COMPELLED DECRYPTION & STATE CONSTITUTIONAL PROTECTION AGAINST SELF-INCRIMINATION

David Rassoul Rangaviz*

INTRODUCTION

Compelled decryption is the most important self-incrimination issue of the digital age. Almost everyone carries a phone on them at all times.[1] When someone is arrested while carrying a phone, the government must get a warrant before searching it.[2] Armed with a warrant, the government can search the phone. But if the phone is locked with an encrypted passcode, the government has two choices: hack in, or force the suspect to unlock it. The former is constrained only by the limits of the government's technical ability and resources. The latter is constrained by the self-incrimination provision of the Fifth Amendment to the United States Constitution, which prohibits any person from being "compelled in any criminal case to be a witness against himself . . . ."[3]

The scope of the Fifth Amendment protection against compelled decryption has "bedevil[ed] courts and scholars" alike.[4] "The scholarship on this question divides roughly between those who would interpret the Fifth Amendment as imposing a high bar to compelling a password and those who would interpret the Fifth Amendment as imposing a low bar."[5] This Article does not try to add to that debate, but instead seeks to change its focus. Unfortunately, all of these recent articles—and state courts that have considered this issue—have overlooked a separate source of protection against compelled self-incrimination: state constitutions.

---

* Staff Attorney, Committee for Public Counsel Services, Public Defender Division Appeals Unit. My thanks to Ian Bruckner, Abbe Dembowitz, and all of the editors at the *American Criminal Law Review* for their insightful comments and suggestions. My thanks also to the other members of the CPCS Appeals Unit, whose collective wisdom improves all of my work. Particular thanks, in this instance, must go to Patrick Levin, who first suggested that I dive into this topic. This article is for Rassoul Rangaviz, who almost certainly would not have read it, but would have been proud for its publication. © 2019, David Rassoul Rangaviz.

1. 95% of American adults own a cell phone, while 77% own a smartphone. *See* Mobile Fact Sheet, Pew Research Center for Internet and Technology (February 5, 2018), https://www.pewinternet.org/fact-sheet/mobile/. "According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." Riley v. California, 573 U.S. 373, 395 (2014).

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

3. U.S. CONST. amend. V.

4. Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 207 (2018) (footnote omitted).

5. Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 769 n.9 (2019) (collecting scholarship).

The government's ability to force a suspect to decrypt a phone is narrowed by corresponding state constitutional protections against self-incrimination, which are often phrased much more broadly than the Fifth Amendment. These distinct, expansive provisions are scarcely mentioned in compelled decryption litigation.[6] That is understandable because, despite the broad text of many state constitutional provisions against compelled self-incrimination, almost every state supreme court has followed in lockstep with the U.S. Supreme Court's Fifth Amendment doctrine when defining the relevant scope of its own constitution.[7] In Massachusetts, for example, that protection falls under article 12 of the Declaration of Rights, which provides that "[n]o subject shall . . . be compelled to accuse, or furnish evidence against himself."[8] Massachusetts law enforcement cannot enlist a suspect in unlocking his own phone, and thereby open its (potentially incriminating) contents for inspection, unless it complies with both the Fifth Amendment *and* article 12.[9]

On March 6, 2019, in *Commonwealth v. Dennis Jones*,[10] the Massachusetts Supreme Judicial Court ("SJC") became the first state supreme court to write the constitutional rules that govern compelled decryption.[11] In *Jones*, the SJC held that law enforcement can obtain a compelled decryption order so long as the government proves, beyond a reasonable doubt, that the suspect knows the passcode to the phone in question.[12] The court reasoned that article 12's self-incrimination clause only protects against the "testimonial" aspect of the act of decryption—just like the Fifth Amendment—and the only "testimony" implicit in the act of unlocking a phone is the suspect's statement: "I know the code."[13] But, according to the SJC, if the government *already* knows that the suspect knows the code, then the suspect has not incriminated himself at all, since he has just told the government something it already knows.[14] The suspect's knowledge of the passcode then becomes a "foregone conclusion" (in the language of federal doctrine)[15] and the government can compel the act of decryption because it gains no testimonial advantage from it.[16]

In its opinion, despite continuing to follow Fifth Amendment doctrine, the SJC emphasized the fundamental textual differences between the self-incrimination

---

6. Even a two-volume treatise dedicated to the subject of state constitutional law makes only a passing mention of the additional protections of state prohibitions against compelled self-incrimination. *See* 1 JENNIFER FRIESEN, STATE CONSTITUTIONAL LAW: LITIGATING INDIVIDUAL RIGHTS, CLAIMS AND DEFENSES § 12.02[2], at 12-6 (2006).

7. 1 MCCORMICK ON EVIDENCE PRACTITIONER TREATISE SERIES § 124 at 728 (Kenneth S. Broun ed., 7th ed. 2013).

8. MASS. DECL. OF RIGHTS art. 12.

9. *See id*.

10. 117 N.E.3d 702 (Mass. 2019).

11. *See* Kerr, *supra* note 5, at 768 n.4 (collecting cases).

12. *Jones*, 117 N.E.3d at 714.

13. *Id*. at 709–15.

14. *Id*. at 709.

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

16. *Jones*, 117 N.E.3d at 709–10.

clause of the Fifth Amendment and that of article 12.[17] Most importantly, the SJC cited the fact that "[a]rticle 12 protects a defendant from being compelled to 'furnish evidence' against himself or herself, as opposed to becoming 'a witness against' himself or herself" like the Fifth Amendment.[18] This was an odd textual hook for the court to hang its hat on, as the majority itself did not betray a hint of recognition that the entry of the passcode would result in the suspect "furnishing" a mountain of "evidence" that the government would then use against him. But this was not the fault of the *Jones* court; this error was set in motion decades ago.

The original sin in article 12 jurisprudence—as in nearly all other state courts[19]—is its needless, lockstep adherence to Fifth Amendment precedent. Under that precedent, state constitutional protection against self-incrimination is, like the Fifth Amendment, exclusively focused on protecting against compelled *testimonial* communication, and affords no protection at all against the compelled disclosure of documents.[20] But there is no reason that state constitutions should be read as narrowly as the Fifth Amendment when their language is often much broader.[21] As the text of article 12 makes plain, the Massachusetts state constitution is concerned with more than just compelling a suspect to serve as a testimonial witness against himself.[22] Unlike the Fifth Amendment, article 12 imposes a flat prohibition against a suspect being both "compelled to accuse" himself *and* being compelled to "furnish evidence" against himself.[23] The former seems to contemplate testimonial communications, while the latter plainly embraces documentary evidence. Unfortunately, this language—despite being repeatedly cited, as in *Jones*, to give article 12 a broader reading than the Fifth Amendment in a variety of contexts—has been functionally read out of article 12. The irony at the heart of article 12 precedent is that the SJC has repeatedly cited the words "furnish evidence" to give more expansive protection to criminal defendants than federal law requires, but it has never once actually considered what they mean.[24]

It does not have to be this way. This unfortunate error has only occurred as a result of an uncritical reliance on Fifth Amendment jurisprudence in Massachusetts's article 12 cases, a near-complete absence of originalist analysis of the proper scope of article 12, a disregard of the privacy concerns that animated the protection of the privilege in the first place, and a prioritization of the needs of

17. *See id.* at 714.

18. *Id.*

19. *See* 1 MCCORMICK ON EVIDENCE, *supra* note 7, at § 124, at 727–28.

20. *See id.; see, e.g.*, State v. Asherman, 478 A.2d 227, 240 (Conn. 1984) (rejecting argument that a prohibition on giving evidence extends beyond testimonial communications).

21. *See* 1 MCCORMICK ON EVIDENCE, *supra* note 7, at § 115, at 691 (noting that state courts are typically "focused upon the Supreme Court's construction of the Fifth Amendment's privilege," and that this focus is "unfortunate" for the development of state constitutional law).

22. *See* MASS. DECL. OF RIGHTS art. 12 ("No subject shall . . . be compelled to accuse, or furnish evidence against himself.").

23. *Id.*

24. *See, e.g.*, Commonwealth v. Burgess, 688 N.E.2d 439, 447–49 (Mass. 1997) (collecting cases).

law enforcement over the rights of defendants invoking the privilege. Building on that foundation, the *Jones* court started from the errant premise that article 12 does not protect the contents of a cell phone at all.[25] From that premise, which neither the litigants nor the SJC even questioned in *Jones*, the result was inevitable. If no one questions that premise in other state supreme courts, the same result will likely follow.

State courts and the defendants before them should start to scrutinize first principles. This Article uses the *Jones* case and article 12 as a cautionary tale for other state court litigants. *Jones* is instructive for litigation in other states because almost half of all state constitutions across the country have language nearly identical to that of article 12.[26] Massachusetts is a particularly clear case in which the state constitution calls for the protection of incriminating documents. The text of article 12 does not just protect against *either* the compelled furnishing of evidence *or* being forced to "accuse" oneself, but includes both protections.[27] To vindicate the full scope of the state constitutional privilege as it was intended and written, they must each be given meaning.[28]

This Article proceeds in three parts. Using Massachusetts as a case study, Part I explains the history that caused critical language of the Massachusetts state self-incrimination clause to be rendered a nullity. Part II dives into the SJC's jurisprudence on compelled decryption, including its recent decision in *Commonwealth v. Jones*, and explains how the SJC's opinion merely reflected the court's earlier error in narrowing the scope of article 12. It further explains the myriad problems with the SJC's approach to compelled decryption. Part III discusses the implications of a proper understanding of article 12 for law enforcement in other areas, highlighting why few other lines of cases would need to fall if the SJC redrew the line of article 12 protection. Nor would law enforcement be rendered unable to unlock encrypted phones altogether; it would just lose the easiest way in, forcing the police to reserve their decryption resources for the types of serious cases that call for the most invasive search practices.

Modern cell phones collect, in a single place, all of a person's most private information. The phones themselves contain voluminous personal information *and* serve as a gateway into all of our other private accounts that exist beyond the confines of the phone itself: email, social networking, banking, and more.[29] As a result, compelling a suspect to enter a phone's passcode forces him to aid the government's examination of the most intimate details of his life. When new technology allows such intrusive government practices, as the Supreme Court reminded us just

25. *See Jones*, 117 N.E.3d at 714.

26. *See infra* note 302.

27. *See* MASS. DECL. OF RIGHTS art. 12.

28. *See infra* Part I.C.

29. *See* BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD 48 (2018) ("You don't have to log in separately to your e-mail, Facebook, Tesla, or thermostat. The companies all assume that if you have access to your phone, you're you.").

last year, courts must be "careful not to uncritically extend existing precedents."[30] With such high stakes, now is the time to thoroughly examine the proper scope of state constitutional protections against compelled self-incrimination. Never have courts confronted such a mismatch between analog doctrine and digital reality. Self-incrimination jurisprudence remains myopically focused on testimonial evidence in a time of a massive expansion in our reliance upon, and generation of, documentary evidence. In Massachusetts, consistent with the text and history of article 12, the state constitution should not allow the expansive disclosure of private papers required by compelled decryption orders.

The SJC is among the very first state courts to consider the issue of compelled decryption. It will hardly be the last. In future cases, other state courts need not follow where the SJC has led. State supreme courts—nearly half of which have an identical constitutional prohibition against the compelled "furnishing" or "giving" of evidence—should conduct a thorough review of their own state constitutions to ensure they do not needlessly follow Fifth Amendment doctrine or the SJC's interpretation of article 12. To that end, litigants, like the courts themselves, must be mindful that each state constitutional claim deserves its own analysis, wholly distinct from that under the Fifth Amendment.

I. THE HISTORY OF ARTICLE 12 OF THE MASSACHUSETTS DECLARATION OF RIGHTS

This Part reviews the history of article 12 and Fifth Amendment jurisprudence and explains how the Fifth Amendment has come to be read as a narrow protection against the compelled disclosure of *testimonial* evidence only. It next explains how that interpretation of the Fifth Amendment jumped, uncritically, from federal court to the SJC as a matter of state constitutional interpretation. Finally, this Part discusses the correct meaning of article 12's prohibition against the compelled furnishing of evidence, which was intended to provide constitutional protection for the English common law privilege against self-incrimination. As explained in greater detail below, when article 12 was adopted in 1780, that common law privilege included protection against the compelled disclosure of private, incriminating documents, such as those found on a modern cell phone.

A. *The Evolution of Self-Incrimination Jurisprudence From* Boyd *to* Fisher

In his recent book, *51 Imperfect Solutions*, Sixth Circuit Judge Jeffrey Sutton explains the concept of "lockstepping" in state constitutional adjudication.[31] Lockstepping, Judge Sutton says, is "the tendency of some state courts to diminish their constitutions by interpreting them in reflexive imitation of the federal courts' interpretation of the Federal Constitution."[32] As Judge Sutton explains, there is no

30. Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).

31. JEFFREY SUTTON, 51 IMPERFECT SOLUTIONS 174 (2018).

32. *Id*. *See also id*. at 9 (noting how "[o]ne article after another talks about the second-tier status of state constitutional claims and the infrequency with which they are raised," and collecting articles to that effect).

good reason for this state of affairs. "State courts have authority to construe their own constitutional provisions however they wish."[33] Indeed, state constitutions have their own text, history, and purpose, and thus *should* be interpreted separately from the federal constitution. To avoid lockstepping, litigants must argue their cases under their state constitutions and take those arguments seriously. It is not enough to just make a federal constitutional argument and slap on a citation to the state provision.[34] Litigants and state courts must engage in "first-principle inquiries into the meaning of the state provisions," grapple with their meaning as distinct from federal law, and rely on all of the ordinary tools of constitutional interpretation.[35]

The SJC takes pride that the "Constitution of the Commonwealth preceded and is independent of the Constitution of the United States. In fact, portions of the Constitution of the United States are based on provisions in the Constitution of the Commonwealth . . . ."[36] And, of course, no one could accuse the SJC of pure "lockstepping" when it comes to article 12 doctrine. Be it the admissibility of breathalyzer evidence,[37] the minimum scope of immunity required to avoid self-incrimination problems,[38] or the standard of proof applicable to *Miranda* waivers,[39] the SJC has often diverged from federal law and raised the state constitutional floor to provide greater protection against self-incrimination to the citizens of the Commonwealth. Citing the "textual differences between art. 12 and the Fifth Amendment"—those differences noted in the introduction—the SJC has "consistently held that art. 12 requires a broader interpretation of the right against self-incrimination than that of the Fifth Amendment."[40]

But the SJC has been in lockstep with the Supreme Court in a much more fundamental sense: the court has never rigorously engaged with the text and history of article 12 to reach any of its rulings under that provision. Again and again, the SJC has simply heard the same substantive arguments previously aired in the Supreme Court and reached a different result (usually following the lead of a dissenting

33. *Id*. at 16.

34. *See id*. at 174 ("If there is a critical conviction of this book, it's that a chronic underappreciation of state constitutional law has been hurtful to state *and* federal law and the proper balance between state *and* federal courts in protecting individual liberty.").

35. *Id*. at 177.

36. Commonwealth v. Upton, 476 N.E.2d 548, 555 (Mass. 1985).

37. *Compare* Opinion of the Justices, 591 N.E.2d 1073 (Mass. 1992), *with* South Dakota v. Neville, 459 U.S. 553 (1983).

38. *Compare* Attorney General v. Colleton, 444 N.E.2d 915 (Mass. 1982), *with* Kastigar v. United States, 406 U.S. 441 (1972).

39. *Compare* Commonwealth v. Hoyt, 958 N.E.2d 834, 844 (Mass. 2011) (holding that "in Massachusetts proof of a valid waiver must be shown beyond a reasonable doubt"), *with* Colorado v. Connelly, 479 U.S. 157, 168 (1986) (holding that generally the government "need prove waiver only by a preponderance of the evidence").

40. Commonwealth v. Mavredakis, 725 N.E.2d 169, 178 (Mass. 2000) (citations and alterations omitted), *overruled on other grounds by* Commonwealth v. Smith, 28 N.E.3d 385 (Mass. 2015).

justice or group of justices).[41] The SJC habitually cites article 12's "furnish evidence" language to justify those higher standards, but it has never considered what those words actually mean for the scope of its protections. Were the court to grapple with the state constitutional text and history, it would see that "furnish evidence" means exactly what it says: suspects cannot be compelled to turn over incriminating documents for government inspection.[42]

Because of the SJC's lockstep adherence to Fifth Amendment precedent, one can only understand the current scope of article 12 by reviewing the history of federal interpretation of the Fifth Amendment.

In 1886, the Supreme Court in *Boyd v. United States* held that the Fifth Amendment forbids the government from compelling a person suspected of a crime from turning over self-incriminating documents.[43] *Boyd* was a case about broken glass. The government entered into a construction contract with defendants that allowed them to import glass duty-free.[44] The government grew suspicious when they imported a second, large shipment of glass duty-free, but the defendants claimed that an "enormous" quantity of the glass in the first shipment had broken in transit.[45] So the government subpoenaed the invoice for the first shipment and used it against the defendants in a forfeiture action.[46] The defendants objected, claiming that the compelled production of the invoice had violated the Fourth and Fifth Amendments.[47]

The Supreme Court agreed. Referring back to the original understanding of the Fifth Amendment, the Court reasoned that:

> [A]ny compulsory discovery by extorting the party's oath, *or compelling the production of his private books and papers*, to convict him of crime, or to forfeit his property, is contrary to the principles of a free government. It is abhorrent to the instincts of an Englishman; it is abhorrent to the instincts of an American. It may suit the purposes of despotic power, but it cannot abide the pure atmosphere of political liberty and personal freedom.[48]

The Court was explicit: the compelled production of incriminating private papers violates the Fifth Amendment. As the above text shows, *Boyd* is expansive in its language. It offers no hint that the Fifth Amendment is reserved only for

41. "There will never be a healthy 'discourse' between state and federal judges about the meaning of core guarantees in our American constitutions if the state judges merely take sides on the federal debates and federal authorities, as opposed to marshaling the distinct state texts and histories and drawing their own conclusions from them." SUTTON, *supra* note 31, at 177 (footnote omitted).

42. *See infra* Part I.C.

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

44. This description of the facts of *Boyd* is taken from an article written by Justice Alito, who reviewed the parties' briefs in the case to clarify the facts underpinning the dispute. *See* Samuel A. Alito, Jr., *Documents & the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27, 33 (1986).

45. *Id.*

46. *Id.*

47. *Id.*

48. *Boyd*, 116 U.S. at 631–32 (emphasis added).

"testimonial" communications. Whether *Boyd*'s holding was correct as a matter of Fifth Amendment doctrine is beyond the scope of this Article.[49] But it was plainly correct as a construction of a prohibition against "furnish[ing] evidence" under article 12, as discussed *infra* Part I.C.

The problem with *Boyd* arises in its discussion of the Fourth Amendment. The Court held that the compelled disclosure of the invoice was also an unreasonable government search and seizure under the Fourth Amendment, which, in turn, made it a violation of the Fifth.[50] With this framing, the two constitutional holdings appear dependent upon one another:

> [W]e are further of opinion that a compulsory production of the private books and papers of the owner of goods sought to be forfeited in such a suit is compelling him to be a witness against himself, within the meaning of the fifth amendment to the constitution, and *is the equivalent of* a search and seizure—and an unreasonable search and seizure—within the meaning of the fourth amendment.[51]

But this Fourth Amendment holding is incorrect. The government can seize private documents if it complies with the warrant and probable cause requirements.[52] There is no categorical prohibition on the seizure of private papers, just as there is no categorical prohibition on the seizure of a person.[53] And responding to a subpoena is not a search at all.[54] The government did not enter into the target's private property or invade his privacy; it forced him, by subpoena, to hand over documents. Consequently, no search had occurred.

Justice Samuel Miller recognized this distinction in a concurring opinion: "There is in fact no search and no seizure authorized by the statute. No order can

---

49. Mr. Jones has recently filed a petition for certiorari to the Supreme Court. *See* Jones v. Massachusetts, No. 19-6275 (petition filed October 16, 2019). I have filed an amicus brief in support of certiorari, on behalf of the Committee for Public Counsel Services, arguing that *Boyd* was correct as a matter of Fifth Amendment doctrine, drawing on many of the points made herein. *See* Amicus Brief of Committee for Public Counsel Services in Support of Petitioner, Jones v. Massachusetts, No. 19-6275 (filed October 24, 2019). *See also* Richard Nagareda, *Compulsion "To Be a Witness" and the Resurrection of* Boyd, 74 N.Y.U. L. REV. 1575, 1575 (1999) (arguing that *Boyd*'s Fifth Amendment holding was correct as a matter of federal law).

50. *See Boyd*, 116 U.S. at 621–22.

51. *Id*. at 634–35 (emphasis added).

52. *See* Alito, *supra* note 44, at 37–38.

53. *See* Nagareda, *supra* note 49, at 1588–89. *See also* Alito, *supra* note 44, at 35–41 (explaining the error of *Boyd*'s Fourth Amendment analysis). This error may be explicable by the fact that the privilege against self-incrimination was "linked to a right to be free from unreasonable searches and seizures" at the time the Federal constitution was written. LEONARD W. LEVY, ORIGINS OF THE FIFTH AMENDMENT: THE RIGHT AGAINST SELF-INCRIMINATION 390 (1968). At the time, it seems the execution of a general warrant was considered both an unlawful search *and* compelled self-incrimination. *See id*. at 390–92. This view may be incorrect by contemporary standards because a direct government search does not compel a suspect to hand over evidence, but it sheds some historical light on one thing: the privilege against self-incrimination was originally understood to extend to the sorts of private papers that are searched and seized in the execution of a general warrant. *See id*. at 391–93.

54. Alito, *supra* note 44, at 37–38.

be made by the court under it which requires or permits anything more than service of notice on a party to the suit."[55] All the court's order required was that the invoices "are to be produced in court, and, when produced, the United States attorney is permitted, under the direction of the court, to make examination in presence of the claimant, and may offer in evidence such entries in the books, invoices, or papers as relate to the issue."[56] The concurring justices rightly did not view this procedure as involving a search at all.[57] But, by conflating the scope of the Fourth and Fifth Amendments and making the two distinct holdings seem interdependent, the *Boyd* majority planted a seed of their demise that would later be used to narrow the Fifth Amendment. Although *Boyd* noted that "the Fourth and Fifth Amendments run almost into each other,"[58] it might be more accurate to say that *Boyd* had crashed the Fourth Amendment through the Fifth.

Boyd was also eroded over time by a line of cases involving bodily evidence. In *Schmerber v. California*, the Court held that the extraction of a blood sample from a defendant who was suspected of drunk driving implicated the Fourth Amendment but not the Fifth Amendment.[59] The Court there reasoned that the Fifth Amendment "protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature, and that the withdrawal of blood and use of the analysis in question in this case did not involve compulsion to these ends."[60] Under *Schmerber*, the Fifth Amendment does not protect suspects against the compelled taking of bodily evidence because that evidence is not itself "communicative" in nature.[61]

Schmerber thus seems to draw a clear line between "testimonial" evidence and all other types of evidence. But in drawing that distinction, the Court plainly contemplated that the pre-existing documents at issue in *Boyd* would fall comfortably on the "testimonial" side of that line. The *Schmerber* Court cited *Boyd* for that exact proposition, saying that "[i]t is clear that the protection of the privilege reaches an accused's communications, whatever form they might take, and the compulsion of responses which are also communications, for example, compliance

55. *Boyd*, 116 U.S. at 639 (Miller, J., concurring).

56. *Id.* at 640.

57. *See id.* at 639 ("There is in fact no search and no seizure authorized by the statute.").

58. *Id.* at 630.

59. Schmerber v. California, 384 U.S. 757, 760–72 (1966).

60. *Id.* at 761. The *Schmerber* Court was building on the intellectual roots of its opinion in *Holt v. United States*, 218 U.S. 245 (1910), which held that a defendant could be compelled to put on a garment believed to have been worn by a murderer while he was held in police custody. Justice Holmes drew the line between compelled "communications" and compelling the use of someone's body to produce physical evidence: "the prohibition of compelling a man in a criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material." *Id.* at 252–53. A series of cases after *Schmerber* "continued the division between testimonial or communicative evidence and physical evidence." Akhil Reed Amar & Renee B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857, 887 (1995) (collecting cases).

61. *Schmerber*, 384 U.S. at 761.

with a subpoena to produce one's papers."[62] Thus, "testimonial" evidence was meant to be synonymous with, or at least plainly include, "communicative" evidence like documents.[63] The *Schmerber* Court made clear that documentary subpoenas fell within the protections of the Fifth Amendment, while the provision of bodily evidence—including compelled fingerprinting, photographing, measurements, voice or handwriting exemplars, or wearing particular clothes—fell outside of its protection.[64] *Schmerber*'s definition of "testimonial" evidence expressly included, by direct citation back to *Boyd*, "compliance with a subpoena to produce one's papers."[65]

These twin foundations, the original error of *Boyd*'s Fourth Amendment holding and the intervening bodily evidence cases, laid the groundwork for *Boyd*'s overruling in *Fisher v. United States*.[66]

Fisher was a tax case.[67] The IRS suspected that certain people had cheated on their taxes and transferred tax documents to their accountants and attorneys, so the IRS issued a summons to the attorneys to get the documents.[68] It has since been taken for granted that *Fisher* overruled *Boyd* and seemingly allowed all documentary subpoenas,[69] but it is important to recognize the distinct context of that case: it involved documents prepared by accountants, for financial purposes, in the possession of the target's attorney.[70] The subpoena sought documents of a far less private character than those found on modern cell phones, and it sought them from a third party. Indeed, the Court started its analysis by noting that the summons had not been directly issued to the accused: "The taxpayer is the 'accused,' and nothing is being extorted from him."[71] And the Court expressly acknowledged that these

62. *Id*. at 763–64.

63. *See* Robert Heidt, *The Fifth Amendment Privilege and Documents—Cutting* Fisher*'s Tangled Line*, 49 MO. L. REV. 439, 456–57 (1984) ("*Boyd*, as reborn in *Schmerber*, qualified this generalization by excepting documents—one type of real or physical evidence, and one type of property. Documents could still be suppressed, regardless of their author, apparently on the ground that they contain communications.").

64. *See Schmerber*, 384 U.S. at 763–64.

65. *Id*. at 764.

66. 425 U.S. 391 (1976). To be precise, *Fisher* overruled *Boyd* in all but name. "Although the Supreme Court has never expressly overruled *Boyd* and squarely held that the contents of all voluntarily created documents are outside the ambit of the Fifth Amendment, the Supreme Court's application of the Fifth Amendment since *Fisher* confirms that the only Fifth Amendment privilege applicable to demands for documents is an 'act of production' privilege." STEVEN M. SALKY & PAUL B. HYNES, JR., THE PRIVILEGE OF SILENCE: FIFTH AMENDMENT PROTECTIONS AGAINST SELF-INCRIMINATION 236 (2d ed. 2014). *See also* United States v. Doe, 465 U.S. 605, 618 (1984) (O'Connor, J., concurring) (stating her view "that the Fifth Amendment provides absolutely no protection for the contents of private papers of any kind," and that *Fisher* "sounded the death-knell for *Boyd*").

67. *See generally* Fisher v. United States, 425 U.S. 391 (1976).

68. *Id*. at 393–94.

69. *See, e.g.*, Kerr, *supra* note 5, at 773–76 (discussing *Fisher*'s narrowing of Fifth Amendment protection and its creation of the foregone conclusion exception at length, with no appreciation, or even recognition, of the financial or third-party character of the documents actually at issue in *Fisher*).

70. *Fisher*, 425 U.S. at 394.

71. *Id*. at 398.

were business and financial records, citing the "[s]pecial problems of privacy" that arise when a subpoena seeks private papers.[72]

In analyzing the scope of Fifth Amendment protections, the Court noted that "[s]everal of *Boyd*'s express or implicit declarations have not stood the test of time."[73] First, its Fourth Amendment holding was inconsistent with certain of the Court's recent cases.[74] If the Fourth Amendment were as categorical as *Boyd* suggested, "its protections would presumably not be lifted by probable cause and a warrant or by immunity."[75] That aspect of *Boyd*, as noted above, was indeed wrong. The government may directly seize a person's private papers (without compelling disclosure by the suspect) if it complies with the warrant and probable cause requirements. And, as noted, a subpoena is not even a search. But, because *Boyd* made its Fourth and Fifth Amendment rulings appear interrelated, the error of one would seem to suggest (if not demand) the correction of the other. As the *Fisher* Court explained: "To the extent . . . that the rule against compelling production of private papers rested on the proposition that seizures of or subpoenas for 'mere evidence,' including documents, violated the Fourth Amendment and therefore also transgressed the Fifth, the foundations for the rule have been washed away."[76]

The Court then moved on to the bodily evidence cases. Citing *Schmerber*—while ignoring the fact that *Schmerber* had expressly reaffirmed the precise holding of *Boyd* that the Court was about to upend—the *Fisher* Court announced that it was "also clear that the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence . . . ."[77] Instead, it "applies only when the accused is compelled to make a Testimonial Communication that is incriminating."[78] But the Court then unilaterally redefined what *Schmerber* meant by "testimonial communications." The only compulsion

---

72. *Id*. at 401 n.7. The Supreme Court "has never considered the foregone-conclusion exception outside of cases involving specific, preexisting business and financial records." Brief of Amici Curiae Electronic Frontier Foundation & ACLU at 15, Seo v. State, No. 18S-CR-595 (Ind. Jan. 1, 2019). The Court has instead, on multiple occasions, "pointedly le[ft] th[e] question open" of whether the Fifth Amendment protects against the compelled disclosure of private papers such as diaries. *See* Amar & Lettow, *supra* note 60, at 888 n.144 (collecting cases). It is thus surprising that the act of production doctrine and foregone conclusion exception have been so uncritically extended into the context of orders involving the most private aspects of people's lives that are found on modern smartphones—photos, emails, calls, texts, and location records—without courts (or litigants) taking any pause to consider why private papers have always been carved out from past holdings of the Court.

73. *Fisher*, 425 U.S. at 407.

74. *See id*. at 407–08.

75. *Id*. at 400.

76. *Id*. at 409 (citation omitted).

77. *Id*. at 408.

78. *Id*. The doctrinal distortions caused by reliance on the bodily evidence cases in the document subpoena context may have been nothing more than the historical happenstance that those cases came first. "The Court decided the bodily evidence cases before it addressed the treatment of self-incriminatory documents in *Fisher*. As a result, the misleading focus in the bodily evidence cases on the presence of testimonial communication had become an entrenched part of Fifth Amendment case law by the time of *Fisher* and, not surprisingly, led the Court in that case down the wrong analytical path." Nagareda, *supra* note 49, at 1630.

that matters, according to *Fisher*, is whether the accused is being forced to make a *contemporaneous* testimonial assertion when responding to the subpoena or court order.[79] *Schmerber*'s two-part protection against compelled testimony *or* communications was suddenly narrowed, with a barely-audible tweak, to the single category of just testimoni*al* communications.[80] Under *Fisher*, the protection against self-incrimination does not extend to the contents of documents that pre-exist the act of governmental compulsion.[81] That is because, as *Fisher* says, a subpoena for pre-existing documents:

> [D]oes not compel oral testimony; nor would it ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought. Therefore, the Fifth Amendment would not be violated by the fact alone that the papers on their face might incriminate the taxpayer, for the privilege protects a person only against being incriminated by his own compelled testimonial communications.[82]

Because the preparation of these documents was "wholly voluntary," they did not contain compelled testimonial evidence of the sort that the Fifth Amendment, as *Fisher* rewrote it, is now concerned with.[83]

Fisher's inventive holding was dubbed the "act of production" doctrine: in the context of a subpoena for documents, the Fifth Amendment only protects the testimonial assertions that are implicit in the actual "act of producing" the documents, but not the documents themselves.[84] For instance, when someone hands over documents in response to a subpoena, they "tacitly concede[] the existence of the papers demanded and their possession or control by the [person handing them over]."[85] This was a far narrower view of Fifth Amendment protection than *Boyd* had established.[86] But were that the entirety of *Fisher*'s holding, it would seem, in practice, to be almost as protective as *Boyd*—even the more limited testimonial act of production would not permit compelled disclosure of private papers.[87]

---

79. *See Fisher*, 425 U.S. at 409–10 (emphasizing that "the preparation of all of the papers sought in these cases was wholly voluntary, and [so] they cannot be said to contain compelled testimonial evidence").

80. *See* Schmerber v. California, 384 U.S. 757, 761 (1966).

81. *See Fisher*, 425 U.S. at 409–10.

82. *Id.* at 409.

83. *Id.*

84. *See* Kerr, *supra* note 5, at 772 ("The act of production doctrine was first adopted in *Fisher*.").

85. *Fisher*, 425 U.S. at 410.

86. *Compare Boyd*, 116 U.S. at 634–35 ("[A] compulsory production of the private books and papers . . . is compelling him to be a witness against himself."), *with Fisher*, 425 U.S. at 410 ("[T]he privilege protects a person only against being incriminated by his own compelled testimonial communications. . . . The taxpayer cannot avoid compliance with the subpoena merely by asserting that the item of evidence which he is required to produce contains incriminating writing, whether his own or that of someone else.").

87. Indeed, this seems to be why Justice Marshall missed the massive implications of *Fisher*'s rewriting of the scope of Fifth Amendment protection. In a separate concurrence, Marshall noted that he "would have preferred it had the Court found some room in its theory for recognition of the import of the contents of the documents themselves." *Fisher*, 425 U.S. at 432 (Marshall, J., concurring in judgment). But, despite those misgivings, he was still "hopeful that the Court's new theory, properly understood and applied, will provide substantially the

To avoid this result, the *Fisher* Court established both the "act of production" doctrine and an exception to it: the "foregone conclusion" doctrine.[88] This exception provides that if the government can prove that it *already* knows about the existence and location of the papers, then any testimonial aspect of the act of production becomes a "foregone conclusion" and the suspect "adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers."[89] The government obtains no testimonial advantage—distinct from its obvious evidentiary advantage—from forcing a suspect to tell it something that it already knows.[90] "To apply the foregone conclusion doctrine, courts look at what the government knows before the act is compelled and ask whether the testimony implied by a compelled act is 'in issue' and would add to the government's case."[91] Under *Fisher*, "[a] valid privilege exists only when the compelled act is testimonial under the act of production doctrine but is not a foregone conclusion."[92]

By highlighting the clear error of *Boyd*'s Fourth Amendment holding and using the gist (while ignoring the text) of the bodily evidence cases, the *Fisher* Court made a fundamental change to the scope of Fifth Amendment protections. So long as the government can establish that it already knows any *testimony* implicit in an act of production, making that testimony a "foregone conclusion," it can compel criminal suspects to turn over their most private papers even if it knows little about the contents of those documents.[93]

---

same protection as our prior focus on the contents of the documents." *Id.* According to Justice Marshall, the Court's recognition of the testimonial aspects of an act of production "seems to me to afford almost complete protection against compulsory production of our most private papers." *Id.* Marshall believed that the analysis called for by the foregone conclusion exception to the act of production doctrine would roughly track the intrusiveness of the document request. In Marshall's view, this analysis would generally allow subpoenas of corporate documents while protecting private papers from compelled disclosure because "the existence of corporate record books is seldom in doubt" whereas "there is little reason to assume the present existence and possession of most private papers." *Id.* "Thus, in practice, the Court's approach should still focus upon the private nature of the papers subpoenaed and protect those about which *Boyd* and its progeny were most concerned." *Id.* at 433. Of course, Justice Marshall's hope about how *Fisher* would apply to private documents was entirely upended by the approach to compelled decryption taken by the SJC in *Jones*, as it removes the protection of the "reasonable particularity" standard that Marshall assumed would work in practice to ensure protection for private papers.

88. *See* Kerr, *supra* note 5, at 776–78 (explaining the alleged need for the foregone conclusion exception to the act of production doctrine).

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

90. *See id.*

91. Kerr, *supra* note 5, at 773.

92. *Id.*

93. *See id.*; *Fisher*, 425 U.S. at 411. While conducting a lengthy exposition of the meaning of the Fifth Amendment, the Court also noted at the end of its opinion that "[w]hether the Fifth Amendment would shield the taxpayer from producing his own tax records in his possession is a question not involved here; for the papers demanded here are not his 'private papers.'" *Fisher*, 425 U.S. at 414, citing *Boyd*, 116 U.S. at 634–35. Again, *Fisher* involved business records in the hands of a third party, but has been uncritically extended to private papers sought directly from the suspect.

B. *The SJC Follows in Lockstep with the Supreme Court*

The SJC was quick to borrow from *Fisher* just four years later. In *Commonwealth v. Hughes*, the defendant was held in contempt for failing to produce a gun pursuant to a court order.[94] The SJC concluded that production of the weapon would require implicit testimonial statements about its existence, location, and control, and thus the contempt order was improper.[95] Analyzed solely under the Fifth Amendment,[96] the case was a straightforward application of *Fisher*'s act of production doctrine and foregone conclusion exception.[97] Because the Commonwealth had obtained a court order for a compelled act of production without establishing its knowledge of the testimony implicit in the act, the foregone conclusion exception was inapplicable.[98] While reiterating *Fisher*'s holding about the scope of the Fifth Amendment, *Hughes* said little about article 12.[99]

Two years later, in *Commonwealth v. Brennan*, the court confirmed that Massachusetts would follow *Fisher*'s lead on the scope of self-incrimination protection.[100] *Brennan* involved breathalyzer tests, which drivers in Massachusetts are required to take or risk suspension of their licenses.[101] The SJC held that article 12 was not implicated by these tests because "the framers of our Declaration of Rights did not contemplate that art. 12 apply to real or physical evidence, the production of which would have no inherently communicative value."[102]

Like *Schmerber*, *Brennan* involved compelled bodily evidence—the results of breathalyzer tests—so it could easily have narrowed the protection of article 12 to "testimonial or communicative" evidence without eliminating protection for preexisting documents, just as the Supreme Court had done in *Schmerber*.[103] The SJC's language, however, went much further, setting out a false historical premise for which it cited no evidence.

First, the court held that the article 12 privilege was meant as a "restate[ment of] the common law rule against self-incrimination,"[104] which is true (as explained *infra* Part I.C). But in doing so, the court failed to recognize that every

94. Commonwealth v. Hughes, 404 N.E.2d 1239, 1241 (Mass. 1980).

95. *Id.* at 1244.

96. The SJC merely dropped a footnote noting that "[a]lso involved are the corresponding provisions of the Constitution of the Commonwealth, art. 12 of the Declaration of Rights." *Id.* at 1241 n.3. At the end of its opinion, the court similarly noted that "[o]ur result, were it not dictated, as we think it is, by the Fifth Amendment, would in our view be required by the rather clearer terms of the Constitution of the Commonwealth." *Id.* at 1246 (citation omitted).

97. *See Fisher*, 425 U.S. at 410–11.

98. *Hughes*, 404 N.E.2d at 1244.

99. *See id.* at 1241 n.3 (noting, in the Court's only mention of art. 12, that "[a]lso involved are the corresponding provisions of the Constitution of the Commonwealth, art. 12 of the Declaration of Rights").

100. Commonwealth v. Brennan, 438 N.E.2d 60 (Mass. 1982).

101. *Id.* at 61–62.

102. *Id.* at 65–66.

103. *See Schmerber*, 384 U.S. at 773.

104. *Brennan*, 438 N.E.2d at 65–66.

commentator regards the common law privilege as including protection against compelled production of private papers.[105]

Instead, the SJC claimed that the common law privilege "was directed toward the forced extraction of confessions and admissions from the lips of the accused."[106] But that historical assertion—which insinuates that the article 12 privilege narrowly protects only against compelled testimony (i.e., "from the lips") that is *highly* incriminating (i.e., "confessions or admissions")—was plainly incorrect. It directly contradicted both Supreme Court and SJC precedent, which recognize that the protection against compelled self-incrimination does not depend at all on the *extent* to which the compelled disclosure would incriminate the suspect.[107] Indeed, the SJC had previously considered and rejected that exact contention: "Both the reason upon which the rule is founded, and the terms in which it is expressed, *forbid* that it should be limited to confessions of guilt, or statements which may be proved, in subsequent prosecutions, as admissions of facts sought to be established therein."[108] That might be the core of the right, but "these were not the whole of its functions."[109] The privilege applies not only to forced confessions, but also to *any* evidence that "would furnish a link in the chain of evidence needed to prosecute the claimant."[110] Neither the common law privilege nor the contemporaneous understanding of the scope of article 12 protection was nearly so narrow as the court claimed.

Starting from this errant premise, the SJC followed *Fisher* in lockstep, holding that article 12 does not apply to "noncommunicative evidence" such as the breathalyzer test results at issue in *Brennan*.[111] And its language and reasoning suggested the same for pre-existing documents.[112] The court emphasized that a contrary rule could harm the interests of law enforcement:

---

105. *See, e.g.*, Nagareda, *supra* note 49, at 1619. *See also id.* at 1619 n.172 (noting that "[a]ll sources to address the point concur" that the common law privilege applied to compelled documentary disclosures). This is discussed in greater detail *infra* Part I.C.

106. *Brennan*, 438 N.E.2d at 66.

107. *See* Hoffman v. United States, 341 U.S. 479, 486 (1951) ("The privilege afforded not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime."); Blaisdell v. Commonwealth, 364 N.E.2d 191, 197–98 (Mass. 1977) ("Where the privilege is applicable, the constitutionally required result is that no balancing of State-defendant interests is permissible to facilitate the admittedly difficult burdens of the prosecution. . . . The protection of the constitutionally protected privilege is not one that yields to 'reasonable' intrusions.").

108. Emery's Case, 107 Mass. 172, 182 (1871) (emphasis added).

109. LEVY, *supra* note 53, at 430.

110. *Hoffman*, 341 U.S. at 486. *See also* Commonwealth v. Freeman, 817 N.E.2d 727, 733 (Mass. 2004) ("This privilege extends not only to answers that would in themselves support a conviction, but also to those that would furnish a link in the chain of evidence needed to prosecute the witness.").

111. *Brennan*, 438 N.E.2d at 66–67.

112. *Id.* at 66 ("[T]he privilege was directed toward the forced extraction of confessions and admissions from the lips of the accused.").

> The refusal of most courts to adopt an expansive interpretation of the privilege has undoubtedly stemmed in part from a concern for the severe constraints on law enforcement practices that would otherwise result, and from the fact that compelled production of physical evidence is far less offensive to common standards of decency. We conclude that art. 12 of the Declaration of Rights applies only to evidence of a testimonial or communicative nature, and that neither a breathalyzer test nor field sobriety tests are communicative to the extent necessary to evoke the privilege.[113]

It was an odd turn—a purportedly originalist analysis of article 12 that seemed most concerned with how contemporary law enforcement might be impacted by a rule forbidding compelled self-incrimination. These were hardly the concerns that animated the drafters of article 12 or the Fifth Amendment, as explained *infra* Part I.C.

But *Brennan*'s holding has never been critically re-examined. Again and again, including in cases where the SJC has applied heightened protection for criminal defendants under the state constitution, the court has reaffirmed the limited scope of article 12. For instance, in *Attorney General v. Colleton*,[114] the SJC held that broader "transactional" immunity was required to avoid a violation of article 12, raising the level of immunity required by the Fifth Amendment.[115] In so doing, the court emphasized that article 12's "furnish evidence" language, while occasionally justifying heightened protections, still "does not change the classification of evidence to which the privilege applies."[116] It did not explain why. Likewise, in *Commonwealth v. Burgess*,[117] the SJC recognized that it had often deviated from federal law, but said that "[n]one of these differences from the [f]ederal standards indicated a departure from the crucial distinction between testimonial and physical evidence."[118] Again, it offered no explanation. Indeed, this principle was so baked in that the defendants in *Burgess* did not even "argue that art. 12 protects them from yielding any nontestimonial evidence."[119] The limited scope of article 12 protection was then, and has since, just been taken as a given by litigants and the court.

To summarize, the SJC narrowed the scope of article 12 in lockstep with the Supreme Court. It did so by borrowing its reasoning wholesale from *Fisher*, which itself overruled *Boyd* by relying upon the error of *Boyd*'s Fourth Amendment

---

113. *Id.* at 67.

114. 444 N.E.2d 915 (Mass. 1982).

115. The Supreme Court had earlier held that the more limited "use" immunity sufficed to avoid a violation of the Fifth Amendment. *See* Kastigar v. United States, 406 U.S. 441 (1972).

116. *Colleton*, 444 N.E.2d at 919.

117. 688 N.E.2d 439 (Mass. 1997).

118. *Id.* at 448. However, the court also recognized the textual differences between the two provisions and at least intimated that those differences could reflect a different scope of protection. "Under the Fifth Amendment only compelled *communication that is testimonial* and potentially incriminating is precluded by the privilege against self-incrimination, and under art. 12 compelled *communication that furnishes evidence* is precluded." *Id.* at 442 (citations omitted, emphasis added).

119. *Id.* at 448.

holding, not recognizing that its Fifth Amendment ruling could stand on its own.[120] The *Fisher* Court then cited a line of bodily evidence cases that had themselves expressly reaffirmed that private papers remained beyond the reach of compelled disclosure.[121] *Fisher* purported to follow those cases, but it placed documentary subpoenas on the wrong side of the line. It recast a protection reserved for all of "an accused's communications, whatever form they might take,"[122] as one intended only for the narrower category of "*testimonial* communications."[123] The Supreme Court has never acknowledged that sleight of hand. Admittedly, the Court redrew the line in a case that involved business and financial records in the hands of third parties, but *Fisher* has since been read to place *all* pre-existing documents outside of protection, regardless of their private character or whether they are sought directly from the suspect.[124]

For its part, the SJC claimed to read article 12 consistently with the scope of the common law privilege, but it has never grappled with the historical evidence around that privilege in a rigorous way. Instead, to reach its result, the court merely asserted that the common law privilege was chiefly concerned with forced confessions. But that is contradicted by every single case—even many of the SJC's own—about the extent of incrimination necessary before a defendant may invoke the privilege: a defendant may not be compelled to furnish *any* link in the evidentiary chain that would aid in his prosecution, not just the final link.

As explained below, this lockstep following of *Fisher* is inconsistent with the correct, intended scope of article 12 protection.

C. *The Proper Scope of Article 12 Includes Protection Against Compelled Disclosure of Pre-Existing Private Papers*

The original understanding of the Fifth Amendment informs that of article 12. In his recent dissent in *Carpenter v. United States*,[125] Justice Gorsuch recognized that "there is substantial evidence that the privilege against self-incrimination was also originally understood to protect a person from being forced to turn over potentially incriminating evidence."[126] Justice Thomas, joined by Justice Scalia, has said the same.[127] Justice Souter, joined by Justices Stevens and Ginsburg, has described the notion that the Fifth Amendment "does not address the admissibility of

120. *See Burgess*, 688 N.E.2d at 448-49 (citing *Fisher* and replicating its analysis for art. 12 purposes).

121. *See* Fisher v. United States, 425 U.S. 391, 408 (1976).

122. Schmerber v. California, 384 U.S. 757, 763–64 (1966).

123. *Fisher*, 425 U.S. at 409 (emphasis added).

124. *See supra* note 66.

125. 138 S. Ct. 2206 (2018).

126. *Id.* at 2271 (Gorsuch, J., dissenting).

127. *See* United States v. Hubbell, 530 U.S. 27, 49 (2000) (Thomas, J., concurring) ("A substantial body of evidence suggests that the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence."). If one considers that the same view was held by Justice Brennan, as shown by his separate concurrence in *Fisher*, there is considerable support for this view across the ideological spectrum. *See Fisher*, 425 U.S. at 414–30 (Brennan, J., concurring in judgment).

nontestimonial evidence" as an "overstatement."[128] This is because the Fifth Amendment was simply intended to constitutionalize the then-existing common law privilege, much like the SJC has held out as the purpose of article 12.[129]

Ironically, given the current scope of Fifth Amendment protection, there is a considerable consensus that the English common law privilege at the time of the adoption of the Fifth Amendment and article 12 barred the compelled production of incriminating documents. Justice Brennan said exactly that in his concurrence in *Fisher*, collecting cases from the King's Bench: "Without a doubt, the common-law privilege against self-incrimination in England extended to protection against the production of incriminating personal papers prior to the adoption of the United States Constitution."[130] Justice Alito said the same in a 1986 law review article, citing much of the same authority.[131] "The crucial historical observation—one not seriously disputed by the Supreme Court, legal commentators, or historians on the subject—is that the common law at the time of the Bill of Rights specifically recognized a privilege against self-incrimination by way of documents."[132]

The most extensive treatment of the issue in the common law cases can be found in *King v. Purnell*.[133] In that case, the English government sought to order Oxford University to produce its records for inspection so the government might obtain incriminating material against the university's vice-chancellor.[134] The vice-chancellor possessed the documents in question, so the order would have required him to turn over materials that would incriminate himself.[135] The King's Bench refused to issue the order, reasoning that "[t]he books were of a private nature" and "[g]ranting such rule would be to make a man produce evidence against himself, in a criminal prosecution."[136] Indeed, the Court stated that it knew of "no instance, wherein this [c]ourt has granted a rule to inspect books in a criminal prosecution

128. United States v. Patane, 542 U.S. 630, 645 (2004) (Souter, J., dissenting).

129. *See* Commonwealth v. Brennan, 438 N.E.2d 60, 65 (Mass. 1982) ("[A]rt. 12 and the many similar constitutional provisions of other States merely restated the common law rule against self-incrimination.").

130. 425 U.S. at 418 n.4 (Brennan, J., concurring in judgment).

131. *See* Alito, *supra* note 44, at 35 (noting that the common law "privilege, as interpreted at the time of the Bill of Rights, encompassed the compulsory production of papers").

132. Nagareda, *supra* note 49, at 1619. *See also id*. at 1619 n.172 (collecting authority for the fact that the common law privilege extended to pre-existing documents and noting that "[a]ll sources to address the point concur" that the privilege applied to compelled documentary disclosures). According to Levy, "[t]he right not to be a witness against oneself imports a principle of wider reach, applicable, at least in criminal cases, to the self-production of any adverse evidence, including evidence that made one the herald of his own infamy, thereby publicly disgracing him." LEVY, *supra* note 53, at 427. If anything, the application of the common law privilege to documentary evidence seems more firmly established than the application to compelled testimony. Evidence law in England during the 1750s reflected "the primacy of writings over testimony." T.P. Gallanis, *The Rise of Modern Evidence Law*, 84 IOWA L. REV. 499, 509 (1999). The law at the time concerning oral testimony was simply a set of "rules governing the *capacity* to testify," but "had relatively little to say about what should happen once a witness began to speak." *Id*.

133. King v. Purnell, (1748) 96 Eng. Rep. 20 (K.B.).

134. *Id*.

135. *See* Nagareda, *supra* note 49, at 1620.

136. King v. Purnell, (1748) 96 Eng. Rep. 20 (K.B.).

nakedly considered."[137] Six separate times, the opinion in *Purnell* uses the phrase "furnish evidence" to refer to the compelled disclosure of private documentary records in response to a government request.[138] Contemporaneous dictionaries of the founding era similarly define "evidence" to include documents.[139]

That privilege was honored in the American colonies.[140] In colonial America, the prohibition against compelled self-incrimination was understood to have the same broad scope as it did in England, implicating both testimony and documentary evidence. "Perhaps no event in early America displays the right and its meaning better than Samuel Hemphill's trial in 1735."[141] Hemphill was a Presbyterian minister whose sermons became the subject of an ecclesiastical inquiry in Pennsylvania.[142] Despite his refusal to hand over copies of them, the sermons were nonetheless found to be "Unsound and Dangerous."[143] Benjamin Franklin came to Hemphill's defense, composing a pamphlet arguing that "[i]t was contrary to the common Rights of Mankind, no Man being obliged to furnish Matter of Accusation against himself."[144] Even the Commission that tried Hemphill "acknowledg[ed] that it had no right to compel delivery of the sermons."[145] Again, the act of "furnishing evidence" was seen to include pre-existing documents like Hemphill's sermons.

---

137. *Id*.

138. *See id*. Similarly, a case in 1744 "refused the prosecution's request that the defendant be required to turn over the records of his corporation; that, said the court, would be forcing him to 'furnish evidence against himself.'" LEVY, *supra* note 53, at 390. Those who read history to apply the privilege only to compelled testimonial statements confuse the earliest origins of the privilege with its scope *at the time of the Constitution's adoption*. "The right was originally a 'right of silence,' in Royal Tyler's words, only in the sense that legal process could not force incriminating statements from the defendant's own lips. Beginning in the early eighteenth century the English courts widened that right to include protection against the necessity of producing books and documents that might tend to incriminate the accused." LEVY, *supra* note 53, at 390.

139. *See* United States v. Hubbell, 530 U.S. 27, 51 n.2 (2000) (Thomas, J., concurring) (citing two dictionaries from the late 1700s).

140. LEVY, *supra* note 53, at 336 ("There is no doubting that England intended her law, the common law included, to be transplanted to her colonies.").

141. Andrew J. M. Bentz, Note, *The Original Public Meaning of the Fifth Amendment and Pre*-Miranda *Silence*, 98 VA. L. REV. 897, 913 (2012).

142. *Id*.

143. *Id*.

144. *Id*. at 913-14. Bentz's article also recounts the response to a piece of legislation passed in Massachusetts in 1754, which required those who purchase liquor to declare their purchases, under oath, to their local tax collectors to enable the collection of an excise tax. "Samuel Cooper, a minister, said that if the state were allowed to extort this type of information from people, 'every other Part may with equal Reason be required, and a Political Inquisition severe as that in Catholick [*sic*] Countries may inspect and controul [*sic*] every Step of his private Conduct.'" *Id*. at 914 (citation omitted). *See also* LEVY, *supra* note 53, at 386. Levy also recounts the 1768 smuggling investigation in Boston of John Hancock, future President of the Continental Congress. It was alleged that, during the investigation, Hancock's private papers had been used against him in violation of his right to compelled self-incrimination: "His office was searched, his desk rifled, his papers seized." LEVY, *supra* note 53, at 397. Hancock was represented in that case by John Adams, who would go on to draft the Massachusetts Declaration of Rights. *See id*. at 397–98.

145. LEVY, *supra* note 53, at 383. But the Commission "had taken Hemphill's refusal as a virtual confession of guilt," thus provoking Franklin's ire. *Id*.

Given this history, it should not be surprising that "all of the state constitutions to address the problem of compelled self-incrimination spoke in terms of a right against compulsion either 'to give evidence' or, equivalently, 'to furnish evidence.'"[146] And these state constitutions came before their federal counterpart: "More innovations in the drafting of constitutions occurred before the fabled meeting in the summer of 1787 to draft the U.S. Constitution than after it."[147] In relevant part, Virginia's Declaration of Rights was the model for the text of these self-incrimination provisions. It came four years before that of Massachusetts, and guaranteed that no person could "be compelled to give evidence against himself."[148] Every state constitution that contained a separate bill of rights followed Virginia's lead, protecting against a suspect being compelled to either "give" or "furnish" incriminating evidence.[149] In Massachusetts, "[t]he imagination of the drafters ran largely to past instances of the arbitrary use of power, and the remedies proposed were influenced by earlier formulations in Bills of Rights in England and Virginia."[150] Indeed, John "Adams's version of a bill of rights went beyond those that had been drafted for such states as Pennsylvania and Virginia, employing mandatory language in at least some of its provisions," including article 12.[151] The Massachusetts Constitution seems to have gone furthest of all, as it imposed a mandatory prohibition on compelling a suspect to both "accuse" himself and "furnish evidence" against himself.[152]

There is no contemporaneous indication that any of these states intended to narrow the common law privilege as it was understood in England or the colonies.[153] Indeed, the SJC was correct in holding that these state provisions were meant to

---

146. Nagareda, *supra* note 49, at 1606 (collecting citations to state constitutions of the founding era).

147. SUTTON, *supra* note 31, at 11 ("When it came time to draft the first eight amendments in the Bill of Rights, for example, Madison and others drew from the existing state constitutions.").

148. VIRGINIA DECLARATION OF RIGHTS § 8 (1776). *See generally* LEVY, *supra* note 53, at 405–12 (explaining the history of Virginia's provision and its impact on other states and the Federal constitution).

149. LEVY, *supra* note 53, at 409–10.

150. OSCAR HANDLIN & MARY HANDLIN, THE POPULAR SOURCES OF POLITICAL AUTHORITY: DOCUMENTS ON THE MASSACHUSETTS CONSTITUTION OF 1780, at 28 (1966).

151. LAWRENCE FRIEDMAN & LYNNEA THODY, THE MASSACHUSETTS STATE CONSTITUTION 11 (G. Alan Tarr ed., 2011) (citing article 12 as the example of such a provision).

152. *See* MASS. DECL. OF RIGHTS art. 12 ("No subject shall . . . be compelled to accuse, or furnish evidence against himself.").

153. In passing the Judiciary Act of 1789, Congress included a provision that would empower federal courts to "compel civil parties to produce their books or papers containing relevant evidence." LEVY, *supra* note 53, at 425–26. Levy posits that the belated addition of language limiting the scope of the Fifth Amendment's self-incrimination provision to just "criminal cases"—language that was not included in Madison's first draft of that clause—was done "with this pending legislation in mind." *Id.* at 426. If so, the narrowing of the Fifth Amendment to criminal cases plainly suggests that the clause was intended to extend to documents, as the pending Judiciary Act only related to compelled production of private papers in civil cases. There would have been no need for the First Congress—which was simultaneously writing (and trying to harmonize) the Judiciary Act and the Fifth Amendment—to narrow the self-incrimination clause to just "criminal cases" if that clause was not intended to extend to pre-existing documents. *See* United States v. Hubbell, 530 U.S. 27, 53 & 56 n.3 (2000) (Thomas, J., concurring) (citing this sequence of events as "suggest[ing] that the Framers believed the Self-Incrimination Clause offered protection against such compelled production" of private papers).

merely restate and provide constitutional protection for the pre-existing common law privilege.[154] "[I]t cannot be sufficiently stressed that the constitutional provisions were primarily devices to protect existing constitutional arrangements as Americans saw them, rather than a program of law reform."[155] Throughout its history, the Massachusetts state constitution has been amended on many occasions.[156] But since its enactment, article 12 itself "has not been amended."[157]

After the adoption of the constitutional protections against self-incrimination, "the earliest state and federal cases were in accord with that previous history" extending the common law privilege to incriminating evidence.[158] In its 1871 decision in *Emery's Case*,[159] the SJC said that the "furnish evidence" language must have meaning above and beyond the "compelled to accuse" language that comes before it: article 12's additional language "may be presumed to be intended to add something to the significance of that which precedes" it.[160] In the words of the SJC, "it is a reasonable construction to hold that it protects a person from being compelled to disclose the circumstances of his offence, the sources from which, or the means by which evidence of its commission, or of his connection with it, may be obtained."[161]

Just as a matter of textual interpretation, article 12 could hardly be read any other way. Without the words "furnish evidence," it still forbids a person from being "compelled to accuse" himself, language that would seem itself fully to embrace testimonial communications. Unlike the text of other state constitutions or the Fifth Amendment, article 12 does not just protect against compelled furnishing of evidence *or* self-accusation. Its text includes both prohibitions. One wonders

---

154. This is not to say that the textual differences between article 12 and the Fifth Amendment demand a different interpretation between those two provisions; the Fifth Amendment could (and should) be read to protect private papers too. *See generally* Nagareda, *supra* note 49 (arguing that the Fifth Amendment should also be construed to apply to documentary subpoenas); *Hubbell*, 530 U.S. at 49 (Thomas, J., concurring) (writing separately to note that "[a] substantial body of evidence suggests that the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence"). Joseph Story, in his definitive Commentaries on the Constitution, noted that the Fifth Amendment's privilege against self-incrimination was "but an affirmance of a common law privilege." 3 JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES § 1782, at 660 (Fred B. Rothman & Co. 1991) (1833). Whatever one thinks about the proper scope of the Fifth Amendment, article 12's more specific textual prohibition on the furnishing of evidence—in addition to its prohibition against a person being "compelled to accuse" himself—makes even more clear that it was intended to embrace the full sweep of the common law privilege, including its prohibition against the compelled disclosure of incriminating private documents.

155. Eben Moglen, *Taking the Fifth: Reconsidering the Origins of the Constitutional Privilege Against Self-Incrimination*, 92 MICH. L. REV. 1086, 1121 (1994).

156. *See* FRIEDMAN & THODY, *supra* note 151, at 17–27 (detailing the full history of revisions to the Massachusetts state constitution since its enactment).

157. *Id*. at 57-58.

158. LEVY, *supra* note 53, at 428.

159. 107 Mass. 172 (1871).

160. *Id*. at 182.

161. *Id*. The SJC went on to say that "the reason upon which the rule is founded, and the terms in which it is expressed, forbid that it should be limited to confessions of guilt, or statements which may be proved, in subsequent prosecutions, as admissions of facts sought to be established therein." *Id*.

what possible additional meaning "furnish evidence" could have if not to expand protection to pre-existing documentary evidence. Every word of a constitutional provision matters and must be given meaning, as "[i]t is a standard principle of constitutional interpretation that all the words of the Constitution must be presumed to have been chosen advisedly."[162] Even Justice Alito has acknowledged that "[t]his language, quite unlike that of the fifth amendment, is most naturally interpreted to apply both to live testimony and to documents."[163] Plus, as to article 12, the SJC has already held that, "[b]ecause the privilege against self-incrimination is 'a fundamental principle of our system of justice,' it 'is to be construed liberally in favor of the claimant.'"[164] The text of article 12—particularly when construed liberally and considered in light of its history—provides protection for the documentary evidence derived from acts of production.

Subsequent precedent confirms as much. Citing *Emery's Case*, the SJC later held that punishing a defendant for refusing to provide law enforcement with the name of a witness who had incriminating information against him violated article 12.[165] The court there specifically rejected the testimonial distinction that it now embraces, saying that although "[i]t might be argued that [the witness]'s name in itself had no tendency to incriminate the defendant," the Commonwealth "was in effect asking the defendant to help [it] secure [its] principal witness in order to prosecute the defendant."[166] The court did not concern itself with the testimonial nature of the defendant's answer. Rather, what mattered was that if the defendant was forced to provide the name of the witness, she "could truly have been said that she herself had helped to furnish the incriminating evidence"—that "evidence" being any statement the government might obtain from the witness.[167] Before *Fisher*, the SJC had never narrowed the scope of article 12 only to testimonial communications. To the contrary, it had specifically rejected arguments to do so.

Applying article 12 to documentary evidence is consistent with other areas of Massachusetts self-incrimination jurisprudence embodied in more recent SJC precedent. For instance, the Supreme Court has held that a violation of a defendant's rights under *Miranda v. Arizona*[168] does not require the suppression of physical evidence derived from that violation.[169] The Supreme Court's reasoning aligned

---

162. Commonwealth v. Mavredakis, 725 N.E.2d 169, 178 (Mass. 2000) (citation and alterations omitted), *overruled on other grounds by* Commonwealth v. Smith, 28 N.E.3d 385 (Mass. 2015).

163. Alito, *supra* note 44, at 79.

164. Commonwealth v. Leclair, 17 N.E.3d 415, 419 (Mass. 2014), quoting Commonwealth v. Borans, 446 N.E.2d 703, 704 (Mass. 1983). This interpretive principle makes sense in light of Massachusetts's constitutional history. An earlier proposed state constitution was "met with resounding defeat at the polls" in 1778 because of its "lack of substantive provisions delineating and protecting the people's natural rights" and its failure to frame a government that would "check tyrannical abuse." FRIEDMAN & THODY, *supra* note 151, at 9.

165. *See* Commonwealth v. Prince, 46 N.E.2d 755, 759 (Mass. 1943).

166. *Id*.

167. *Id*.

168. 384 U.S. 436 (1966).

169. *See* United States v. Patane, 542 U.S. 630 (2004). It is for this reason that the Fourth Circuit recently held that a *Miranda* violation that resulted in the suspect unlocking her phone did *not* require suppression of the

with *Fisher*, that the Fifth Amendment is primarily concerned with compelled *testimonial* communications, but physical fruits of a *Miranda* violation are not testimonial.[170] The SJC, however, has expressly rejected this distinction, raising the state constitutional floor and holding that even physical evidence derived from *Miranda* violations must be suppressed as a matter of state constitutional law under article 12. In *Commonwealth v. Martin*,[171] the court broke down the barrier between testimonial communications and their tainted physical fruits, holding that the distinction "has no relevance here" because the defendant had been "asked to *communicate* incriminating information to the police."[172] The SJC thus embraced *Schmerber*'s line between communicative and non-communicative evidence, ignoring *Fisher*'s "testimonial" distinction entirely.

Under *Martin*, article 12's prohibition against compelled self-incrimination extends to the exclusion of derivative physical evidence.[173] If the barrier between testimonial and derivative evidence falls in the *Miranda* context—and *Miranda* is itself derived from the privilege against self-incrimination—there is little reason why it should stand when considering the constitutionality of document subpoenas and compelled decryption orders.

Seldom is the text and history of a constitutional provision so unanimous. Despite the unquestioned import of the common law privilege—which extended to pre-existing documentary evidence—and the SJC's recognition that article 12 was meant to have the same scope as that privilege, the court has nonetheless narrowed article 12 in reliance upon federal precedent interpreting the Fifth Amendment. Like state courts across the country, the SJC followed where the Supreme Court led without ever pausing to ask "why the privilege should be limited to compulsion to engage in 'testimonial' activity."[174] The SJC has never recognized that the broad

---

evidence derived from the act of decryption. *See* United States v. Oloyede, F.3d 302, 309 (4th Cir. 2019). But the SJC has itself recently recognized that the contents of a phone that are the fruit of a *Miranda* violation must be suppressed under art. 12 because suppression, as a matter of state constitutional law, extends beyond just the testimonial fruit of a *Miranda* violation. *See* Commonwealth v. Vasquez, 130 N.E.3d 174, 190–91 (Mass. 2019).

170. *Patane*, 542 U.S. at 637–38. Justice Souter's *Patane* dissent also points out certain inconsistencies even in the Supreme Court's own treatment of derivative evidence under the Fifth Amendment. For example, in *United States v. Hubbell*, the Court—while reaffirming *Fisher*'s act of production doctrine—also noted that "[c]ompelled testimony that communicates information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory. It is the Fifth Amendment's protection against the prosecutor's use of incriminating information derived directly *or indirectly* from the compelled testimony of the respondent that is of primary relevance in this case." 530 U.S. 27, 38 (2000) (emphasis added, and internal citation and quotation marks omitted). Thus, even act of production cases express concern for the incriminating nature of derivative evidence while focusing solely on the testimonial nature of the act of production itself. *But see* Doe v. United States, 487 U.S. 201, 208 n.6 (1988) (explaining that the prohibition against the use of derivative evidence "assumes that the suspect's initial compelled communication is testimonial").

171. 827 N.E.2d 198 (Mass. 2005).

172. *Id*. at 204.

173. *Id*. at 200 (holding that "physical evidence obtained in these circumstances . . . is presumptively excludable from evidence at trial").

174. *See* 1 MCCORMICK ON EVIDENCE, *supra* note 7, § 124, at 726.

language of article 12 "does not require this result."[175] That federal precedent, it cannot be emphasized enough, concerned only *financial records sought from third parties*.[176] Compelled decryption requires a suspect to directly disclose all of his most private papers. Nonetheless, this uncritical, lockstep adherence to Supreme Court precedent has culminated in the SJC's permissive approach to compelled decryption.

II. THE ACT OF PRODUCTION DOCTRINE AND COMPELLED DECRYPTION

To date, the U.S. Supreme Court has never considered the issue of compelled decryption, and only a handful of courts have.[177] Indeed, the SJC may itself have given this issue the most robust treatment of any appellate court. But in each case, the SJC declined to re-examine *Fisher*'s "act of production" doctrine or its "foregone conclusion" exception.[178] Nor has the SJC questioned whether its lockstep limitation on the scope of article 12 should be changed or returned to its original, intended meaning, to match the novel intrusiveness of compelled decryption. Instead, the SJC has allowed the government to compel suspects to enter passcodes to phones so long as the government has established (as a "foregone conclusion") that the suspect knows the code.[179] This Part starts by tracing the development of the SJC's compelled decryption jurisprudence, from the SJC's 2014 decision in *Gelfgatt* to its 2019 decision in *Jones*. With that groundwork laid, it then explains the error of the court's analysis under article 12 as both a practical and historical matter. It concludes by explaining why the act of production doctrine, invented by the Supreme Court in the context of subpoenas for finite classes of documents, is a particularly poor fit for the novel context of cell phone decryption.

A. *The SJC's Approach to Compelled Decryption Under Article 12 and its Opinion in* Jones

The SJC has never even questioned the premise of compelled decryption. That is, can the government obtain a court order requiring a person to unlock their phone on threat of incarceration at all? At first blush, this appears no different from analogous contexts in which the court has struck down statutes under article 12. For instance, in 1992 the SJC held in *Opinion of the Justices to the Senate* that the refusal of a breathalyzer test could not be admissible to create an adverse inference

175. *Id.* at 726–27. ("To the contrary, a broader construction of the privilege is somewhat suggested by the terms of some formulations of it, as for example those providing that no person 'shall be compelled to give evidence against himself.' Such nuances in terminology have not, however, been regarded as of much significance.").

176. *See* Fisher v. United States, 425 U.S. 391, 398 (1976).

177. *See* Kerr, *supra* note 5, at 768 n.4 (collecting cases).

178. *See* Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014); Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019).

179. *See Jones*, 117 N.E.3d at 716.

against the accused in a drunk driving case.[180] If refusal were admissible, the court said, "[t]he accused [would be] placed in a 'Catch-22' situation: take the test and perhaps produce potentially incriminating real evidence; refuse and have adverse testimonial evidence used against him at trial."[181] This seems identical to the situation of a suspect confronted with a compelled decryption order: unlock the phone and produce incriminating real evidence (as well as information about every other aspect of his life) or refuse and (a) go to jail, plus (b) have an adverse testimonial inference used at trial.[182] The consequences on both sides of this "Catch-22" seem far more grave than in the breathalyzer refusal context. But the SJC has never seen the issue so simply.

First, in *Commonwealth v. Gelfgatt*, the court considered the Fifth Amendment and article 12 implications of compelled decryption.[183] The court described the testimonial aspect of entering a passcode as follows: "By such action, the defendant implicitly would be acknowledging that he has ownership and control of the computers and their contents."[184] The act of entering the code "would be a communication of his knowledge about particular facts that would be relevant to the Commonwealth's case."[185] But the court then went on to apply the foregone conclusion doctrine and conclude that these testimonial aspects of the act of decryption—"his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key"—were already known to the government in the case before them and proven to the degree necessary to establish a "foregone conclusion."[186]

In considering the issue under article 12, the SJC reverted to its past jurisprudence limiting the state constitutional protection to only testimonial communications. The court again concluded that the circumstances of compelled decryption did not "dictate an analytical departure from the Federal standard."[187] Instead, if the Commonwealth can establish the testimonial aspect of the act of decryption to be a foregone conclusion, its order to compel entry of the passcode complies with both the Fifth Amendment *and* article 12.[188]

Which leads to the SJC's recent opinion in *Commonwealth v. Jones*.[189] At its outset, *Jones* raised two significant issues unaddressed in *Gelfgatt*. First, the court

180. Opinion of the Justices to the Senate, 591 N.E.2d 1073, 1078 (Mass. 1992).

181. *Id.*

182. If the government is later able to hack into the phone and obtain incriminating evidence, it will likely argue at trial that the defendant refused to unlock the phone because he knew the incriminating evidence that was on it. If the government cannot hack into the phone, it will likely let the defendant sit in jail until he purges the contempt. Either way, the defendant will have suffered severe consequences from his refusal to unlock the phone, a reflection of the "Catch-22" that the decryption order placed him in.

183. Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014).

184. *Id.* at 614.

185. *Id.*

186. *Id.* at 615.

187. *Id.* at 617.

188. *See id.*

189. Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019).

needed to translate the phrase "foregone conclusion" into a more familiar standard of proof. The choice was between the "clear and convincing evidence" standard (advocated by the Commonwealth) and proof beyond a reasonable doubt (advocated by the defense).[190] Second, the case asked whether the Commonwealth could seek renewed orders for compelled decryption (after an earlier order is denied) when it obtains additional evidence, and what rules should govern such renewed orders.[191] The SJC solicited amicus briefs on both of these questions.[192]

In response, an amicus brief from the Massachusetts Attorney General's Office answered neither of these solicited questions, but raised a new one. The brief opened:

> This Court should expound not only on the *standard of proof*, but also on *what needs to be proven*, for the government to obtain a *Gelfgatt* order. It should hold that, in order satisfy the "foregone conclusion" exception to the privilege against self-incrimination, the government should need to prove only knowledge of the precise facts that a suspect would be implicitly communicating by engaging in the compelled conduct at issue. In a situation like the one presented, the precise fact asserted is simply that the suspect is able to access the device. The government should need to prove no more. To the extent that some have read a more burdensome test into the *Gelfgatt* opinion, this Court should clarify that no such test is required.[193]

According to the Attorney General's Office, the SJC's opinion in *Gelfgatt* had, by its ambiguity, suggested that the government's "foregone conclusion" burden might also require it to prove its knowledge about the specific contents of the encrypted device.[194] According to the amicus submission, in heavy reliance on the work of Professor Orin Kerr (who submitted his own amicus brief making the same point), this was wrong.[195] The Attorney General argued that the only "testimonial" aspect to an act of decryption is the suspect's statement, "I know the

190. Brief of the Appellee for Defendant at 21–27, Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019) (SJC-12564) (arguing in favor of "beyond a reasonable doubt" standard); Brief for Commonwealth at 19-22, Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019) (SJC-12564) (arguing for "clear and convincing evidence" standard). *See* Commonwealth v. Jones, 117 N.E.3d 702, 716 (Mass. 2019) (rejecting Commonwealth's argument and requiring proof beyond a reasonable doubt).

191. Brief of the Appellee for Defendant at 14–19, Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019) (SJC-12564) (arguing that renewal motions were within the trial court's discretion, akin to reconsideration); Brief for Commonwealth at 42–50, Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019) (SJC-12564) (arguing that renewal motions should not be limited only to information that was not available to the Commonwealth at the time of the first motion). *See Jones*, 117 N.E.3d at 719–20 (rejecting defendant's argument and reversing denial of the renewed motion).

192. *See* Amicus Solicitation, Docket Entry #7, Commonwealth v. Jones (SJC-12564), http://www.ma-appellatecourts.org/display_docket.php?src=party&dno=SJC-12564.

193. Brief for the Att'y Gen. as Amicus Curiae in Support of the Commonwealth at 3-4, Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019) (SJC-12564) (emphasis in original).

194. *See id*. at 11–12.

195. *Id.*

code."[196] So long as the government can prove that the suspect knows the code—to whatever standard of proof the SJC would ultimately require in *Jones*—law enforcement can obtain a *Gelfgatt* order and force the suspect to decrypt his device.[197]

The SJC agreed with the Attorney General entirely. Seeking to clarify its opinion in *Gelfgatt*, the court could not have been more explicit: "In the context of compelled decryption, the only fact conveyed by compelling a defendant to enter the password to an encrypted electronic device is that the defendant knows the password, and can therefore access the device."[198] The entry of the passcode "convey[s] no information about the contents of the . . . phone."[199] Any showing that the Commonwealth has to make concerning the contents of the phone, including concerns about probable cause for the search and the particularity of its scope, is properly considered only as a matter of the Fourth Amendment and its state constitutional counterpart, article 14.[200]

Writing separately, and only for herself, Justice Barbara Lenk did not agree that articles 12 and 14 could live in such "splendid isolation."[201] According to Justice Lenk, the Commonwealth should have to "demonstrate, beyond a reasonable doubt, that the accused knows the passcode to the device *and* that the government already knows, with reasonable particularity, the existence and location of relevant, incriminating evidence it expects to find on that device."[202] Uncomfortable with a rule that allows the government to compel a suspect to unlock the digital door to his entire life—including call logs, texts, emails, bank records, and geolocation information—with no showing related to the contents of the device, Justice Lenk warned that "[t]he court's decision sounds the death knell for a constitutional protection against compelled self-incrimination in the digital age."[203]

She was right, but for the wrong reasons. By its terms, the majority's view of the testimonial aspect of an act of decryption has a tempting logic. When a person enters the passcode to their phone, the only assertion implicit in that act would seem to be that the person knows the code. You do not necessarily make a statement about the contents of your smartphone every time you unlock it.[204] Even granting that the majority is right about how it applied the act of production doctrine, accepting that result gives rise to a number of profound analytical flaws—flaws that seemed to motivate Justice Lenk's concurrence. But when correct

196. *Id*. at 4-5.
197. *Id*.
198. Commonwealth v. Jones, 117 N.E.3d 702, 710 (Mass. 2019).
199. *Id*. at 711 n.10.
200. *See id*. at 711 n.11.
201. *Id*. at 722 n.1 (Lenk, J., concurring).
202. *Id*. at 721 (emphasis added).
203. *Id*. at 724.
204. *But see* Laurent Sacharoff, *What Am I Really Saying When I Open my Smartphone? A Response to Orin S. Kerr*, 97 TEX. L. REV. ONLINE 63 (2019) (arguing that this is wrong and that Justice Lenk's approach is correct).

reliance upon a legal doctrine yields absurd results, we should not distort the doctrine to avoid the absurdity. We should question the doctrine itself.

B. *The Multiple Errors in the SJC's Approach*

The advent of modern cell phones has created a critical mismatch between analog doctrine and digital reality—a single act of production with the slightest testimonial implications can now reveal every detail of a person's life.[205] When new technology empowers the government to engage in much more intrusive surveillance, courts should be wary of uncritical reliance on past doctrines that arose in the analog age. Even if *Fisher* itself is never overruled or re-examined, its act of production doctrine should not be imported into the distinct, far more intrusive context of compelled decryption. This is not a mere application of *Fisher*'s reasoning, but rather a marked extension, and "any extension of that reasoning to digital data has to rest on its own bottom."[206]

This is just as true when the government directly searches and seizes information, as it did in *Riley* and *Carpenter*, as when it compels disclosure from the suspect, as it did in *Jones*. Justice Lenk was right to sound a warning about the limits of the majority's rule—it will not be a "difficult endeavor" for the government to prove, even beyond a reasonable doubt, that a person in possession of a phone knows its passcode.[207] The imposition of that heightened standard was a Pyrrhic victory for Mr. Jones. The standard, frankly, is almost irrelevant. What matters is what the government needs to show and, even more importantly, whether it can obtain a compelled decryption order at all.

The myriad problems with relying on *Fisher*'s act of production doctrine in compelled decryption litigation all stem from the fact that the doctrine removes the legal dispute from the practical, real-world stakes of the case. *Fisher* focuses the analysis on a legal fiction. By "decoupl[ing] the content of documents from the act by which they are produced," the act of production doctrine "takes on an unreal, make-believe quality."[208] *Jones* misses the forest for an irrelevant tree, divorcing legal analysis from reality. Defendants do not resist compelled decryption orders

---

205. *See* Riley v. California, 573 U.S. 373, 395 (2014) (noting that cell phones allow people to "keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate").

206. *Id*. at 393. The Electronic Privacy Information Center recently filed a compelling amicus brief in a pending New Jersey Supreme Court case about compelled decryption. The brief sets out in detail how a "broad interpretation of the [foregone conclusion] exception places an astonishing amount of sensitive data in the hands of law enforcement through coercion of the suspect," and how the effort to extend *Fisher* is akin to the attempted doctrinal extensions that were rejected by the Supreme Court in *Riley* and *Carpenter*. *See* Brief for the Electronic Privacy Information Center as Amicus Curiae at 4, State v. Andrews (N.J. Appeal No. A-72-18).

207. Commonwealth v. Jones, 117 N.E.3d 702, 724 (Mass. 2019) (Lenk, J., concurring). *See also* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 1003 (2018) ("This standard would be vastly easier for the government to meet in practice because evidence that the person uses the phone regularly is likely sufficient to establish that the person knows the password.").

208. Nagareda, *supra* note 49, at 1601 ("It is rather like the Wizard of Oz imploring supplicants to pay no attention to the man behind the curtain.").

and the government does not seek them because the act of decryption might *itself* convey incriminating information to the government.[209] They are concerned about opening their phone for government inspection; it is the contents of the phone that both sides of the dispute really care about. Those pre-existing contents are what is really at stake and should be the focus of the analysis. By focusing on the act of production while ignoring the derivative evidence on the phone, the SJC got it "precisely backward."[210]

That backward approach starts by distorting the constitutional text. Indeed, the majority's textual analysis of article 12 is hard to even follow, for the court relies upon the "furnish evidence" language to impose a heightened "beyond a reasonable doubt" standard of proof while simultaneously ignoring what those words mean for the scope of the protection of the privilege.[211] When the means of compulsion are so significant, and the intrusiveness of disclosure so substantial, the SJC must revisit the proper scope of article 12, or at least not import analog doctrine into a novel digital context. The state constitution should be read consistent with its purpose (to constitutionalize the common law privilege), history (that the common law privilege applied to pre-existing documents), and plain terms (in that "furnish evidence" means what it says).[212] The government should not be able to compel someone to open their smartphone and thereby "furnish" the most intimate details of the person's life for government examination. A constitutional prohibition on the compelled furnishing of evidence has somehow been read not to protect against a circumstance in which the government compels someone to turn over nearly all of the private documents in their life. No one in 1780 could have imagined such a state of affairs.

That textual distortion yields absurd results. Perhaps most glaringly, the doctrine established in *Jones* causes article 12 protection to have an inverse relationship with the intrusiveness of the government's request for incriminating information.[213] For instance, if the government subpoenaed me to testify about the specific contents of one email, that would plainly violate article 12 if the contents of that email were incriminating.[214] But if the government seeks a *Gelfgatt* order to

209. *See* Kerr, *supra* note 5, at 795 (entry of the passcode "is a consequence of how the technology works, not evidence the government wants").

210. Nagareda, *supra* note 49, at 1602.

211. *See Jones*, 117 N.E.3d at 714.

212. *See supra* at Part I.C.

213. *Compare* Fisher v. United States, 425 U.S. 391, 411 (1976) (holding that the government must establish as a foregone conclusion "the existence and possession of the papers" sought in the context of subpoenas for specific sets of documents), *with Jones*, 117 N.E.3d at 714 (holding that the government need only establish that the defendant knows the password to the phone when it seeks to search the entire contents of the phone, with no showing necessary as to any documents on the phone itself).

214. It is not entirely clear whether the foregone conclusion doctrine applies to compelled testimonial communications aside from those implicit in an act of production. This seems impossible, however, as it "would imply that defendants should be forced to testify or suspects not be allowed to invoke their Miranda privilege whenever the government already knows what their answers will be." Michael S. Pardo, *Disentangling the Fourth Amendment and the Self-Incrimination Clause*, 90 IOWA L. REV. 1857, 1889 (2005). The foregone

decrypt my phone, it can do so if it proves only that I know the code to my phone. In other words, the government is barred from obtaining compelled testimony from me about *one* specific email, but it can circumvent article 12 and easily obtain a *Gelfgatt* order compelling me to turn over a copy of *every* email that I have ever sent or received (and everything else on the phone, too).[215] The broader the government's request, the lower its burden. In applying the act of production doctrine to compelled decryption, the intrusiveness of the government's request somehow becomes a virtue rather than a vice.

This error is the culmination of a self-incrimination jurisprudence that seems unconcerned with the protection of privacy. The *Jones* majority simply assumes that privacy is the exclusive province of the Fourth Amendment and article 14.[216] At no point in its opinion does the majority seem concerned about the intrusiveness of the disclosure that the government is seeking to compel by requiring decryption. The SJC did not consider the difference between the third-party disclosure of a discrete set of financial documents in *Fisher* and the expansive disclosure of private documents on a phone. Nowhere does *Jones* discuss the privacy interests at stake: that the examination of the phone will yield a person's most intimate information for the government's ready examination. To the SJC, privacy was not the province of article 12.

---

conclusion doctrine thus seems applicable only to the testimony implicit in compelled acts of production, not compelled testimony. That limitation on the foregone conclusion exception—making it applicable to "testimonial" acts of production but not "testimony" itself—only further exposes the unprincipled nature of the exception. *See* Alito, *supra* note 44, at 49 (describing the "foregone conclusion" exception as the "most unsatisfying and misleading portion of *Fisher*," since it "appears on its face to be inconsistent with the settled understanding of the privilege, because the privilege has never been restricted to testimony that is not cumulative"); *see also* Nagareda, *supra* note 49, at 1597–98.

215. The same holds true if we just compare a document subpoena to a compelled decryption order: if the government seeks to have me turn over a single email, its description of that email must be specific enough to comply with the "reasonable particularity" standard to show its pre-existing knowledge of the email's existence and establish the predicate of the foregone conclusion doctrine. *See* Kerr, *supra* note 5, at 775. But if the government seeks a compelled decryption order for the full contents of my phone, it can (under *Jones*) do so without complying with that standard at all, on a mere showing that I know the code to the phone. *See Jones*, 117 N.E.3d at 714. Under the SJC's approach, a defendant subject to a compelled decryption order loses the protection of the "reasonable particularity" standard that otherwise applies to all other subpoenas for documents. This is not my gloss on *Jones*; the SJC said so. The court noted that "[t]he analysis would be different had the Commonwealth sought to compel the defendant to produce specific files located in the" phone. *Id.* at 711 n.10. "If that had been the case, the production of the files would implicitly convey far more information than just the fact that the defendant knows the password," such as "the existence of the files, his control over them, and their authenticity." *Id.* But, because the Commonwealth sought access to *everything* on the phone, it did not need to make any showing about its contents since the entry of the passcode "convey[s] no information about the contents of the . . . phone." *Id.* The court said this all so matter-of-factly that one could be forgiven for missing the absurdity. By the SJC's own admission, far greater protection is afforded to compelled disclosures that are far less intrusive. That is one critical reason why the act of production doctrine, and its foregone conclusion exception, is such a glaringly poor fit for the digital age.

216. *See Jones*, 117 N.E.3d at 711 n.11.

In reality, "the protection of personal privacy is a central purpose of the privilege against compelled self-incrimination."[217] Until its opinion in *Fisher*, which fundamentally changed the scope of protection against compelled self-incrimination, the Supreme Court had repeatedly recognized that the Fifth Amendment "enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment."[218] Indeed, the SJC had previously relied on these precedents in noting that the privilege reflects "our respect for the inviolability of the human personality and of the right of each individual to a private enclave where he may lead a private life."[219] For some reason, these privacy principles have been lost to history, just as governmental compulsion has become most intimately intrusive.

Further, to have this zone of privacy extend only to testimonial evidence defines the scope of constitutional protections by mere happenstance. It seems odd to have the extent of article 12's protection depend on whether a person stores something in their memory or writes it down on a scrap of paper (or, as here, in the memory of their smartphone). As Justice Brennan observed in his *Fisher* concurrence:

> I perceive no principle which does not permit compelling one to disclose the contents of one's mind but does permit compelling the disclosure of the contents of that scrap of paper by compelling its production. Under a contrary view, the constitutional protection would turn on fortuity, and persons would, at their peril, record their thoughts and the events of their lives. The ability to think private thoughts, facilitated as it is by pen and paper, and the ability to preserve intimate memories would be curtailed through fear that those thoughts or events of those memories would become the subjects of criminal sanctions however invalidly imposed.[220]

The same could be said about modern smartphones. People have increasingly outsourced their brains to their phones—they write email reminders for everything, use GPS maps to drive everywhere, and no longer bother to memorize phone numbers.[221] Information that was once kept in our minds is now stored on our phones. But the scope of constitutional protections should not turn on the "fortuity" that someone stores a piece of incriminating information on their phones. Luddites do not deserve greater constitutional protection than millennials. Documentary

---

217. Fisher v. United States, 425 U.S. 391, 416 (1976) (Brennan, J., concurring in judgment). *See also* Schmerber v. California, 384 U.S. 757, 767 (1966) ("The values protected by the Fourth Amendment thus substantially overlap those of the Fifth Amendment helps to protect.").

218. Griswold v. Connecticut, 381 U.S. 479, 484 (1965). *See also* Couch v. United States, 409 U.S. 322, 327 (1973) ("By its very nature, the privilege is an intimate and personal one. It respects a private inner sanctum of individual feeling and thought and proscribes state intrusion to extract self-condemnation.").

219. Attorney General v. Colleton, 444 N.E.2d 915, 917 (Mass. 1982) (citation omitted).

220. *Fisher*, 425 U.S. at 420 (Brennan, J., concurring in judgment).

221. *See* TOMMY ORANGE, THERE, THERE 67 (2018) ("I depend on the internet for recall now. There's no reason to remember when it's always just right there, like the way everyone used to know phone numbers by heart and now can't even remember their own. Remembering itself is becoming old-fashioned.").

evidence is no different from testimonial evidence—both communicate the contents of a suspect's mind, one is just reduced to writing.

For this reason, Justice Brennan was clear in both his opinion in *Schmerber* and his concurrence in *Fisher* that "the protection of the privilege reaches an accused's communications, *whatever form they might take*."[222] The communicative nature of the evidence sought—not the communicative nature solely of the act of production—should matter for self-incrimination purposes. Modern smartphones are simply "a substitute for the perfect memory that humans lack."[223] Indeed, "the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[224] Considering the close relationship many people have with their phones, "[f]orcing an individual to give up possession of these intimate writings may be psychologically comparable to prying words from his lips."[225] In this context, *Fisher* is unworkable.

The notion that "[n]othing [is] your own except the few cubic centimetres inside your skull" should stay in 1984.[226] The tenuous line drawn in *Fisher* between testimonial and documentary evidence makes constitutional protection turn on the happenstance of where communicative evidence happens to be memorialized. Perhaps this fortuity made sense when *Fisher* was decided in 1976, when cutting edge technology involved a rotary dial. But it has particularly devastating consequences in the twenty-first century, as the advance of technology has allowed a single act of production with slight testimonial implications to unlock mountains of intimate and intrusive documentary evidence.

III. THE IMPLICATIONS OF A PROPER READING OF ARTICLE 12

This Part addresses the likely consequences of reading state constitutional protections against self-incrimination to preclude compelled decryption. It starts by emphasizing that such a holding need not encroach into other doctrinal domains. Orders seeking bodily evidence, subpoenas to third parties, and subpoenas to suspects seeking business or financial records would all still be permissible. Instead, redrawing this doctrinal line would focus self-incrimination doctrine on the core zone of protection that compelled decryption invades: the forced disclosure of personal papers. This Part then goes on to explain that, as it stands, the advent of biometric decryption technology may soon render the developing doctrine outmoded before it is even settled. If the doctrine does not change its focus to the contents of smartphones rather than the mere act of unlocking them, such technology will allow the government readily to access biometrically encrypted devices without

222. *Schmerber*, 384 U.S. at 763–64 (emphasis added).

223. Alito, *supra* note 44, at 39.

224. Riley v. California, 573 U.S. 373, 385 (2014).

225. Alito, *supra* note 44, at 39. *See also* Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, 97 TEX. L. REV. ONLINE 73, 82 (2019) ("Being parted from one's cellphone is like losing one's memory and one's mental map of the world.").

226. GEORGE ORWELL, 1984, at 27 (1949).

any testimonial act of production at all. Next, this Part emphasizes the practical consequence of allowing the government to force suspects to unlock their phones: police will seek to do so more often. Even without that power, the police can still use technical workarounds or solicit third party assistance to access encrypted phones; they will just need to prioritize their investment of resources in deciding when to do so. Other state courts—which are almost evenly divided in the language of the self-incrimination provisions of their constitutions—will soon confront this issue. Thus, this Part concludes by arguing that, when they do, those state courts must consider the protections of their own constitutions, distinct from the protections of the Fifth Amendment.

A. *Few Other Areas of Self-Incrimination Jurisprudence Would be Upended by a Proper Reading of Article 12*

To redraw the testimonial-nontestimonial distinction consistent with *Schmerber* and *Boyd* would not require the SJC, or any other state court, to cast aside its entire body of self-incrimination jurisprudence. The rule thus derived would hold that the government cannot compel a suspect to furnish his private, incriminating papers for government examination. A return to the line drawn in *Schmerber* protecting all of a suspect's private communications, testimonial or not,[227] would impose a stark new limit on compelled decryption orders. But it would not require a wholesale change in how law enforcement gathers other evidence.

As Professor Richard Nagareda noted in his seminal 1999 article, *Compulsion "To Be a Witness" and the Resurrection of Boyd*, one must be mindful of the difference between the two ways the government gets evidence.[228] Under article 12, the government may not compel a suspect to "accuse" or "furnish evidence" against himself, be it testimonial or (as argued *supra* in Part I) documentary. That provision recognizes that there is something especially "cruel" about compelling a suspect to "produce the evidence against him . . . from his own mouth."[229] But the government may seize such evidence directly, with its own hands and "by its own independent labors," so long as it complies with the search and seizure provisions of article 14 and the Fourth Amendment.[230] Although article 12 and the Fifth Amendment categorically forbid direct compelled disclosure from the suspect, article 14 and the Fourth Amendment prohibit only "unreasonable" government searches and seizures.[231] In many cases, the government may obtain directly, via a

227. *See Schmerber*, 384 U.S. at 763–64 ("It is clear that the protection of the privilege reaches an accused's communications, whatever form they might take, and the compulsion of responses which are also communications, for example, compliance with a subpoena to produce one's papers.").

228. *See* Nagareda, *supra* note 49, at 1622–23.

229. Miranda v. Arizona, 384 U.S. 436, 460 (1966).

230. *Id.*

231. *See* Nagareda, *supra* note 49, at 1622.

search or seizure, that which it cannot compel the suspect to turn over.[232] So, for starters, when the government does *not* enlist a suspect in the uncovering of evidence—be it verbal or documentary—there is no article 12 problem at all.

Second, if the SJC simply re-draws the *Schmerber* line, it would not need to throw out its entire bodily evidence jurisprudence. *Schmerber* itself distinguished between communicative and non-communicative evidence, placing pre-existing documents squarely on the "communicative" side of that dichotomy.[233] But, as Professor Nagareda explained, when the government seeks bodily evidence it is not compelling the disclosure of communications; it is instead taking a distinct type of evidence directly rather than forcing the suspect to hand over his private thoughts or documents.[234] There is a difference between compelling an accused "to exhibit his physical characteristics" or provide "an identifying physical characteristic," and forcing him to hand over communications (either verbal or documentary) that "speak his guilt."[235] "[T]he Supreme Court has repeatedly defined testimony in a manner that strongly suggests that evidence derived from brain function is different from evidence derived from other bodily functions."[236]

The SJC could simply return to the *Schmerber* line protecting "communicative" evidence in addition to "testimonial" evidence, and thus separate mind from body.[237] The bodily evidence cases do not require the suspect to use the contents of his mind or disclose communicative evidence.[238] In the leading handwriting exemplar case, for example, the Supreme Court explained that handwriting might be a "*means* of communication," but the provided exemplar, "in contrast to the content of what is written, like the voice or body itself, is an identifying physical characteristic."[239] Indeed, the Court specifically distinguished document subpoenas, which,

---

232. *See id.* at 1622–23 ("The distinction is not, as the modern Court would have it, between testimonial communication and preexisting forms of incriminatory evidence. Rather, the fundamental distinction is between two different modes of information gathering by the government: the compulsion of a person 'to be a witness against himself' in the sense of giving self-incriminatory evidence—testimonial, documentary, or otherwise—and the taking of such evidence by the government through its own actions. The former is forbidden categorically by the Fifth Amendment, whereas the latter may take place, upon compliance with the strictures of the Fourth.").

233. *See* Schmerber v. California, 384 U.S. 757, 763–64 (1966).

234. *See* Nagareda, *supra* note 49, at 1627.

235. United States v. Wade, 388 U.S. 218, 222–23 (1967).

236. SALKY & HYNES, *supra* note 66, at 286. This has even occurred in cases that have come after *Fisher*. *See, e.g.*, Doe v. United States, 487 U.S. 201, 210 n.9 (1988) ("We do not disagree with the dissent that the expression of the contents of an individual's mind is testimonial communication for purposes of the Fifth Amendment.").

237. This line also has deep philosophical roots. *See* WILLIAM DAVIES, NERVOUS STATES: DEMOCRACY AND THE DECLINE OF REASON 38 (2018) (tracing writings of Hobbes and Descartes to emphasize their split between mind and body, and noting that "[t]o experience a sensation . . . is not really to achieve *knowledge* so much as to be afflicted by movements of matter").

238. *See* Doe v. United States, 487 U.S. 201, 219–20 (1988) (Stevens, J., dissenting) (explaining how compelling a person to use the contents of his mind to "assist the prosecution in convicting him of a crime" runs afoul of the Fifth Amendment, based on the line drawn in the bodily evidence cases). "The only limiting principle on forced extraction of incriminating physical evidence appears to be conduct that 'shocks the conscience,'" but such government conduct "is prohibited by other portions of the Bill of Rights and not by the Self-Incrimination Clause." SALKY & HYNES, *supra* note 66, at 41.

239. Gilbert v. California, 388 U.S. 263, 266 (1967) (emphasis added).

at the time, fell within Fifth Amendment protection.[240] The SJC could readily hold, hewing to the bright line previously drawn in *Schmerber*, that such non-documentary bodily evidence falls outside of any newly revised scope of article 12 protection.[241]

Third, applying article 12 to compelled decryption would not require the SJC to categorically hold that *all* document subpoenas constitute compelled self-incrimination. For example, in the context of *Fisher*, the government sought financial records in the hands of the suspect's attorney.[242] By recognizing that article 12 was intended to establish a core zone of privacy protection for compelled disclosures, the SJC would not need to protect information that is either (a) in the hands of third parties,[243] or (b) related to financial or business records, as in *Fisher*, rather than private documents.[244] The core of the right—protection against compelled *direct* disclosure of *private* documents—does not define its outer bounds, and article 12 would not necessarily need to apply to all communicative evidence even if it were held to apply to the contents of a personal cell phone.

Indeed, pre-*Fisher* precedent bears out the distinction between personal and business documents. For example, in *Shapiro v. United States*, the Supreme Court addressed a subpoena for documents that a federal price control statute required the defendant to retain and make available for inspection.[245] The Court reasoned that there was a "sufficient relation between the activity sought to be regulated and the public concern" animating the price control statute to allow the compelled disclosure of the documents.[246] The Court thus held that "the privilege which exists as to private papers cannot be maintained in relation to records required by law to be

240. *Id.*

241. Professor Nagareda re-imagines the outcome of the bodily evidence cases by reference to the notion that the government "could have constructed a life-size model" of the defendant's person once it had him in custody, and so it can force the defendant (once he is lawfully seized) to do the same things that it could have had its model do. *See* Nagareda, *supra* note 49, at 1628. Using this framing, Nagareda argues that the handwriting and voice exemplar cases should fall *within* the protection against compelled self-incrimination because the government's mute and lifeless model of the defendant could not provide such exemplars. *Id.* To Nagareda, the suspect is being compelled to use his mind to give the government evidence it will use against him. *Id.* "Consistent with the Fourth Amendment, the government unilaterally may seize documents that contain the handwriting of a person and may intercept examples of the person's voice by way of duly authorized wiretaps or recordings made by government informants. What the government may not do is to compel the person to produce exemplars in order to provide a link in the chain of incriminatory evidence." *Id.* at 1629. Nagareda may be right, but that is not the line drawn in *Schmerber*, nor is it the line a court would need to draw to protect suspects against compelled decryption.

242. *See* Fisher v. United States, 425 U.S. 391, 394 (1976).

243. Past cases have recognized an exception to this principle for when documents in a third party's possession could be deemed to be in the owner's "constructive possession." *See, e.g.*, Couch v. United States, 409 U.S. 322, 329–33 (1973) (noting that "possession bears the closest relationship to the personal compulsion forbidden by the Fifth Amendment," while recognizing that "situations may well arise where constructive possession is so clear or the relinquishment of possession is so temporary and insignificant as to leave the personal compulsions upon the accused substantially intact").

244. *See Fisher*, 425 U.S. at 394.

245. Shapiro v. United States, 335 U.S. 1, 1 (1948).

246. *Id.* at 32.

kept."[247] Before *Fisher*, the Supreme Court repeatedly recognized that "there is an important difference in the constitutional protection afforded their possessors between papers exclusively private and documents having public aspects."[248]

Since *Fisher*, some judges have continued to recognize this distinction and tried to fit voluntarily-created private papers within the protections of the privilege, with limited success.[249] The New Jersey Supreme Court, for example, retained *Boyd*'s protection against the compelled disclosure of private papers in its common law. Drawing heavily from Justice Brennan's concurrence in *Fisher*—while also proudly emphasizing Brennan's prior role as a justice on the New Jersey Supreme Court—that court "affirm[ed] [its] belief in the *Boyd* doctrine" and protected private documents under its state common law privilege.[250] When a subpoena seeks documents, "a court must look to their contents, not to the testimonial compulsion involved in the act of producing them," to determine whether those documents "lie within that special zone of privacy that forms the core of the documents protected by *Boyd* and its progeny."[251] The New Jersey Supreme Court has thus returned to the privacy rationale that underlies the privilege against self-incrimination. This holding can and should be applied equally to compelled decryption orders.

Subpoenas for business records, or even personal records held in the possession of third parties, could be held to fall outside of article 12 protection. *Fisher* itself repeatedly noted that the subpoena in that case did not involve private papers and had gone to a third party rather than to the accused.[252] The government will continue to litigate the propriety of forcing device manufacturers to decrypt devices belonging to their customers.[253] But compelled decryption still unavoidably implicates the heart of the privilege: the forced disclosure of personal, private papers sought directly from the suspect.

---

247. *Id.* at 33. Of course, there must be limits on the "required records" principle.

> [A] statute that required all Americans to keep a diary in which they recorded every arguably illegal act that they committed, or make a tape-recorded confession whenever they committed an illegal act, would not empower the authorities, under the aegis of the required-records doctrine, to compel the production of the diary or the tape.

Smith v. Richert, 35 F.3d 300, 303 (7th Cir. 1994).

248. Davis v. United States, 328 U.S. 582, 602 (1946). Justice Marshall also stressed the need to protect private papers in his dissent in *Couch v. United States*. 409 U.S. 322, 350 (1973) (Marshall, J., dissenting) ("Diaries and private letters that record only their author's personal thoughts lie at the heart of our sense of privacy.").

249. *See* 1 MCCORMICK ON EVIDENCE, *supra* note 7, at § 137, at 775 n. 5 (collecting cases).

250. *In re* Grand Jury Proceedings of Guarino, 516 A.2d 1063, 1070 (N.J. 1986).

251. *Id.*

252. Fisher v. United States, 425 U.S. 391, 398 (1976) ("Agent or no, the lawyer is not the taxpayer. The taxpayer is the 'accused,' and nothing is being extorted from him.").

253. *See, e.g.*, *In re* Apple Inc., 149 F. Supp. 3d 341 (E.D.N.Y. 2016) (holding that a compelled decryption order sent to Apple was unlawful under the All Writs Act, 28 U.S.C. § 1651(a), and that Apple cannot be forced to assist a government investigation against its will).

B. *The SJC's Current Path Ensures Article 12's Imminent Obsolescence*

The same rule should govern the next frontier of compelled decryption: biometrics.[254] Many smartphones now unlock by fingerprint or facial recognition of the owner. The new doctrinal approach outlined above would refocus article 12 and analogous state constitutional protections on the *result* of an act of production—the compelled furnishing of incriminating private papers—as opposed to the testimony implicit *in* that act of production. Biometric decryption would thus fall within the reinvigorated scope of constitutional protection because it has the exact same result as entering the passcode: it unlocks the phone and discloses its contents. With this change in focus, using a finger to unlock a phone is no different than entering a four-digit passcode because it would similarly result in the compelled disclosure of private papers.

Under current doctrine, however, the march of technological progress will only further erode the scant protections of *Gelfgatt* and *Jones* "because providing fingerprints or other body parts is not testimonial."[255] When one presses her thumb to a phone, she makes no statement about her relationship with that phone because it may or may not unlock. Given this, the SJC's entire body of compelled decryption doctrine will soon be rendered obsolete if the court retains its narrow focus on the act of production doctrine rather than the compelled furnishing of documentary evidence. If article 12 protects only testimonial communications, the next (and current) generation of smartphones will eliminate *all* protections against compelled decryption. In a world of biometric decryption, judicial decisions about passwords will be wasted ink. The government will freely be able to force suspects to place their fingers on phones and unlock their most private papers for government review, with no judicial review or factual showing necessary to do so.[256] By errantly focusing on the legal fiction of the act of decryption, rather than the result of that act—which is the same regardless of how the phone is decrypted—*Jones* (and cases like it) will leave constitutional protection to the fortuity of whether a device is encrypted by password or by fingerprint. A self-incrimination jurisprudence that relies upon the act of production doctrine, and remains unconcerned with privacy, is destined for obsolescence in a twenty-first century in which even non-testimonial acts of production can yield every detail of a person's life.[257]

---

254. The term "biometrics" is used herein to refer to the act of unlocking a phone by reliance on a facial scan or fingerprint rather than an alphanumeric password.

255. Kerr & Schneier, *supra* note 207, at 1003.

256. Advances in cognitive neuroscience will render the distinction between compelled testimony and compelled communications even more important, because "we can expect a future in which we will be able to extract self-incriminating patterns of brain function from a person without requiring the person to speak or even make a responsive gesture." SALKY & HYNES, *supra* note 66, at 285.

257. Multiple courts have held that biometric decryption is not testimonial. *See In re* White Google Pixel 3 XL Cellphone in a Black Incipio Case, 2019 WL 3401990 (D. Idaho July 26, 2019); State v. Diamond, 905 N.W.2d 870 (Minn. 2018); *In re* Search of [Redacted] Washington, D.C., 317 F. Supp. 3d 523 (D.D.C. 2018); Commonwealth v. Baust, 89 Va. Cir. 267 (Va. Cir. Ct. 2014). Two others have held that compelling the

Indeed, the doctrine of *Jones* is already subject to easy evasion. Consider, for instance, if the government does not know whether the suspect knows the code. It cannot meet its "foregone conclusion" burden. To evade the already-slight protection of *Jones*, the government could simply immunize the compelled act of production—it can just agree not to use the mere act of production itself against the suspect.[258] But the documents revealed by that act (the entire contents of the phone) will not be subject to the same grant of immunity. Of course, immunity need not extend to the use of pre-existing documents if article 12 protection does not extend to those documents.[259] Thus, either by the advance of technology or the creative grant of immunity, *Jones*'s exclusive focus on the knowledge of the code is already obsolete.

---

production of a biometric key is equally as testimonial as providing a passcode. *See In re* Residence in Oakland, California, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019); *In Re* Application for a Search Warrant, 236 F. Supp. 3d 1066 (N.D. Ill. 2017); *see also* United States v. Warrant, 2019 WL 4047614 (N.D. Cal. Aug. 26, 2019) (permitting biometric decryption where phone is found "on the person of one of the individuals named" in the warrant *and* where the police "have information that the particular individual who is compelled to apply his or her biometric feature(s) has the ability to unlock that device"). The latter cases, much like the concurring justice of the SJC in *Jones*, seem to be admirably incorrect. Those cases reason, for example, that a biometric code is "functionally equivalent" to a numeric passcode, and so "if a person cannot be compelled to provide a passcode because it is a testimonial communication, a person cannot be compelled to provide one's finger, thumb, iris, face, or other biometric feature to unlock that same device." *In re* Residence in Oakland, California, 354 F. Supp. 3d at 1015–16. But that is wrong as a matter of doctrine. Under *Fisher*, the *function* of the act of decryption does not matter; what matters is what it *communicates*. Again, it is admirable for these courts to try to avoid such a counterintuitive, intrusive, and absurd result. But judges would be better off admitting that the correct application of *Fisher*'s "act of production" doctrine provides no protection at all against compelled biometric decryption, which is yet another reason to change that underlying doctrine itself rather than distort how one applies it.

258. *See* 1 MCCORMICK ON EVIDENCE, *supra* note 7, at § 138, at 779 (noting that the scope of immunity need only be "as broad as the protection of the privilege").

259. Professor Kerr dismisses this concern by saying that the Supreme Court has already held that using such a grant of immunity to evade the act of production doctrine is not permissible. *See* Kerr, *supra* note 5, at 775 n.50 (citing United States v. Hubbell, 530 U.S. 27, 42–43 (2000)). I am not so sure.

Immunity need only be "as broad as the protection of the privilege" itself. *See* 1 MCCORMICK ON EVIDENCE, *supra* note 7, at § 138, at 779. As a result, the narrower testimonial aspect of an act of production in the compelled decryption context, as compared to that in the context of document subpoenas, may well result in a corresponding reduction in the scope of required immunity. In *Hubbell*, the Supreme Court emphasized that a traditional document subpoena is "designed to elicit information about the *existence* of sources of potentially incriminating evidence," which requires derivative use immunity. 530 U.S. at 43 (emphasis added). The defendant there "ma[d]e extensive use of the contents of his own mind in identifying the hundreds of documents responsive to the requests in the subpoena." *Id.* (citation omitted). But Mr. Jones will have to do no such thing. As Professor Kerr himself argues, a response to a compelled decryption order says nothing about the "existence" of derivative information on the phone; it just says "I know the code." See Kerr, *supra* note 5, at 779. When an act of production says nothing about the "existence" of the derivative information, "the government need not immunize" the defendant against the use of that information when it seeks to compel the act of production. William J. Stuntz, *Self-Incrimination and Excuse*, 88 COLUM. L. REV. 1227, 1278 n.185 (1988) (resolving the contradiction between the scope of required immunity and the act of production doctrine by reference to "the fact that one of the testimonial aspects of producing evidence is the acknowledgment of the existence of that evidence"). Because compelling a suspect to decrypt his phone makes no testimonial statement about the existence of the documents on the phone, it seems that, per the logic of *Hubbell* and Professor Stuntz, the government can entirely sidestep *Jones* just by immunizing the narrower act of production while readily using the contents of the phone against the "immunized" suspect. This appears doctrinally correct, but defies common sense.

Even by its terms, the SJC's announced doctrine turns on semantics. That is because, if the government seeks to order the suspect "to orally state, or write down, her passcode," then "almost everyone . . . agrees" that would be impermissible.[260] Even the *Jones* majority recognized that such an order would be on weak constitutional footing because the foregone conclusion doctrine seems to apply only to compelled acts of production, like the act of unlocking the phone, and not compelled testimony, like orally stating the code.[261] Under its ruling, the SJC was careful to note that "[t]he defendant may therefore only be compelled to enter the password to the . . . phone, not disclose it."[262] This is a truly bizarre limitation on government power, turning exclusively and explicitly on the semantics of the compulsive order. Article 12 protects suspects from having to *tell* the government their code, but provides scant protection against their being forced to *unlock* their devices upon request and hand them over. Of course, both roads lead to exactly the same place: the phone unlocked for government inspection. It is illogical to have so much turn on so little, and again exposes the absurdity of *Jones*'s narrow focus on the act of production with no concern for the documents produced.

What matters is what happens: the government is forcing a suspect to open their phone for inspection. Self-incrimination doctrine should assess this reality rather than the legal and technical triviality called for by application of the act of production doctrine. Unfortunately, by focusing on the act of production rather than the contents of the phone, "[t]oday's doctrine is highly sensitive to changes in available technology and in the common usage of existing technology, including small changes to default settings, or in the details of how a particular product is implemented in software."[263] This renders the doctrine "brittle" by allowing case outcomes to hinge on "the details of the software used" rather than the intrusive nature of the compelled disclosure.[264] This doctrinal myopia may also exacerbate systemic inequalities, as sophisticated defendants learn what phone settings ensure the greatest protection against compelled decryption while Luddites are left to the vulnerabilities of factory defaults.[265]

On the other hand, if Professor Kerr were right, it would defy the doctrine. A bar on derivative use would be in obvious tension with the notion that the Fifth Amendment does not protect the contents of derivative documents. A suspect would have to be immunized against the use of documents even when he has not implicitly or explicitly testified to their existence. By this view, two self-incrimination doctrines would point in opposite directions: immunity doctrine would disallow the derivative use of the non-testimonial contents of documents, while the act of production doctrine would not. Again, these absurdities show why the underlying doctrine itself is what needs to change.

260. Sacharoff, *supra* note 204, at 64.

261. *See* Commonwealth v. Jones, 117 N.E.3d 702, 710 n.9 (Mass. 2019).

262. *Id*.

263. Aloni Cohen & Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, 32 HARV. J. L. & TECH. 1 at 232–33 (2018).

264. *Id*. at 233.

265. *See id*.

To recap, if the voluminous contents of smartphones are rightly considered to fall within the scope of article 12 protection, little other precedent would have to change. Bodily evidence would remain unprotected pursuant to *Schmerber*'s bright line between communicative and non-communicative evidence. And business records, or even personal documents sought indirectly from third parties, could also be regarded as unprotected because they fall outside of the zone of privacy that is the central concern of article 12. But the irreducible core of protection precisely covers the context of compelled decryption: when the government seeks to force a suspect to directly hand over *all* of his most private papers.[266] This approach avoids a world in which technology forces the obsolescence of constitutional protections, which would otherwise turn entirely on semantics.

C. *Foreclosing Compelled Decryption Will Force Law Enforcement to Reserve its Resources and Conduct Intrusive Cell Phone Searches Only in the Serious Cases that Call for Them*

Judicial reluctance to read state constitutions to provide more expansive protection against compelled decryption will likely be founded in a concern over what such a reading would mean for the exigencies of law enforcement. If the police cannot force a suspect to unlock his phone, their job might be made more difficult. But the privilege against self-incrimination was not written with that purpose in mind,[267] and courts should not abandon constitutional principles to ease the burdens on police investigations. The needs of law enforcement are not a proper consideration in the context of a constitutional provision that imposes a categorical prohibition on the compelled furnishing of evidence to the government.[268] State courts should scrutinize the language and history of their own privileges against self-incrimination to determine their scope. Those provisions are far too important for the sort of fair-weather originalism that bends to the whim of law enforcement.[269]

---

266. *See supra* Part III.A.

267. *See* Nagareda, *supra* note 49, at 1605–23.

268. As explained, once the privilege attaches its protections are absolute, regardless of the needs of law enforcement or the seriousness of the case. There is no exigency exception to the self-incrimination privilege. *See In re* Grand Jury Investigation, 22 N.E.3d 927, 935–36 (Mass. 2015) ("[T]he privilege against self-incrimination admits no balancing of State-defendant interests and does not yield to reasonable intrusions. Law enforcement, for instance, plainly could not compel a defendant to disclose where he allegedly hid a murder weapon, even if the police could establish probable cause to believe that the weapon was hidden somewhere in his house and that, if given a warrant, they would likely be able to find the weapon eventually anyway.") (internal citations and alterations omitted).

269. Plus, one might reasonably question whether foreclosing compelled decryption would even have any adverse effect on law enforcement, despite claims to the contrary. "Pretty much continuously since the 1990s, U.S. law enforcement agencies have claimed that encryption has become an insurmountable barrier to criminal investigation." SCHNEIER, *supra* note 29, at 193. Indeed, the dire warnings of the Director of the FBI in 1997 are indistinguishable from those delivered by Attorney General William Barr in July 2019. *Compare The Impact of Encryption on Public Safety: Before the Permanent Select Comm. On H. Affairs*, 105th Cong. 1 (1997) (Statement of Louis J. Freeh, Director, Federal Bureau of Investigation) ("Law enforcement is in unanimous

Of course, given *Jones*, changing the meaning of the Massachusetts constitution would require a deviation from the status quo.[270] And the endowment effect—that "[p]eople react far worse when they lose something they once had than they do if they do not receive something in the first place—is a powerful cognitive bias and obstacle to change."[271] Police and prosecutors are not immune from that impulse. But a change in doctrine will be a necessary corrective to a five-year mistake that has errantly aided government investigations since *Gelfgatt* was decided in 2014. Under article 12, the police never should have had the power to compel suspects to decrypt their phones in the first place.

Further, one cannot overlook the impact that legal rules have on police behavior: the easier it is for police to obtain compelled decryption orders, the more they will do so.[272] This in turn will encourage the sorts of prosecutions in which cell phones searches are most common. The majority of cases involving the search of a cell phone are street-level drug prosecutions where the police search the phone of an arrestee to obtain evidence, likely in the form of text messages, that inculpates the defendant in suspected drug distribution.[273] These are the very arrests and prosecutions that drive racial disparities in criminal adjudication.[274] Rules create

---

agreement that the widespread use of robust unbreakable encryption ultimately will devastate our ability to fight crime and prevent terrorism."), *with* William P. Barr, *Keynote Address at the International Conference on Cyber Security* (July 23, 2019) ("[T]his form of 'warrant proof' encryption poses a grave threat to public safety by extinguishing the ability of law enforcement to obtain evidence essential to detecting and investigating crimes. . . . The costs of irresponsible encryption that blocks legitimate law enforcement access is ultimately measured in a mounting number of victims—men, women, and children who are the victims of crimes—crimes that could have been prevented if law enforcement had been given lawful access to encrypted evidence."). The sky has yet to fall.

Former General Counsel of the FBI, James Baker, has recently written that, weighing concerns about law enforcement against national security, Attorney General Barr and other "public safety officials should embrace encryption." James Baker, *Rethinking Encryption*, Lawfare (Oct. 22, 2019). And a recent paper published by a working group of law enforcement officials and computer scientists, including Baker, engages in a far more nuanced analysis of the pros and cons of mobile phone encryption. That paper rejects, outright, the "straw m[a]n" that "law enforcement will be unable to protect the public unless it can obtain access to all encrypted data through lawful process." Carnegie Endowment for International Peace, Encryption Working Group, *Moving the Encryption Policy Conversation Forward*, at 9 (Sept. 2019) ("Throughout modern history, there have been technologies to destroy information and there has been much information that was beyond the reach of law enforcement. The same is true today and society continues to function.").

270. *See* Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019).

271. RACHEL E. BARKOW, PRISONERS OF POLITICS: BREAKING THE CYCLE OF MASS INCARCERATION 75 (2019).

272. *See* United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring in judgment) (recognizing that surveillance that is "difficult and costly" is "therefore rarely undertaken").

273. *See* Patrick Brown, *Searches of Cell Phones Incident to Arrest: Overview of the Law As It Stands and a New Path Forward*, 27 HARV. J. L. & TECH. 563, 576 (2014) (explaining how searches of cell phones are used in furtherance of drug prosecutions); Alexandra Crandall, *A Call for Probationer Data Privacy: Can States Require Cell Phone Search Waivers?*, 49 ARIZ. ST. L.J. 1487, 1497 (2017) (explaining why probationer cell phones are routinely searched, "especially in cases of drug trafficking," because "drug traffickers often use cell phones to complete their sales").

274. *See* Christopher Ingraham, *White people are more likely to deal drugs, but black people are more likely to get arrested for it*, WASHINGTON POST (Sept. 30, 2014). *See also* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 48 (2017) (highlighting

incentives. The easiest way into a phone is by compelling entry of the code. Easing the burden for law enforcement to obtain compelled decryption orders will result in an evidentiary windfall in the very prosecutions that drive racial disparities in the criminal justice system. That result cannot be overlooked.

We also cannot forget that the alternative to compelled decryption is not necessarily the complete loss of evidence. The police can always seek a suspect's consent to unlock and search a phone.[275] And, to the extent that evidence exists outside of the phone, the government can solicit the cooperation of third parties to try to get it.[276] The government also already has a number of ways that it can get around encryption short of forcing the suspect to furnish the code.[277]

As a result, when the government seizes a device pertinent to a serious or violent crime, it can invest its resources in unlocking the device or forcing the help of third parties to try to get what's inside. But government resources are finite. A low bar is an invitation to conduct more searches in more cases by "making available at a relatively low cost such a substantial quantum of intimate information about any person."[278] Greater protection will require law enforcement to use these encryption "workarounds," forcing the government to pick and choose when it will invest its finite resources and try to decrypt seized devices. It will naturally reserve its finite resources for more serious cases. This might also cause the federal government, which has even greater resources that it can use to decrypt devices, to take over certain serious state investigations.[279] But making it easy for the government to obtain compelled decryption orders ensures that cell phone searches will occur more often. Imposing a state constitutional barrier will reserve this intrusive investigative practice for the serious cases that deserve it.

---

one study finding that despite equivalent rates of marijuana use by all races, African Americans were 3.73 times more likely to be arrested for marijuana possession than whites were").

275. *See* Roseanna Sommers & Vanessa K. Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance*, 128 YALE L.J. 1962 (2019) (reporting results of a study in which 97.1% of people unlock their phones and hand them over upon request).

276. *See* Choi, *supra* note 225, at 80 ("Data communications are pervasive and highly leaky, and even the widespread availability of end-to-end encryption cannot erase the basic incentives for third parties . . . to cooperate with prosecutors."); SCHNEIER, *supra* note 29, at 174 ("When people use third parties for data storage and processing, that data can't be encrypted. Even companies that provide encrypted data storage often allow for files to be recovered, because that's what most users demand. All of that data will always be available with a warrant, and in some cases without one.").

277. *See generally* Kerr & Schneier, *supra* note 207, (explaining the basic principles of encryption and the common "workarounds" that law enforcement can use to avoid it).

278. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (explaining how police reliance on cheap technologies "evades the ordinary checks that constrain abusive law enforcement practices," such as "limited police resources"). *See also id.* at 429 (Alito, J., concurring in the judgment) (echoing the practical effect of technology that allows the police to conduct surveillance that was formerly "difficult and costly and therefore rarely undertaken" in a way that is now "relatively easy and cheap").

279. *See* Kerr & Schneier, *supra* note 207, at 1014 (citing the "distributional effects" that encryption workarounds will have on law enforcement).

D. *Principles of Equilibrium Adjustment Weigh in Favor of Strong Protection Against Compelled Decryption*

From an originalist perspective, the SJC's opinion in *Jones* is unimaginable. It allows the government to force a suspect, on threat of incarceration, to turn over for inspection almost every private document he owns concerning the most intimate details of his life.[280] The Framers never could have imagined such an awesome power. But encryption technology would also have been unfamiliar to them. John Adams could hardly have fathomed that evidence could be locked behind an impenetrable door to which only the suspect holds the key. For this very reason, Professor Orin Kerr argues that an "equilibrium adjustment" approach to constitutional interpretation—which involves adjusting the burdens on law enforcement to maintain the historical surveillance status quo in light of new technologies—favors allowing compelled decryption because "the technology is effectively hiding routine evidence behind password gates."[281] Because the password barrier is new, Kerr argues, the government's burden to breach it should be low.[282]

What Professor Kerr overlooks, and what the Supreme Court recognized in *Riley*, is that the documents on a cell phone are not "routine evidence" at all. Cell phones combine, in a single, easily searched package, documents that either could never have existed in the Founding era at all, or never would have existed at such volumes in the same location. The word "phone" itself is a misnomer: "They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[283] And many other accounts—email, banking, social networking, and more—are directly linked to and accessible from modern smartphones. Further, mobile applications often keep users logged in by default, allowing anyone with access to the phone access to the account.[284] The "smartphone has evolved into a centralized security hub for pretty much everything."[285] And a cell phone collects all of this distinct, intrusive

280. And it does so without the government having made any showing whatsoever that it knows anything about their contents. *See Jones*, 117 N.E.2d at 711 n.10.

281. Kerr, *supra* note 5, at 794. The Supreme Court took just this equilibrium adjustment approach in its recent opinion in *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

282. Of course, one may reasonably question Professor Kerr's premise. The probabilistic nature of decryption makes it just like any other piece of evidence that the government may or may not obtain. As Professor Kerr has elsewhere argued: "[I]n a broader sense, there is nothing new about the dynamics of encryption. The success of investigative tools and methods are always matters of chance. When a crime occurs, an eyewitness might have seen it, or maybe no one did. When the police interrogate a suspect, the suspect might confess or refuse to talk. [. . .] No law enforcement technique works every time. The challenges of encryption are no exception to that general rule." Kerr & Schneier, *supra* note 207, at 1013. Simply put, "[t]he notion that the world has never seen a technology that is impervious to detection is complete nonsense." SCHNEIER, *supra* note 29, at 194.

283. Riley v. California, 573 U.S. 373, 393 (2014).

284. Brief for the Electronic Privacy Information Center as Amicus Curiae at 13, State v. Andrews (N.J. Appeal No. A-72-18).

285. SCHNEIER, *supra* note 29, at 48. And, as our phones become even more interconnected with other smart devices, anyone with access to the phone will increasingly "be able to reconstruct a startlingly intimate model of who we are, what we think about, where we go, and what we do." *Id*. at 59.

information in a single place, puts it in the arrestee's pocket, and brings it to the prosecutorial doorstep. Documents that might have been stored in a dozen disparate locations are now conveniently consolidated on the phone, which is seized at the time of arrest. In one fell swoop, the government can now get evidence it might have taken weeks or months to obtain, via a series of searches and subpoenas. Law enforcement has never been able to gather so much, so quickly.

Moreover, much of the data on a cell phone is "qualitatively different" than anything that might have existed in the pre-digital age, including web browsing history, location information, and other application information that "can form a revealing montage of the user's life."[286] The ubiquity of phones has itself changed habits of communication. "As cell phone users turn away from phone calls and towards text messages and emails, cell phone data will increasingly track and memorialize all conversations. Already, Americans send texts and emails twice as often as they call."[287] Seized text messages and emails empower the government to perfectly reconstruct past conversations, a surveillance power never before possible. Thus, a cell phone "contains a broad array of private information never found in a home in any form" before smartphones existed.[288] The evidence contained on a phone is "an entirely different species" of intrusive, private information.[289] The lock may be new, but so is the quantity and quality of information behind it. To compare compelled decryption orders to the tax-record subpoena at issue in *Fisher* is "like saying a ride on horseback is materially indistinguishable from a flight to the moon."[290] Such orders "implicate privacy concerns far beyond those implicated by the" compulsion of tax records from an accountant.[291] Principles of equilibrium adjustment do not favor such an awesome government power.

Quite the contrary beyond the confines of the phone itself: the "zone of privacy" protected by self-incrimination provisions has never been smaller.[292] Technology has wrought enormous advances in powers of government surveillance. Everything we do on the Internet is tracked and recorded.[293] "If police want to know about a suspect, and the data has been collected by private third parties, those private companies are hard-pressed to push back and protect the information from lawful government requests."[294] And "[w]ith a valid warrant, police can obtain

286. *Riley*, 573 U.S. at 396.

287. Brief for the Electronic Privacy Information Center as Amicus Curiae at 10, State v. Andrews (N.J. Appeal No. A-72-18).

288. *Riley*, 573 U.S. at 397.

289. Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).

290. *Riley*, 573 U.S. at 393.

291. *Id.*

292. Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

293. FERGUSON, *supra* note 274, at 1–12 (detailing the surveillance powers of Internet data). *See also* SCHNEIER, *supra* note 29, at 57 (explaining how the surveillance power of smart devices is a function of their design and the commercial incentives of those who sell them).

294. FERGUSON, *supra* note 274, at 18.

most anything big data companies have collected for consumer purposes."[295] Even without a warrant, domestic surveillance programs have required the most popular Internet and phone companies to release the private communications of their users.[296] The "Internet of Things" has brought with it "the presence of interconnected devices . . . that are always on, are always with us and, together, ensure the total surveillance of everyday movements, habits, and intellectual endeavors."[297]

The police also directly collect, store, and analyze vast amounts of data about individual citizens. The National Crime Information Center contains 13 million active records searchable by officers from their patrol cars, 800,000 men and women are listed on federal and state sex-offender registries, the federal DNA database contains 12 million searchable DNA profiles, and 117 million Americans have their images in law enforcement databases.[298] "[T]echnology now exists that potentially could link 30 million private CCTV surveillance cameras together in a truly massive surveillance system."[299] Powers of surveillance have never been greater. "[T]he information age has robbed us of informational privacy" already.[300] Any attempt to restore the past equilibrium cannot ignore the full effect of this vast new surveillance technology.

Thus, just from a surveillance perspective, technology has inured massively to the benefit of law enforcement. The government simply does not need the added ability to compel citizens to turn over, actively and on threat of imprisonment, yet more intimate information about themselves. "[O]ur accusatory system of criminal justice demands that the government seeking to punish an individual produce the evidence against him by its own independent labors, rather than by the cruel, simple expedient of compelling it from his own mouth."[301] If encryption technology is novel, so too is the intrusive effect of forcing a citizen to turn over a decrypted digital device.

E. *Litigants and Courts Must Address State Constitutional Protections Without Lockstep Adherence to Fifth Amendment Precedent*

This is an ongoing constitutional conversation. As noted, about half of state constitutions have the same prohibition on a suspect being compelled to either "give" or "furnish" incriminating evidence,[302] making this an area ripe for state

295. *Id*. at 17.

296. KHIARA BRIDGES, THE POVERTY OF PRIVACY RIGHTS, 135–36 (2017).

297. *Id*. at 135.

298. FERGUSON, *supra* note 274, at 14–16, 97.

299. *Id*. at 101.

300. BRIDGES, *supra* note 296, at 139.

301. Miranda v. Arizona, 384 U.S. 436, 460 (1966).

302. 23 state constitutions have language analogous to that of Massachusetts. *See* ALA. CONST. art. I, § 6 ("compelled to give evidence against himself"); ARIZONA CONST. art. 2, § 10 ("compelled in any criminal case to give evidence against himself"); CONN. CONST. of 1818, art. I, § 9 ("compelled to give evidence against himself"); DEL. CONST. art. I, § 7 ("compelled to give evidence against himself"); ILLINOIS CONST. art. I, § 10 ("compelled in a criminal case to give evidence against himself"); KY. CONST. § 11 ("compelled to give evidence

constitutional law to provide heightened protection for criminal defendants. Before *Fisher*, "there was considerable authority that some state privileges prohibited any compelled activity, whether testimonial or not, giving rise to incriminating evidence or information implicating the person so compelled."[303] With the advent of new technologies, and the intrusive government surveillance that has come with it, the scope of state constitutional protection deserves re-examination.[304]

---

against himself"); LA. CONST. art. I, § 16 ("compelled to give evidence against himself"); ME. CONST., art. I § 6 ("compelled to furnish or give evidence against himself"); MD. CONST. DEC. OF RIGHTS, art. 22 ("compelled to give evidence against himself"); MISS. CONST. art. 3, § 26 ("compelled to give evidence against himself"); NEB. CONST. art. I, § 12 ("compelled, in any criminal case, to give evidence against himself"); N.H. CONST. Pt. 1, art. 15 ("compelled to accuse or furnish evidence against himself"); N.C. CONST. art. I, § 23 ("compelled to give self-incriminating evidence"); OKLA. CONST. art. II, § 21 ("compelled to give evidence which will tend to incriminate him"); PA. CONST. art. I, § 9 ("compelled to give evidence against himself"); R.I. CONST. art. I, § 13 ("compelled to give self-incriminating evidence"); S.D. CONST. art. VI, § 9 ("compelled in any criminal case to give evidence against himself"); TENN. CONST. art. I, § 9 ("compelled to give evidence against himself"); TEX. CONST. art. I, § 10 ("compelled to give evidence against himself"); UTAH CONST. art. I, § 12 ("compelled to give evidence against himself"); VT. CONST. ch. I, art. X ("compelled to give evidence against oneself"); VA. CONST. art. I, § 8 ("compelled in any criminal proceeding to give evidence against himself"); WASH. CONST. art. I, § 9 ("compelled in any criminal case to give evidence against himself").

303. *See* 1 MCCORMICK ON EVIDENCE, *supra* note 7, at § 124, at 727–28. Two states deviate slightly from *Fisher*'s federal line. Georgia—which has a state constitution phrased more like the Fifth Amendment, *see infra* note 304—forecloses a suspect from being compelled to "engage in an act which will create evidence incriminating the person." 1 MCCORMICK ON EVIDENCE, *supra* note 7, at § 124, at 728. But even Georgia courts do not protect a person from being "compelled to act so as to assist authorities in obtaining already existing evidence of this sort." *Id*. And New Jersey, which has no state constitutional provision against self-incrimination *at all*, *see infra* note 304, provides a limited "*Boyd*-like protection for the content of at least some private papers" under its common law. 1 MCCORMICK ON EVIDENCE, *supra* note 7, at § 137, at 776.

304. 24 states mirror the narrower text of the Fifth Amendment, prohibiting compelled "testimony" or service as a witness against oneself. *See* ALASKA CONST. art. I, § 9 ("compelled in any criminal proceeding to be a witness against himself"); ARKANSAS CONST. art. 2, § 8 ("compelled, in any criminal case, to be a witness against himself"); CALIFORNIA CONST. art. 1, § 15 ("compelled in a criminal cause to be a witness against themselves"); COLORADO CONST. art. II, § 18 ("compelled to testify against himself"); FLORIDA CONST. art. I, § 9 ("compelled in any criminal matter to be a witness against oneself"); GEORGIA CONST. art. I, § 1, Para. XVI ("compelled to give testimony"); HAWAII CONST. art. I, § 10 ("compelled in any criminal case to be a witness against oneself"); IDAHO CONST. art. I, § 13 ("compelled in any criminal case to be a witness against himself"); INDIANA CONST. art. I, § 14 ("compelled to testify against himself"); KANSAS CONST. BILL OF RIGHTS § 10 ("No person shall be a witness against himself"); MICH. CONST. art. I, § 17 ("compelled in any criminal case to be a witness against himself"); MINN. CONST. art. I, § 7 ("compelled in any criminal case to be a witness against himself"); MO. CONST. art. I, § 19 ("compelled to testify against himself"); MT. CONST. art. 2, § 25 ("compelled to testify against himself"); NEV. CONST. art. 1, § 8 ("compelled, in any criminal case, to be a witness against himself"); N.M. CONST. art. 2, § 15 ("compelled to testify against himself"); N.Y. CONST. art. 1, § 6 ("compelled in any criminal case to be a witness against himself"); N.D. CONST. art. 1, § 12 ("compelled in any criminal case to be a witness against himself"); OHIO CONST. art. I, § 10 ("compelled, in any criminal case, to be a witness against himself"); OR. CONST. art. I, § 12 ("compelled in any criminal prosecution to testify against himself"); S.C. CONST. art. I, § 12 ("compelled in any criminal case to be a witness against himself"); W. VA. CONST. art. III, § 5 ("compelled to be a witness against himself"); WIS. CONST. art. I, § 8 ("compelled in any criminal case to be a witness against himself"); WYO. CONST. art. I, § 11 ("compelled to testify against himself in any criminal case").

Iowa has no self-incrimination clause, but reads the protection into its due process provision. *See* Amana Soc. v. Selzer, 94 N.W.2d 337, 339 (Iowa 1959). New Jersey has a statute that protects against self-incrimination, *see* N.J. Stat. Ann. § 2A:84A-19, but no provision in its constitution. *See* State v. White, 142 A.2d 65, 70 (N.J. 1958).

Compelled decryption cases are fast appearing in state courts across the country. Indeed, two other state appellate courts decided compelled decryption cases the very same week as the SJC's opinion in *Jones*.[305] Neither addressed the scope of state constitutional protection. But state courts should not reflexively follow where *Fisher* and *Jones* have led—each constitution has its own rich history that deserves detailed examination. "[T]here is great value in the on-going dialogue among the states and between the states and the federal government on significant constitutional questions."[306] Before marching in lockstep with the SJC, other state supreme courts should interrogate the proper scope of their own privileges against self-incrimination and how they apply to compelled decryption.

But courts cannot do that alone. The onus will be on defense attorneys to represent their clients effectively by giving their state constitutions the rigorous historical treatment that this Article has tried to give to article 12.[307] While serving as a justice on the New Hampshire Supreme Court, Justice Souter explained why strong, developed advocacy is indispensable to a state court's proper consideration of state constitutional claims:

> It is the need of every appellate court for the participation of the bar in the process of trying to think sensibly and comprehensively about the questions that the judicial power has been established to answer. Nowhere is the need greater than in the field of State constitutional law, where we are asked so often to confront questions that have already been decided under the National Constitution. If we place too much reliance on federal precedent we will render the State rules a mere row of shadows; if we place too little, we will render State practice incoherent. If we are going to steer between these

---

305. *See* People v. Spicer, 125 N.E.3d 1286 (Ill. App. Ct. 2019) (disagreeing with *Jones*'s reasoning, and concluding "that the proper focus [of the foregone conclusion inquiry] is not on the passcode but on the information the passcode protects"); State v. Johnson, 576 S.W.3d 205 (Mo. Ct. App. 2019) (hewing almost exactly to the same reasoning as *Jones*). Another recent case, from the Oregon Court of Appeals, followed the *Jones* approach. *See* State v. Pittman, 300 Or. App. 147 (Oct. 16, 2019). And more cases are now pending in the Indiana Supreme Court, *see* Seo v. State, No. 18S-CR-595 (Ind. 2018), the Supreme Court of Pennsylvania, *see* Commonwealth v. Davis, 176 A.3d 869 (Pa. Super. 2017), allocatur granted Oct. 3, 2018, appeal docket 56 MAP 2018, and the Supreme Court of New Jersey, *see* State v. Andrews, No. A-72-18 (N.J.).

306. Hon. Scott Kafker, *Surveying Constitutional Territory: Book Review of Lawrence Friedman & Lynnea Thody's the Massachusetts State Constitution*, 42 RUTGERS U. L. REV. 913, 926 (2011).

307. Of course, the regular omission of any focus on state constitutional claims has a rational historical basis. As Judge Sutton explains, the relative under-protection of individual rights by state courts was a significant part of the explanation for the focus of litigants on federal constitutional claims. *See* SUTTON, *supra* note 31, at 14–15. But Judge Sutton also convincingly argues that there are specific reasons that litigants should focus on state constitutional arguments today. For example, state-court decisions apply to fewer people, thus avoiding the institutional hesitancy of a U.S. Supreme Court that "announce[s] rights and remedies for fifty States, one national government, and over 320 million people." *Id.* at 16. "In some settings, the challenge of imposing a constitutional solution on the whole country at once will increase the likelihood that federal constitutional law will be underenforced, that a 'federalism discount' will be applied to the right. State courts face no such problem in construing their own constitutions." *Id.* at 17; *see also id.* at 175.

> extremes, we will have to insist on developed advocacy from those who bring the cases before us.[308]

CONCLUSION

In *Riley v. California*, the Supreme Court held that the government was required to obtain a warrant before it could search a cell phone seized incident to arrest.[309] The government argued that the pre-existing "search incident to arrest" doctrine, which lets officers search an arrestee's person and the area within his immediate control, allowed an officer to open and search the contents of a person's cell phone.[310] The Supreme Court disagreed, recognizing that it was confronting a new physical and technological reality: everyone carries phones, and those phones' "immense storage capacity" far exceed the boundaries of what could previously be carried around in the physical world.[311] Given the intrusiveness of a search of a cell phone, the Court interposed a new limitation on an old doctrine. It did the same last year in *Carpenter v. United States*,[312] holding that the third-party doctrine does not apply to cell-site location information ("CSLI") because of its "depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection."[313] When new technology would allow old doctrines to enable highly intrusive searches, the Supreme Court has proven itself willing to take a second look.[314]

The same rethinking needs to occur in state constitutional law. Unfortunately, that did not happen in Massachusetts. The SJC's opinion in *Jones* is the culmination of decades of error. Following the Supreme Court's lead in its interpretation of the distinct language of the Fifth Amendment, the SJC has read the words "furnish evidence" entirely out of article 12. As currently understood, those words have no substantive meaning. From that premise, the result in *Jones* was inevitable. Though the case seems correctly decided by its terms, it is deeply flawed in its doctrinal assumptions. The SJC should return article 12 to the scope announced in *Boyd*: a protection against the compelled disclosure of private papers. Justice Louis Brandeis once called *Boyd* "a case that will be remembered as long as civil liberty lives in the United States."[315] State courts can and should revive it.

Again, *Fisher* involved a substantially different context than compelled decryption. The government sent a subpoena to a third party seeking a limited set of

---

308. State v. Bradberry, 522 A.2d 1380, 1389 (N.H. 1986) (Souter, J., concurring).

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

310. *Id.* at 398.

311. *Id.* at 393.

312. Carpenter v. United States, 138 S. Ct. 2206 (2018).

313. *Id.* at 2223.

314. *See id.* at 2222 ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents.").

315. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

the suspect's tax records.[316] The effort to apply *Fisher* to compelled decryption echoes the government's attempts to apply the search incident to arrest doctrine to the search of cell phones (in *Riley*) or the third-party doctrine to CSLI (in *Carpenter*). This argument ignores the massively different level of intrusiveness that the new digital technology has allowed. A case that requires a person's attorney to turn over tax records simply does not dictate the conclusion that a suspect can be forced to directly turn over all of his most private papers. Even setting aside the differences between the Fifth Amendment and article 12, *Fisher* arises on massively different facts than the circumstances presented by compelled decryption.

In choosing between which of two outcomes a state constitution might demand—loss of evidence or compulsion of deeply-intrusive disclosures—state courts can only seek guidance from the constitutional text, history, and past decisions interpreting their self-incrimination clauses. Massachusetts precedent weighs squarely in favor of protection against compelled decryption. Unlike the state prohibition against unreasonable searches, article 12 admits "no balancing of State-defendant interests" and does not "yield[] to 'reasonable' intrusions."[317] Indeed, "[t]hat shield is positive and unequivocal. It is subject to no condition."[318] Once the privilege attaches, it can only be overcome by a grant of immunity or by waiver.[319] If the prohibition on the compelled furnishing of evidence includes private documentary evidence, consistent with the common law privilege that article 12 was meant to memorialize, the rule that attaches is unbending. The SJC could not have used starker language. Compelled evidence may not even "furnish a link in the chain of evidence needed to prosecute the witness."[320]

Under article 12, the government cannot compel a suspect to disclose pre-existing private papers that will tend to incriminate him. As explained, such a holding would not require a complete overruling of the bodily evidence cases because the SJC could easily draw a line between communicative and non-communicative evidence (the same line the Supreme Court drew in *Schmerber*). In doing so, the SJC could narrow the protection even further, drawing a line between business records and private documents, as well as documents held by the suspect versus those held by a third party. No matter where the SJC sets the outer bounds of the article 12 privilege, the compelled production of private papers rightly falls within any proper understanding of its scope.

Consequently, the government can only obtain a compelled decryption order either by providing the suspect with immunity or if the suspect voluntarily waives his rights. If this results in the government losing some amount of evidence, that is the cost that the Framers of the privilege determined should be borne. Courts

316. *See Fisher*, 425 U.S. at 394.
317. Blaisdell v. Commonwealth, 364 N.E.2d 191, 197 (Mass. 1977).
318. *In re* Opinion of the Justices, 15 N.E.2d 662, 665 (Mass. 1938).
319. *Blaisdell*, 364 N.E.2d at 197.
320. Commonwealth v. Freeman, 817 N.E.2d 727, 733 (Mass. 2004).

cannot "reassess this judgment to make the prosecutor's job easier."[321] "[W]e should have no hesitation in holding that the Government must lose some cases rather than the people lose their immunities from compulsory self-incrimination."[322] And the government will not necessarily lose any evidence at all—it has other means of decrypting devices aside from forcing the suspect to furnish the code. It can also seek consent to search or the assistance of third parties. Eliminating the easiest way into the phone does not block the government's path; it just makes it slightly steeper. Any loss of evidence would be a choice borne of limited resources. Foreclosing compulsion will simply require the government to prioritize its cases, invest decryption resources efficiently, and reserve intrusive searches for the serious cases that most deserve them.

The text of article 12 was a product of experience, based on the scope of the English common law privilege, and reflects an intentional choice by its framers "that in a free society, based on respect for the individual, the determination of guilt or innocence by just procedures, in which the accused made no unwilling contribution to his conviction, was more important than punishing the guilty."[323] As technology allows searching government scrutiny of a suspect's most private sphere for incriminating evidence, state courts must re-examine first principles of state constitutional law to ensure that defendants not be enlisted in turning those materials over for government review.

321. Gamble v. United States, 138 S. Ct. 1960, 2009 (2019) (Gorsuch, J., dissenting).
322. Shapiro v. United States, 335 U.S. 1, 71 (1948) (Jackson, J., dissenting).
323. LEVY, *supra* note 53, at 432.