No. 19-6275

IN THE
# Supreme Court of the United States

DENNIS JONES,

*Petitioner,*

v.

COMMONWEALTH OF MASSACHUSETTS,

*Respondent.*

On Petition For A Writ Of Certiorari To
The Supreme Judicial Court for the
County of Suffolk

## BRIEF OF AMICUS CURIAE COMMITTEE FOR PUBLIC COUNSEL SERVICES IN SUPPORT OF PETITION FOR A WRIT OF CERTIORARI

DAVID RASSOUL RANGAVIZ
*Counsel of Record*
COMMITTEE FOR PUBLIC
COUNSEL SERVICES
44 Bromfield Street
Boston, MA 02108
(617) 910-5835
drangaviz@publiccounsel.net

*Attorney for Amicus Curiae*

## QUESTION PRESENTED

Whether the Fifth Amendment to the United States Constitution tolerates the compelled decryption of cell phones, which would force citizens to open for government review "a digital record of nearly every aspect of their lives." *Riley* v. *California*, 573 U.S. 373, 395 (2014).

## TABLE OF CONTENTS

Question Presented ..... i

Table of Authorities..... iii

Interest of Amicus Curiae.....1

Summary of Argument.....2

Argument.....4

I. *FISHER* IS CONTRARY TO THE ORIGINAL MEANING OF THE FIFTH AMENDMENT, WHICH PROTECTS AGAINST THE COMPELLED DISCLOSURE OF INCRIMINATING PRIVATE PAPERS .....4

II. EVEN IF *FISHER* IS RETAINED, THE ACT OF PRODUCTION DOCTRINE SHOULD NOT BE EXTENDED TO COMPELLED DECRYPTION .....12

III. THE SJC'S APPROACH TO COMPELLED DECRYPTION YIELDS ABSURD RESULTS AND ENSURES THE FIFTH AMENDMENT'S IMMINENT OBSOLESCENCE .....17

Conclusion .....25

## TABLE OF AUTHORITIES

**Cases**

*Boyd* v. *United States*,
116 U.S. 616 (1886).....3, 7, 8, 9
*Carpenter* v. *United States*,
138 S. Ct. 2206 (2018).....3, 4, 14, 21
*Commonwealth* v. *Jones*,
481 Mass. 540 (2019) .....17, 18, 20, 21
*Fisher* v. *United States*,
425 U.S. 391 (1976).....*passim*
*Gamble* v. *United States*,
No. 17-646 (U.S. June 17, 2019).....24
*King* v. *Purnell*,
96 Eng. Rep. 20 (K.B. 1748) .....5
*Malloy* v. *Hogan*,
378 U.S. 1 (1964).....7
*Minnesota* v. *Dickerson*,
508 U.S. 366 (1993).....12
*Olmstead* v. *United States*,
277 U.S. 438 (1928).....24
*Patton* v. *United States*,
281 U.S. 276 (1930).....1
*Riley* v. *California*,
573 U.S. 373 (2014).....*passim*
*Schmerber* v. *California*,
384 U.S. 757 (1966).....9, 10
*Shapiro* v. *United States*,
335 U.S. 1 (1948).....24
*Silverman* v. *United States*,
365 U.S. 505 (1961).....12

*United States* v. *Hubbell*,
530 U.S. 27 (2000).....*passim*
*United States* v. *Jones*,
565 U.S. 400 (2012).....23

**Statutes**

Mass. Gen. Laws ch. 211D, §§ 1, 2, 4 .....1

**Other Authorities**

Akhil Reed Amar & Renee B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 Mich. L. Rev. 857 (1995).....14
Bruce Schneier, *Click Here To Kill Everybody* (2018).....14, 22, 24
Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, 97 Tex. L. Rev. Online 73 (2019).....16, 23
David Rangaviz, *Compelled Decryption & State Constitutional Protection Against Self-Incrimination*, 57 Am. Crim. L. Rev. ____ (forthcoming 2019).....2
George Orwell, *1984* (1949).....21
Jeffrey S. Sutton, *51 Imperfect Solutions* (2018) .....6
Joseph Story, *Commentaries on the Constitution of the United States* (1833) .....6
Leonard W. Levy, *Origins of the Fifth Amendment: The Right Against Self-Incrimination* (1968) .....6
McCormick on Evidence (2013) .....19

Michael S. Pardo, *Disentangling the Fourth Amendment and the Self-Incrimination Clause*, 90 Iowa L. Rev. 1857 (2005) .....11
Michael W. McConnell, *Active Liberty: A Progressive Alternative to Textualism and Originalism?*, 119 Harv. L. Rev. 2387 (2006).....12
Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L.J. 989 (2018)....21, 22, 24
Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767 (2019).....17, 20
Richard A. Epstein, *The Classical Liberal Alternative to Progressive and Conservative Constitutionalism*, 77 U. Chi. L. Rev. 887 (2010) .....12
Richard Nagareda, *Compulsion "To Be a Witness" and the Resurrection of Boyd*, 74 N.Y.U. L. Rev. 1575 (1999) .....5, 6, 11, 20
Roseanna Sommers & Vanessa K. Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance*, 128 Yale L.J. 1962 (2019) .....22
Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. Pitt. L. Rev. 27 (1986) ..... passim
William J. Stuntz, *Self-Incrimination and Excuse*, 88 Colum. L. Rev. 1227 (1988) .....19

**Constitutional Provisions**

U.S. Const. amend. V .....2

## INTEREST OF AMICUS CURIAE

The Committee for Public Counsel Services ("CPCS") is a statewide public defender agency. Its responsibility is "to plan, oversee, and coordinate the delivery" of legal services to certain indigent litigants in Massachusetts, including those charged with crimes. See Mass. Gen. Laws ch. 211D, §§ 1, 2, 4.

The multiple errors in the decision of the Supreme Judicial Court of Massachusetts ("SJC"), from which Mr. Jones now seeks certiorari, will have a profound impact on the clients represented by CPCS. See *Patton* v. *United States*, 281 U.S. 276, 304 (1930) ("Whatever rule is adopted affects not only the defendant, but all others similarly situated."). The SJC's permissive approach to compelled decryption ensures that the government will readily seek to force Massachusetts defendants to unlock their phones for inspection. This is an issue of critical importance to many clients represented by CPCS.[1]

---

[1] Pursuant to Rule 37.6, counsel for amicus curiae states that no counsel for a party authored this brief in whole or in part, and no party or counsel for a party made a monetary contribution intended to fund the preparation or submission of this brief. No other person or entity made a monetary contribution to the preparation or submission of this brief. Pursuant to Rule 37.2, amicus curiae states that it provided counsel for both Petitioner and Respondent timely notice of its intent to file this brief, and both parties provided written consent to its filing.

## SUMMARY OF ARGUMENT

Compelled decryption is the fundamental self-incrimination issue of the digital age. When the government seizes cell phones during an arrest, or in the course of an investigation, it must get a warrant before searching them. See *Riley* v. *California*, 573 U.S. 373 (2014). But if a phone is locked with an encrypted passcode, the government has two choices: hack in, or force the suspect to decrypt the phone. The former is constrained only by the limits of the government's technical ability and resources; the latter is constrained by 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." U.S. Const. amend. V. See generally David Rangaviz, *Compelled Decryption & State Constitutional Protection Against Self-Incrimination*, 57 Am. Crim. L. Rev. ___ (forthcoming 2019) (making similar arguments to those herein as a matter of state constitutional law).

As explained in Mr. Jones's petition, lower courts have divided along multiple lines in regard to what Fifth Amendment rules apply in such circumstances. This brief does not endeavor to address those splits. It instead asks this Court to grant the petition to correct its own decades-old error, which has led lower courts down a road that allows the government to enlist defendants in exposing their most private papers for inspection, on threat of incarceration. The Framers of the Fifth Amendment never could have imagined this state of affairs. This Court should no longer tolerate it.

Until this Court's opinion in *Fisher* v. *United States*, 425 U.S. 391 (1976), no court would have even considered giving the government this power. But *Fisher* dramatically narrowed the scope of the Fifth Amendment – effectively overruling the more expansive protections of *Boyd* v. *United States*, 116 U.S. 616 (1886) – and held that it protects only against government compulsion of *testimonial* communications. Acts of production, like unlocking a phone, are not entitled to protection so long as the government already knows the testimony implicit in the act. For Fifth Amendment purposes, the contents of the documents derived from the act of production are, themselves, entirely irrelevant.

That is wrong. Nothing in the history of the Fifth Amendment supports such a cramped view of its protections. Indeed, three Justices of this Court have said so. See *United States* v. *Hubbell*, 530 U.S. 27, 49 (2000) (Thomas, J., concurring); *Carpenter* v. *United States*, 138 S. Ct. 2206, 2271 (2018) (Gorsuch, J., dissenting); Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. Pitt. L. Rev. 27, 35 (1986). But even if *Fisher* is right, its extension to compelled decryption is wrong. *Fisher* dealt with a subpoena for a limited set of financial records prepared by and in the possession of a third party, yet lower courts are passively extending it to allow the government to force suspects to directly disclose *all* of their most private papers. But see *Carpenter*, 138 S. Ct. at 2222 ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents.").

Only this Court can conduct the wholesale re-examination of Fifth Amendment precedent that compelled decryption demands. Absent a return to the original, correct understanding of the Fifth Amendment, judicial decisions about passwords will be wasted ink. In a world with phones that can be unlocked with a glance or a fingerprint, the Fifth Amendment will pose no barrier to government inspection. To avoid its planned obsolescence, the Fifth Amendment must protect what matters: the forced disclosure of incriminating, personal papers.

## ARGUMENT

### I. *FISHER* IS CONTRARY TO THE ORIGINAL MEANING OF THE FIFTH AMENDMENT, WHICH PROTECTS AGAINST THE COMPELLED DISCLOSURE OF INCRIMINATING PRIVATE PAPERS

Ironically, given the current scope of Fifth Amendment protection, there is an overwhelming consensus that the English common law privilege at the time of the adoption of the Fifth Amendment barred the compelled production of incriminating private documents. "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." *Hubbell*, 530 U.S. at 49 (Thomas, J., concurring). See also *Carpenter*, 138 S. Ct. at 2271 (Gorsuch, J., dissenting) ("[T]here 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."). This is not up for genuine debate. "All sources to address the point concur that common law at the time of the Fifth Amendment barred the compelled production of self-incriminatory documents." Richard Nagareda, *Compulsion "To Be a Witness" and the Resurrection of Boyd*, 74 N.Y.U. L. Rev. 1575, 1619 n.172 (1999) (collecting sources).

The most extensive treatment of the common law privilege is found in *King* v. *Purnell*, 96 Eng. Rep. 20 (K.B. 1748), in which 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. The vice-chancellor was himself the custodian of records, so the order would have required him to turn over self-incriminating materials. The King's Bench refused to issue the order, reasoning that "[t]he books were of a private nature" and a court may not "make a man produce evidence against himself, in a criminal prosecution." *Id*. Indeed, the Court stated that it knew of "no instance, wherein this court has granted a rule to inspect books in a criminal prosecution nakedly considered." *Id*.

Given this history, it should not be altogether 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.'" Nagareda, *supra* at 1606. And "[w]hen it

came time to draft the first eight amendments in the Bill of Rights … Madison and others drew from the existing state constitutions." Jeffrey S. Sutton, *51 Imperfect Solutions* at 11 (2018). Madison's novel phrasing of the Fifth Amendment – "[n]o person ... shall be compelled in any criminal case to be a witness against himself" – though it used slightly different words, did not narrow the scope of that existing privilege. See Nagareda, *supra* at 1603-25; see also 3 Joseph Story, *Commentaries on the Constitution of the United States* § 1782, pp. 662 (1833) ("This also is but an affirmance of a common law privilege."); *Hubbell*, 530 U.S. at 50 (Thomas, J., concurring) (collecting dictionaries of the founding era that define "the term 'witness' as a person who gives or furnishes evidence").

After the adoption of the state and federal constitutional protections against self-incrimination, "the earliest state and federal cases were in accord with that previous history" recognizing the scope of the privilege to extend to incriminating documents. Leonard W. Levy, *Origins of the Fifth Amendment: The Right Against Self-Incrimination* at 390 (1968). And the Congress itself, in passing the Judiciary Act of 1789, included a provision that would empower federal courts to "compel civil parties to produce their books or papers containing relevant evidence." *Id*. at 425. The belated addition of language limiting the scope of the self-incrimination privilege to just "criminal case[s]" – language that was not included in Madison's first draft of that clause – was done "with this pending legislation in mind." *Id*. at 426. That narrowing 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 provision to just "criminal cases" if that clause was not also thought to extend to pre-existing documents. See *Hubbell*, 530 U.S. at 53 n.3 (Thomas, J., concurring).

In *Boyd* v. *United States*, 116 U.S. 616 (1886), this Court decided the scope of the self-incrimination clause in accordance with the correct, original understanding that a "witness" means one who gives evidence. The Court reasoned that

> any 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.[2]

---

[2] The Fifth Amendment has been incorporated against the States via the Fourteenth Amendment. See *Malloy* v. *Hogan*, 378 U.S. 1, 6 (1964). As to state prosecutions, like this one, the stark language of this Court's 1886 opinion – and the apparent unanimity at that time on the meaning of the privilege – sheds light on exactly what right the drafters of the Fourteenth Amendment thought they were incorporating in 1868.

*Id*. at 631-32 (emphasis added). Nothing in *Boyd* suggested that the protection of the Fifth Amendment is reserved only for "testimonial" communications.

Yet this Court said exactly that in *Fisher*, rejecting *Boyd*'s correct understanding of the Fifth Amendment, and allowing the government to force a person to furnish incriminating evidence to be used against him in a criminal case. In addition to entirely ignoring the original meaning of the Fifth Amendment, *Fisher* suffered from two profound analytical flaws.

First, *Fisher* emphasized that *Boyd* had erred in a separate portion of its opinion, in which the Court had held that the government's subpoena also constituted an unreasonable *search* under the Fourth Amendment. That aspect of *Boyd*, to put it gently, was indeed very wrong. A subpoena is not a search at all. See Alito, *supra* at 35-36 ("[T]he immutable fact is that searches and seizures on the one hand, and subpoenas on the other, are quite different and are very differently regulated by the fourth and fifth amendments."). But the *Fisher* Court made it appear as though the two distinct holdings were somehow interrelated or interdependent, and that the error of one demanded the correction of the other.[3] That is

[3] As *Fisher* put it: "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." 425 U.S. at 409 (citation omitted).

equally wrong. *Boyd*'s view of the scope of the Fifth Amendment did not depend on its Fourth Amendment holding. It could have (and should have) stood on its own.

Second, the *Fisher* Court relied upon, and selectively cited language from, a new line of bodily evidence cases. Before *Fisher*, in *Schmerber* v. *California*, 384 U.S. 757 (1966), this Court had held that the extraction of a blood sample from a defendant who was suspected of drunk driving did not implicate the Fifth Amendment. 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." *Id.* at 761. But *Schmerber* also contemplated that the documents at issue in *Boyd* would fall comfortably on the "testimonial or communicative" side of that line, citing *Boyd* for the proposition that: "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." *Id.* at 763-64 (citing *Boyd*, 116 U.S. at 616). Thus, under *Schmerber*, "testimonial" evidence was meant to be synonymous with "communicative" evidence, like documents.

*Fisher* changed that. Purporting to follow *Schmerber* – while ignoring the fact that the opinion

had expressly reaffirmed the precise holding of *Boyd* that the Court was about to upend – the Court announced that it was "also clear that the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a Testimonial Communication that is incriminating." *Fisher*, 425 U.S. at 408. And the Court then completely redefined that zone of protection. A privilege meant for all of "an accused's communications, whatever form they might take," *Schmerber*, 384 U.S. at 763-64, was suddenly recast as one reserved only for "compelled *testimonial* communications." *Fisher*, 425 U.S. at 409 (emphasis added). Protection for "testimony *or* communications" was transformed, with a barely-audible tweak, into just "testimoni*al* communications." This Court has never acknowledged that sleight of hand.

*Fisher*'s holding was dubbed the "act of production" doctrine: when the government subpoenas documents, the Fifth Amendment only protects any assertions implicit in the actual "act of producing" those documents, but not the documents themselves. For instance, "[c]ompliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the [defendant]." *Id.* at 410. Of course, were that the entirety of *Fisher*'s holding, it would seem about as protective as *Boyd* – even the more limited testimonial act of production would not allow the compelled disclosure of private papers. To avoid this result, *Fisher* established both the "act of production" doctrine *and* an exception to it: the "foregone

conclusion" doctrine. If the government can prove that it *already knows* about the existence of the papers, then the 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." *Id.* at 411. The government obtains no *testimonial* advantage – distinct from its obvious evidentiary advantage – by compelling a suspect to tell it something that it already knows.

Neither the "act of production" doctrine nor the "foregone conclusion" exception has any grounding in the original meaning of the Fifth Amendment.[4] *Fisher* does not even pay lip service to the Framers or what they might have intended. The rule created there, out of whole cloth, is just the sort of "original-meaning-is-irrelevant, good-policy-is-constitutional-law school of jurisprudence" that has

---

[4] It appears that the foregone conclusion exception applies only to compelled acts of production and not compelled testimony. Indeed, that must be so. Were it otherwise, 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). 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* 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* at 1597-98.

been repeatedly disavowed. *Minnesota* v. *Dickerson*, 508 U.S. 366, 382 (1993) (Scalia, J., concurring). See Michael W. McConnell, *Active Liberty: A Progressive Alternative to Textualism and Originalism?*, 119 Harv. L. Rev. 2387, 2415 (2006) ("[Originalism] supplies an objective basis for judgment that does not merely reflect the judge's own ideological stance.").

Seldom is history so unanimous. The English common law privilege, and every state constitution of the founding era, forbade the government from forcing a citizen to furnish incriminating evidence against himself. Madison's turn of phrase "was synonymous with" that understanding. *Hubbell*, 530 U.S. at 53 (Thomas, J., concurring). And *Boyd* "was faithful to this historical conception of the privilege." *Fisher*, 425 U.S. at 419 (Brennan, J., concurring in judgment).

*Fisher* is not, and should be overruled.

## II. EVEN IF *FISHER* IS RETAINED, THE ACT OF PRODUCTION DOCTRINE SHOULD NOT BE EXTENDED TO COMPELLED DECRYPTION

Where a rule of decision lacks any foundation in the text, history, or purpose of the Constitution, this Court should – at the very least – "refuse to extend it one inch beyond its previous contours." Richard A. Epstein, *The Classical Liberal Alternative to Progressive and Conservative Constitutionalism*, 77 U. Chi. L. Rev. 887, 903 (2010). See *Silverman* v. *United States*, 365 U.S. 505, 512 (1961) (refusing to re-examine precedent, but also "declin[ing] to go

beyond it, by even a fraction of an inch"). Even if *Fisher* is not overruled, 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*; it is a marked extension. And "any extension of that reasoning to digital data has to rest on its own bottom." *Riley*, 573 U.S. at 393.

*Fisher* was a tax case. The IRS suspected that certain people had cheated on their taxes, those people transferred their tax documents to their attorneys, and the IRS issued a summons to the attorneys to get those documents. Thus, the case involved a subpoena for a limited class of documents, created by accountants, for tax purposes, in the possession of the target's attorney. The subpoena there sought documents of a far less private character than those found on modern cell phones, and it sought those documents from a third party. Indeed, the *Fisher* Court started its analysis by noting that the summons had not been directly issued to the accused. *Fisher*, 425 U.S. at 398 ("The taxpayer is the 'accused,' and nothing is being extorted from him."). And the Court acknowledged that these were business and financial records, recognizing the "[s]pecial problems of privacy" that arise when a subpoena seeks private papers. *Id*. at 401 n.7. Since *Fisher*, this Court has, on multiple occasions, "pointedly le[ft] th[e] question open" of whether the Fifth Amendment protects against the compelled disclosure of private papers. Akhil Reed Amar & Renee B. Lettow, *Fifth Amendment First*

*Principles: The Self-Incrimination Clause*, 93 Mich. L. Rev. 857, 888 n.144 (1995) (collecting cases).

That open question must now be answered. *Fisher* should not apply to private papers, which cell phones unavoidably contain in spades. "When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents." *Carpenter*, 138 S. Ct. at 2222. The effort to apply *Fisher* to compelled decryption echoes the government's past 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*) – it ignores the massively different level of intrusiveness that cell phones have allowed. Even 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." *Riley*, 573 U.S. at 393. And our phones are a gateway into all of our most private accounts that exist beyond the confines of the phone itself: email, social networking, banking, and more. "Your smartphone has evolved into a centralized security hub for pretty much everything." Bruce Schneier, *Click Here To Kill Everybody* at 48 (2018).

Modern cell phones combine, in a single, easily-searched package, documents that either never could have existed in the Founding era at all, or never would have existed together in the same place. Documents that might have been stored in a dozen disparate locations are now consolidated on

the phone, put in the arrestee's pocket, and conveniently delivered to the prosecutorial doorstep. This is the furthest thing from the third-party subpoena for tax records at issue in *Fisher*.

Perhaps the tenuous line between testimonial and documentary evidence made a modicum of sense in 1976, when cutting-edge technology involved a rotary dial, and this Court considered only narrow document subpoenas for business records. But it does not work in the 21st century. The breadth and depth of private information contained in modern cell phones simply did not exist when this Court invented the act of production doctrine. Today, we depend on our phones for recall. People have increasingly outsourced their brains to their phones – they correspond voluminously by email and text, use Google maps to drive everywhere, and no longer bother to learn phone numbers by heart. Information that was once kept in our minds is now stored on our phones. "They are a substitute for the perfect memory that humans lack." Alito, *supra* at 39. See also *Riley*, 573 U.S. at 385 ("[T]he proverbial visitor from Mars might conclude they were an important feature of human anatomy.").

Never has this Court faced 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. Today, technology allows a single act of production (entering a code) to unlock a mountain of one's most private

papers. 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." Alito, *supra* 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.").

In this context, *Fisher* is unworkable. A case that requires a third party to turn over a narrow set of financial records does not compel the conclusion that a suspect can be forced to directly turn over all of his most private papers. Indeed, Justice Marshall wrote separately in *Fisher* to emphasize his hope that the "Court's rationale provide[d] a persuasive basis for distinguishing between the corporate-document cases and those involving the papers of private citizens." *Fisher*, 425 U.S. at 432-33 (Marshall, J., concurring in judgment) ("[I]n 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."). That distinction has broken down. No lower court has questioned the premise of whether the act of production doctrine should apply to compelled decryption at all. If this Court does not overrule *Fisher*, it certainly should not extend it.

## III. THE SJC'S APPROACH TO COMPELLED DECRYPTION YIELDS ABSURD RESULTS AND ENSURES THE FIFTH AMENDMENT'S IMMINENT OBSOLESCENCE

Below, the SJC held that the government can obtain a compelled decryption order so long as it proves, as a foregone conclusion, that the suspect knows the passcode to the phone in question. See *Commonwealth* v. *Jones*, 481 Mass. 540, 551 (2019). The government need not make any showing about the *contents* of the phone to obtain the order; it is enough just to prove that the suspect knows the code. If this Court does not overrule *Fisher*, and even opts to extend it to compelled decryption, it cannot follow that approach.

The SJC's approach is absurd. For starters, it narrows the scope of Fifth Amendment protection as the government broadens its request for information. If the government had sought to have Mr. Jones turn over a *single* email, it would have had to describe the contents of that email with "reasonable particularity" to establish the predicate for application of *Fisher*'s foregone conclusion doctrine. As with any document subpoena, the government would have had to know something about the contents of that email to meet its burden. See Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767, 775 (2019). But if the government seeks a compelled decryption order – thereby forcing Mr. Jones likely to have to turn over *every* email he has ever sent or received – it needs only to prove that he

knows the code to the phone, with no showing required for the contents of *any* of his emails. A defendant subject to a compelled decryption order loses the protection of the "reasonable particularity" standard entirely. Thus, under the SJC's approach, greater protection is afforded to compelled disclosures that are far less intrusive.

And the SJC's analysis turns, quite explicitly, on pure semantics. The SJC recognized that the government can never force a suspect to actually tell it the passcode to the phone, for that is compelled *testimony* to which the foregone conclusion doctrine does not apply. See *Jones*, 481 Mass. at 547 n.9; *supra* note 4. Instead, 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." *Id.* (emphasis added). Thus, in the SJC's view, Fifth Amendment protection turns exclusively on the phrasing of the compulsive order: suspects are absolutely protected against telling the government their code, but must unlock their devices themselves upon request and hand them over immediately. That is a truly bizarre state of affairs. Both roads lead to precisely the same place: the phone unlocked for government inspection. It is silly to have so much turn on so little, and again points up the absurdity of staying so narrowly focused 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 his phone for inspection.

Even the scant protection of *Jones* is subject to easy evasion. If the government has no clue whether the suspect knows the code – and thus cannot meet its *Jones* burden – it can simply immunize the compelled act of production and agree not to use the fact that the suspect entered the code against him. But it would still be free to use the contents of the phone against the suspect because a grant of immunity need only be "as broad as the protection of the privilege" itself. McCormick on Evidence, Vol. 1, § 138 at 779 (2013). A subpoena for a specific set of documents, unlike a compelled decryption order, is "designed to elicit information about the *existence* of sources of potentially incriminating evidence," and so requires derivative use immunity. *Hubbell*, 530 U.S. at 43 (emphasis added). But if the act of entering a passcode to a phone says nothing at all about the existence of documents on the phone – as the SJC held below – "the government need not immunize" the defendant against the derivative use of that information when it compels the act of production. William J. Stuntz, *Self-Incrimination and Excuse*, 88 Colum. L. Rev. 1227, 1278 n.185 (1988). The government can immunize *just* the act of decryption, obtain a court order forcing the "immunized" suspect to enter the code, and then freely use the contents of the phone against him. Following the SJC's analysis, that appears to be doctrinally correct, but it makes no sense.

The source of all of this absurdity, and the SJC's fundamental mistake, is the careful wall it constructed between its legal analysis and the practical effect of its order. The SJC ignored the

obvious reality that no one actually cares about the act of decryption. Defendants do not resist these orders, and the government does not seek them, because the act of unlocking the phone might *itself* convey incriminating information. Both sides just care about the contents of the phone. See Kerr, *supra* at 795 (entry of the passcode "is a consequence of how the technology works, not evidence the government wants"). But the act of production doctrine "decouple[s] the content of documents from the act by which they are produced," giving it "an unreal, make-believe quality." Nagareda, *supra* at 1601 ("It is rather like the Wizard of Oz imploring supplicants to pay no attention to the man behind the curtain."). This legal artifice is "woefully out of touch with the realities of subpoena practice." Alito, *supra* at 46. The documents on the phone are what's really at stake, and they should be the focus of the analysis. By focusing on the act of production, while ignoring the derivative evidence, the SJC got it "precisely backward." Nagareda, *supra* at 1602. These cases should be about what they are about.

Ultimately, the decision below is the culmination of a self-incrimination jurisprudence that considers itself entirely unconcerned with the protection of privacy. The SJC simply assumed that privacy was the exclusive province of the Fourth Amendment. See *Jones*, 481 Mass. at 549 n.11. But that is not so. "Expressions are legion in opinions of this Court that the protection of personal privacy is a central purpose of the privilege against compelled self-incrimination." *Fisher*, 425 U.S. at 416 (Brennan, J., concurring in judgment) (collecting

cases). For some reason, this privacy rationale for the Fifth Amendment privilege has been lost to history, just as government compulsion has become most intimately intrusive.

Adherence to the SJC's approach will soon – even by its own terms – provide no protection at all. If this Court retains a narrow focus on testimonial communications, the next (and current) generation of smartphones will eliminate *all* protections against compelled decryption. See *Carpenter*, 138 S. Ct. at 2218 ("[T]he rule the Court adopts must take account of more sophisticated systems that are already in use or in development." (citation omitted)). Phones that unlock by facial recognition or fingerprint will be unprotected "because providing fingerprints or other body parts is not testimonial." Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L.J. 989, 1003 (2018). A self-incrimination jurisprudence that does not protect compelled private documents is destined for obsolescence in a 21st century in which even non-testimonial acts of production can yield "[t]he sum of an individual's private life." *Riley*, 573 U.S. at 394. In the words of the concurring Justice below, the SJC's approach "sounds the death knell for a constitutional protection against compelled self-incrimination in the digital age." *Jones*, 481 Mass. at 566 (Lenk, J., concurring).

* * *

The notion that "[n]othing [is] your own except the few cubic centimetres inside your skull," should stay in *1984*. George Orwell, *1984* at 27 (1949). Today's cell phones have "immense storage capacity,"

allowing citizens to "carry a cache of sensitive personal information with them as they [go] about their day." *Riley*, 573 U.S. at 393-95. And, as our phones become even more interconnected with other digital devices, anyone with access to them "will be able to reconstruct a startlingly intimate model of who we are, what we think about, where we go, and what we do." Schneier, *supra* at 59.

The only thing that stands between the government and this trove of information – information that the government intends to use as evidence at the defendant's criminal trial – is a password. The government seeks to force this defendant, under threat of incarceration, to unlock the digital door to this mass of private papers, which may lead to yet further incarceration. Under the Fifth Amendment, the police should not have the power to force suspects to decrypt their cell phones.

It bears emphasis that such a rule will not result in a complete loss of evidence. See generally Kerr & Schneier, *supra* at 996 (explaining the basic principles of encryption and the common "workarounds" that law enforcement can use to avoid it). The police can still seek consent to unlock and search a seized phone. 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 study in which 97.1% of people unlock their phones and hand them over upon request). And, to the extent that the evidence exists outside of the phone, the government can solicit the cooperation of

third parties to try to get it. See Choi, *supra* 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."). "In short, it is not empirically obvious that extending the self-incrimination privilege to cellphones would alter overall rates of criminal prosecution." *Id.*

But the cheapest, easiest way into a phone is to force the suspect to unlock it. And cheap searches are habit-forming. 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." *United States* v. *Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring). See also *id.* at 429 (Alito, J., concurring in judgment) (noting how, "[i]n the pre-computer age, the greatest protections of privacy were … practical" because intrusive surveillance was "difficult and costly and therefore rarely undertaken").

Eliminating the easiest way into a phone will not necessarily block the government's path; it just makes it a bit steeper. Foreclosing compulsion will require the government to prioritize its cases, selectively invest decryption resources, and reserve the most intrusive searches for the serious cases that most deserve them. "That encryption will stymie some government investigations does not make it unique. … The success of investigative tools and methods are always matters of chance." Kerr & Schneier, *supra* at 1013. Like any other investigative

technique, "the government must work with the inherently probabilistic nature of encryption workarounds." *Id.* ("No law enforcement technique works every time. The challenges of encryption are no exception to that general rule."). This is just a modern iteration of an old problem. "The notion that the world has never seen a technology that is impervious to detection is complete nonsense." Schneier, *supra* at 194.

Even if disallowing compelled decryption does result in the loss of evidence, that is the cost that the Framers of the privilege against self-incrimination themselves determined should be borne. "It is not for this Court to reassess this judgment to make the prosecutor's job easier." *Gamble* v. *United States*, No. 17-646, slip op. at 24 (U.S. June 17, 2019) (Gorsuch, J., dissenting). "[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." *Shapiro* v. *United States*, 335 U.S. 1, 71 (1948) (Jackson, J., dissenting). This Court should return the Fifth Amendment to its correct, original meaning – as a robust protection against the compelled disclosure of incriminating private papers. That privilege is far too important for the sort of fair-weather originalism that bends to the whim of law enforcement.

Justice Brandeis once called *Boyd* "a case that will be remembered as long as civil liberty lives in the United States." *Olmstead* v. *United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting). This Court should revive it.

## CONCLUSION

For these reasons, and those stated by Mr. Jones, this Court should grant the petition for a writ of certiorari.

Respectfully submitted,

DAVID RASSOUL RANGAVIZ
*Counsel of Record*
COMMITTEE FOR PUBLIC
COUNSEL SERVICES
44 Bromfield Street
Boston, MA 02108
(617) 910-5835
drangaviz@publiccounsel.net

*Attorney for Amicus Curiae*