryption communicates anything beyond knowledge of the password, it should still forbid compelled decryption because a phone is not a document, or even a collection of documents; it is a tangible object, easily analogous to a tool or weapon.[142] Some content on a digital device is written—messages, emails, and captions, for example—so it is natural to compare that content to documents.[143] A digital device, however, can also hold software that more closely analogizes to a tool in the physical world.[144]

---

137. *See Fisher*, 425 U.S. at 410 (discussing communicative aspects of producing evidence); *Doe*, 465 U.S. at 608, 614 (declining to overturn district court determining act communicated existence, possession, and authenticity of documents); United States v. Hubbell, 530 U.S. 27, 40 (2000) (noting disagreement focused entirely on significance of testimony inherent in production).

138. *See* Sacharoff, *supra* note 57, at 67 (describing nearly impossible task of determining implicit communication resulting from acts); Alito, *supra* note 35, at 46 (noting act-of-production theory abstract and difficult to apply).

139. *See* Sacharoff, *supra* note 57, at 69 (claiming all testimonial aspects of act amount to inferences). Sacharoff highlights the distinction between oral testimony and testimony given through an act and concludes that all communications garnered from an act are inferences. *See id.* (observing people must make inferences to glean implicit facts).

140. *See* Fisher v. United States, 425 U.S. 391, 410 (1976) (recognizing production of evidence had its own communicative aspects). The Court acknowledged that "[c]ompliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer." *Id.* Furthermore, compliance concedes "the taxpayer's belief that the papers are those described in the subpoena." *Id.*

141. *See* Sacharoff, *supra* note 57, at 67 (claiming unlocking device communicates ownership of device and possession of files).

142. *See* Riley v. California, 573 U.S. 373, 393 (2014) (noting cell phone functionality includes camera, rolodex, tape recorder, diary, television, and map).

143. *See* Donohue, *supra* note 114, at 557 (comparing right to privacy between email and traditional letter). Text messages resemble written notes, emails take the place of what otherwise might have been letters, and portable document format (PDF) files can be saved to a device or attached to emails. *See id.* at 556-57 (noting email replacing traditional types of communication like telephone calls and letters).

144. *See Riley*, 573 U.S. at 396 (describing mobile software applications (apps) offering range of tools for managing life information). The Court in 2014 claimed that the average smart phone had thirty-three apps

In some cases, the perpetrator of a crime may even use the device as a weapon, for example to harass or threaten someone on a social media app or hack into a video app to film under someone's clothing without their knowledge.[145]

If it is unconstitutional to require a suspect to procure a gun, even if police know the suspect possesses the gun, it follows that it is unconstitutional to require a suspect to procure their unencrypted phone, even if police know the suspect can decrypt it.[146] If courts extend the foregone conclusion doctrine to the compelled decryption of a phone, will they also allow officers to compel other types of evidence if the officers can prove the suspect possesses the evidence, or even allow officers to force a confession because the officers strongly believe the suspect is guilty?[147]

4. Knowledge of a Password Is Not the Focus of the Foregone Conclusion Doctrine

Focusing the foregone conclusion doctrine on the suspect's knowledge of the password rather than the government's knowledge of the sought evidence incorrectly applies the doctrine.[148] As defined in *Fisher*, and applied in *Doe* and *Hubbell*, the foregone conclusion doctrine asks whether law enforcement already knows the existence and location of the compelled papers.[149] In all three cases, the government compelled the papers and the critical evidence within; the existence and location of the papers were—or were not—the foregone conclusions.[150]

---

installed and that there were over a million apps available in app stores. *See id.* (discussing pervasive nature of apps).

145. *See* Liguori, *supra* note 14, at 334 (discussing cyber weapons, hacking tools, and systems vulnerabilities); Kerr, *supra* note 109, at 12 (referring to tools on cell phone used to hide data).

146. *See* Seo v. State, 148 N.E.3d 952, 958 (Ind. 2020) (describing investigator's confirmation he would fish for incriminating evidence if given access); Commonwealth v. Hughes, 404 N.E.2d 1239, 1244 (Mass. 1980) (holding production of revolver would incriminate suspect).

147. *See* Pardo, *supra* note 33, at 1888-89 (specifying government's knowledge should not dictate whether Fifth Amendment privilege applies).

148. *See* Nagareda, *supra* note 3, at 1599 (stating *Fisher*'s reliance on preexisting government knowledge to identify foregone conclusions speculative and unwieldy); Kiok, *supra* note 20, at 76 (claiming analogies to older technology do not reflect how encryption works).

149. *See* Fisher v. United States, 425 U.S. 391, 411 (1976) (stating foregone conclusion of existence and location of papers); United States v. Doe, 465 U.S. 605, 614 n.13 (1984) (stating government could have claimed foregone conclusion of possession, existence of papers but did not); United States v. Hubbell, 530 U.S. 27, 44 (2000) (holding government's foregone conclusion claim of existence and location deficient for lack of prior knowledge); *Compelled Decryption Primer*, *supra* note 54, at 2 (describing general rule of foregone conclusion exception).

150. *See* People v. Spicer, 125 N.E.3d 1286, 1290 (Ill. App. Ct. 2019) (arguing doctrine withholds Fifth Amendment protection when government knows compelled evidence's existence, location, and authenticity); *supra* note 149 and accompanying text (applying foregone conclusion doctrine).

Shifting the goal posts to require only proof that the suspect knows the device's password is disingenuous.[151] Many courts and scholars agree that using a password to unlock a device is analogous to producing documents so the government can search their contents.[152] The password itself is not the evidence, so proof that the password is known should not activate the foregone conclusion doctrine.[153]

As elaborated upon in *Hubbell*, the Fifth Amendment protects "compelled statements that lead to the discovery of incriminating evidence even though the statements themselves are not incriminating and are not introduced into evidence."[154] Entering a password, while surely not itself incriminating, will lead to the incriminating evidence the government seeks; therefore, the Fifth Amendment should protect the password.[155]

B. Compelling a Suspect to Decrypt an Electronic Device Without Particularity Violates the Fourth Amendment

Additional constitutional issues stemming from compelled decryption become apparent when considering the Fourth Amendment implications.[156] When police have probable cause to believe they may find evidence of a crime on a suspect's device, they can secure a search warrant to search the device and a court order to compel decryption if they cannot access the device.[157] Once police have access, they may perform an expansive search—often described as a fishing expedition—looking well beyond the information they had probable cause to search.[158] Although the particularity requirement of the Fourth Amendment forbids the type of general search that occurs when a government

151. *See Spicer*, 125 N.E.3d at 1291 (noting State seeking cell phone's contents rather than device password per se). The *Spicer* court specified that the proper focus is on the information the password protects, not the password itself. *See id.* (clarifying State sought decrypted information, not password).

152. *See* Seo v. State, 148 N.E.3d 952, 957 (Ind. 2020) (extending observations to compelled production); Commonwealth v. Davis, 220 A.3d 534, 548-49 (Pa. 2019) (holding foregone conclusion doctrine applies if government establishes knowledge of *evidence's* existence, possession, and authenticity); Sacharoff, *supra* note 1, at 237 (analogizing entering password to handing over documents).

153. *See Spicer*, 125 N.E.3d at 1292 (asserting State on fishing expedition and foregone conclusion doctrine thus not applicable).

154. *See* United States v. Hubbell, 530 U.S. 27, 37 (2000) (clarifying protection applies to statements leading to incriminating evidence).

155. *See Davis*, 220 A.3d at 543 (calling Fifth Amendment privilege broad because it protects compelled testimony leading to incriminating evidence).

156. *See* Sacharoff, *supra* note 9, at 1645-46 (drawing parallels between use of electronic devices and Framers' experiences).

157. *See* LAFAVE, *supra* note 64 (noting requirement of particularity closely linked to requirement of probable cause); Kerr, *supra* note 17, at 768 (asserting investigators seek court orders instructing suspects to produce decrypted version of data).

158. *See supra* note 109 and accompanying text (discussing likelihood of extensive search once device accessible and police obtain warrant); People v. Spicer, 125 N.E.3d 1286, 1292 (Ill. App. Ct. 2019) (holding State searching Spicer's phone without seeking specific information constituted fishing expedition).

searches a suspect's entire phone, there are no limits in practice.[159] This type of general search—the government rifling through a suspect's photos or systematically scanning their bank transactions—is no less repugnant to the American sense of privacy than when the government rifles through their bedroom drawers or home office.[160]

When a court forces a suspect to decrypt a device for police investigation, the general nature of the search that follows exacerbates the intrusiveness of the compelled act and does not ensure the government had prior knowledge of the vast array of evidence it received.[161] In essence, the search that follows compelled decryption violates the Fourth Amendment if there is no particularity.[162] Courts must not ignore the reality of the search that occurs once a suspect turns over an unencrypted device and the breadth of personal information that becomes available to law enforcement.[163]

C. Law Enforcement Has Other Options to Recover Device Data and Evidence Without Further Eroding Constitutional Rights

There are other ways to provide law enforcement with reasonable access to digital devices without stripping all citizens of their constitutional rights.[164] Legally obtaining digital evidence may be more costly or time consuming than compelling decryption, but the Constitution does not guarantee the government free access to any information it desires.[165]

1. Lawful Hacking

Many law enforcement agencies around the country already use one method of gathering encrypted evidence: state-sanctioned hacking.[166] Lawful hacking, as it is otherwise known, consists of members of law enforcement exploiting

159. *See supra* note 109 and accompanying text (noting lack of limits on government digital searches).

160. *See* Friess, *supra* note 64, at 1016 (asserting Fourth Amendment requires more limitations than those currently allowing digital rummaging); Gershowitz, *supra* note 11, at 629 (describing intrusion possible once officers possess device).

161. *See* Riley v. California, 573 U.S. 373, 393 (2014) (rejecting search of cell phone not intrusion beyond arrest itself); Kerr, *supra* note 109, at 20 (noting harm of overbroad searches magnified once computers store more and more information).

162. See Clark, *supra* note 5, at 1986 (describing particularity requirement).

163. *See* Kerr, *supra* note 109, at 20 (noting particularity requirement does not impose serious limits on searching electronics); Friess, *supra* note 64, at 980 (claiming search of email content more intrusive than wiretapping or video surveillance because more personal); Gershowitz, *supra* note 11, at 587 (noting cell phones hold enormous volume of personal data).

164. *See* Seo v. State, 148 N.E.3d 952, 962 (Ind. 2020) (emphasizing existence of additional methods of locating digital evidence without violating Fifth Amendment rights).

165. *See* Pardo, *supra* note 33, at 1881 (calling subpoenas efficient way for government to obtain evidence).

166. *See Seo*, 148 N.E.3d at 962 (naming companies with products available for police to enable access to locked devices); Nicas, *supra* note 83 (reporting law enforcement agencies in all fifty states have tools to get into encrypted phones).

system vulnerabilities or using malware to access a device's contents.[167] Lawful hacking can occur when an identified suspect denies police access to their device, when police possess a device with no identified owner, or when a suspect or victim is no longer alive to give consent or unlock the device.[168] No device is impenetrable.[169] Hacking can be slow and expensive, costing thousands of dollars per device and taking a few weeks or longer, and sometimes it does not even work.[170] Nevertheless, it has given investigators access into hundreds of thousands of phones that otherwise would have remained out of their reach.[171]

Although lawful hacking does not implicate the Fifth Amendment because it does not compel the suspect to assist in their own prosecution, lawful hacking raises Fourth Amendment issues regarding the search's reasonableness.[172] Privacy concerns and the issue of overbroad warrants are still relevant, but proper procedures could manage these concerns.[173]

2. Third-Party Warrants

Much of the information law enforcement seeks from the device may be found elsewhere, perhaps with a third party or otherwise saved in a location separate from the device, such as the cloud.[174] If a user enables the back-up function, photos, emails, contacts, and messages may be stored on a third party's cloud servers.[175] If police have probable cause to believe a third party possesses evidence of a crime, they can follow standard warrant procedures to require the third party to provide it.[176] Again, although obtaining the evidence from a third party removes the Fifth Amendment concerns, the Court has wrestled with the Fourth Amendment implications of accessing digital evidence through third

167. *See* Liguori, *supra* note 14, at 319 (defining "lawful hacking" or "government hacking").

168. *See* N.Y. CNTY. DIST. ATT'Y'S OFF., *supra* note 9, at 4 (identifying scenarios where police cannot obtain consent to search device).

169. *See* Nicas, *supra* note 83 (quoting Apple spokesperson).

170. *See id.* (explaining why hacking tools not panacea for encryption).

171. *See id.* (suggesting records show U.S. authorities searched hundreds of thousands of phones over past five years).

172. *See* Liguori, *supra* note 14, at 329 (acknowledging legal hacking raises complex issues, state must comply with fundamental rights and due process).

173. *See id.* at 329-32 (highlighting need to develop clear and legal procedural framework for lawful hacking). Liguori suggests many prerequisites and limitations, such as employing lawful hacking techniques only after less intrusive means fail, requiring warrants, and allowing only for investigating more serious crimes. *See id.* at 332 (suggesting structure in compliance with fundamental rights and due process in mind). Others have suggested a technical search protocol should accompany every digital search warrant to place essential constitutional limitations on the scope of digital searches. *See* Clark, *supra* note 5, at 2010 (asserting similar strict standards must apply to device searches and physical searches).

174. *See* Ozedirne, *supra* note 107, at 1231 (describing cloud computing and highlighting large amounts of data stored on cloud); Sofge, *supra* note 115 (asserting third parties own significant amount of personal data migrated to servers).

175. *See* N.Y. CNTY. DIST. ATT'Y'S. OFF., *supra* note 9, at 7 (listing various data sources and availability on third-party cloud servers).

176. *See* Seo v. State, 148 N.E.3d 952, 962 (Ind. 2020) (suggesting officers use Stored Communications Act to obtain data from third parties).

parties and has restricted the breadth of information that police can compel from third parties without a warrant.[177]

3. Summons for Particular Known Files

The government could also avoid the Fourth and Fifth Amendment issues associated with compelled decryption by—as in *Fisher*—compelling only those voluntarily created documents or files it can particularly identify in a warrant and has probable cause to believe exist on the device.[178] In these situations, compliance with the summons can once again be described as a question "not of testimony but of surrender."[179] A district court used this approach in *In re Boucher*, when an Immigration and Customs Enforcement agent viewed files with names suggestive of child pornography during a lawful border search, and later used a court order to compel those files only.[180] Absent restrictions on the search of the device following decryption, the search strays into overbroad and testimonial territory.[181]

IV. CONCLUSION

Current Fourth and Fifth Amendment doctrine regarding the compelled decryption of digital devices fails to consider how recent technology advances affect privacy interests. Several exceptions to the protections once established have watered down the alloy of the Fourth and Fifth Amendments, which was once a powerful declaration of the rights of an individual against a government who might abuse its powers. Enabling the government to compel decryption of a suspect's digital devices treads too far on the fundamental rights against self-incrimination and unreasonable search and seizure that Americans have come to expect. If this controversy is left to state and lower federal courts, the government may continue to exploit the foregone conclusion loophole, ignore

177. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (holding government request of detailed location data constituted search under Fourth Amendment). The *Carpenter* Court declined to extend the third-party doctrine to CSLI data, holding that acquiring CSLI data constituted a search requiring a warrant supported by probable cause. *See id.*

178. *See* Fisher v. United States, 425 U.S. 391, 410-11 (1976) (holding production of documents not testimonial self-incrimination). Once law enforcement has access to the device, courts and scholars have proposed solutions to minimize unnecessary intrusions beyond the warrant, through inventory of the files viewed or copied from the device, or strict protocols to limit the search. *See* Sacharoff, *supra* note 9, at 1699 (recommending courts insist on meaningful inventories of searched devices); Gershowitz, *supra* note 11, at 618, 621 (detailing growing search protocol use to minimize unnecessary intrusion and ensure warrant imposes boundaries).

179. *See Fisher*, 425 U.S. at 411 (quoting *In re* Harris, 221 U.S. 274, 279 (1911)) (describing circumstances under which testimony absent from document production).

180. *See In re* Grand Jury Subpoena to Boucher, No. 06-MJ-91, 2009 WL 424718, at *1-2 (D. Vt. Feb. 19, 2009) (summarizing factual background).

181. *See* Clark, *supra* note 5, at 2012 (noting limits of police discretion executing physical searches different than digital searches).

the particularity requirement for digital searches, and ultimately narrow fundamental Fourth and Fifth Amendment rights.

The Supreme Court must establish a new framework that fully considers the privacy implications of forced, invasive compulsion orders. The Founders forbade forced self-incrimination and restricted the government from rifling through every desk drawer and bookshelf in a person's home. The Court must similarly restrict forced cooperation to prevent unmitigated rifling through a person's digital device.