TESTIMONY IN THE MACHINE: A GRADED TEST FOR COMPELLED DIGITAL DISCLOSURE AND THE RIGHT AGAINST SELF-INCRIMINATION UNDER ARTICLE 20(3)

Jitendra Singh Bhadouriya, Advocate, Madhya Pradesh High Court

ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023 have significantly expanded the State's practical capacity to compel production of digital devices, without addressing whether the act of unlocking such a device through a passcode, biometric credential, or hardware key is itself testimonial compulsion under Article 20(3) of the Constitution of India. This paper argues that existing Indian jurisprudence, properly read, already supplies the analytical tools needed to answer this question: State of Bombay v. Kathi Kalu Oghad and Selvi v. State of Karnataka, taken together, establish that a compelled act is testimonial when it requires an accused to draw on personal knowledge, regardless of the form the compulsion takes. Indian courts confronting compelled digital disclosure since 2020 have not converged on this test, producing a documented pattern of disagreement between the Karnataka High Court's decision in Virendra Khanna v. State of Karnataka and subsequent rulings, including the Delhi High Court's decision in Sanket Bhadresh Modi v. CBI. This paper further argues that the American "foregone conclusion" doctrine, the strongest available counter-argument, should not be imported into Article 20(3) analysis given its own contested status in the United States and its poor doctrinal fit with the mental-privacy rationale of Selvi. Applying this analysis to Prevention of Money Laundering Act enforcement practice, where digital seizure is now routine, this paper proposes a graded three-tier constitutional framework distinguishing passcodes, biometric credentials, and hardware security keys, offered as a proposal for further scrutiny rather than a settled conclusion, pending either legislative clarification or a properly framed test case before the Supreme Court of India.

Keywords: Article 20(3); Self-Incrimination; Compelled Decryption; Digital Evidence; Bharatiya Sakshya Adhiniyam; Bharatiya Nagarik Suraksha Sanhita; Testimonial Compulsion; Prevention of Money Laundering Act.

I. INTRODUCTION

The Bharatiya Sakshya Adhiniyam, 2023 ("BSA") and the Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS"), both operative since 1 July 2024, have brought renewed urgency to a question Indian courts have so far answered only inconsistently: can an investigating officer or a court compel an accused to disclose the password, PIN, pattern, biometric credential, or recovery key required to access a digital device, without violating the constitutional privilege against self-incrimination under Article 20(3) of the Constitution?

For the purposes of this paper, "compelled digital disclosure" refers to any state-directed requirement that an accused provide the means of access to a digital device or account including passwords, PINs, alphanumeric patterns, biometric unlocking (fingerprint or facial recognition), one-time passwords, recovery keys, and hardware security tokens.[1] These mechanisms are not interchangeable: each raises a distinct question of whether the accused is being made to communicate knowledge or merely to permit access, a distinction this paper treats as constitutionally significant.

The statutory architecture makes the question unavoidable. Section 94 of the BNSS empowers a court or an officer-in-charge to issue a written order requiring a person to produce a document, electronic communication, or communication device believed to contain relevant material,[2] with Section 96 providing a search-warrant backstop where compliance is doubted.[3] Once a device is accessed, Section 63 of the BSA governs how its contents become admissible evidence, subject to a certification requirement under the Act's Schedule a certificate from the person in possession of the device and, in addition, a separate certificate from an independent expert authenticating the record, including its hash value.[4] Read together, Sections 94 and 96 BNSS supply the mechanism of compulsion, while Section 63 BSA governs admissibility once access is obtained yet no provision in either code addresses whether the initial act of unlocking a device is itself a testimonial act protected by Article 20(3). Each of these provisions, examined in Part II, raises a live constitutional question that the statutory text itself leaves unanswered.

The Supreme Court has not resolved this question directly, and the matter may be closer to its docket than commonly assumed: a Special Leave Petition arising from proceedings connected

[1]This definition is adopted for the purposes of this paper and does not track a statutory definition; no BSA, BNSS, or IT Act provision defines "compelled digital disclosure" as such.
[2]Bharatiya Nagarik Suraksha Sanhita, 2023, § 94 (India).
[3]Bharatiya Nagarik Suraksha Sanhita, 2023, § 96 (India).
[4]Bharatiya Sakshya Adhiniyam, 2023, §§ 62–63 (India).

to Virendra Khanna v. State of Karnataka remains pending before the Supreme Court.[5] In Virendra Khanna, a single judge of the Karnataka High Court held that directing an accused to disclose a device password does not amount to testimonial compulsion, reasoning that the password functioned like a document or object rather than a communication of knowledge, and that resulting access to the device did not offend the right to privacy recognised in Justice K.S. Puttaswamy v. Union of India.[6] This paper argues that this reasoning sits uneasily against two other lines of authority: State of Bombay v. Kathi Kalu Oghad, which permits compulsion of physical attributes such as fingerprints and handwriting samples precisely because they exist independent of the accused's mental processes,[7] and Selvi v. State of Karnataka, which held that compelled narco-analysis and similar techniques violate Article 20(3) because they extract the contents of the accused's mind.[8] The relationship between these two lines of precedent, as applied to passwords and passcodes, remains unresolved, and this paper does not treat it as settled by Virendra Khanna alone a broader survey of subsequent High Court decisions is undertaken in Part IV to establish whether, and to what extent, a genuine doctrinal divergence exists.

A password or passcode arguably differs from the physical evidence contemplated in Kathi Kalu Oghad in a specific respect: it is content that exists only in the accused's memory, rather than a bodily attribute that exists independently of it a distinction increasingly discussed in comparative literature under the label of cognitive privacy. Biometric credentials complicate this picture further, since they are physical in one sense but, when used specifically to unlock a device containing self-incriminating material, may carry testimonial implications not present in the historical fingerprint or handwriting cases. Encryption adds a further layer: modern devices are, by design, inaccessible without the specific credential sought, which is part of why compelled-disclosure disputes have become frequent only in the smartphone era, and why this question has also occupied courts in the United States[9] and, in a different statutory form, the United Kingdom.[10]

---

[5]Special Leave Petition (Crl.) No. 1622/2022, arising from proceedings connected to Virendra Khanna v. State of Karnataka, W.P. No. 1983/2021 (Kar. H.C.), reported as pending before the Supreme Court of India as of the last recorded listing; the precise current status should be independently confirmed against the Supreme Court's cause list before reliance in the final draft.

[6]Virendra Khanna v. State of Karnataka, W.P. No. 11759/2020 (Kar. H.C. Mar. 12, 2021) (India).

[7]State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808 (India).

[8]Selvi v. State of Karnataka, (2010) 7 S.C.C. 263 (India).

[9]Riley v. California, 573 U.S. 373 (2014).

[10]Regulation of Investigatory Powers Act 2000, c. 23, §§ 49, 53 (U.K.).

Research question: Does compelling an accused to disclose the means of accessing a digital device constitute testimonial compulsion under Article 20(3), and if the answer varies by the type of credential involved, what constitutional test should govern that variation under the BSA-BNSS framework?

This paper proceeds doctrinally, through statutory and case-law analysis, supplemented by a comparative examination of United States and United Kingdom approaches to compelled decryption, and an applied case study of Prevention of Money Laundering Act ("PMLA") investigations, used here as an illustration of how the doctrinal questions raised in Parts II through V operate in a high-frequency enforcement context rather than as an independent line of argument.

Building on this analysis, this paper tentatively proposes as a matter for further scrutiny rather than a settled conclusion a graded framework distinguishing passcodes and patterns, biometric credentials, and hardware security keys for constitutional purposes, and defends this proposal against the strongest available counter-argument, the American foregone-conclusion doctrine.[11] The remainder of the paper proceeds as follows: Part II maps the BSA-BNSS-IT Act statutory architecture; Part III examines the Kathi Kalu Oghad–Selvi relationship in detail; Part IV surveys High Court decisions to establish the actual state of doctrinal consensus or divergence; Part V engages the foregone-conclusion doctrine and comparative law; Part VI applies the analysis to PMLA/ED practice; Part VII sets out the proposed graded framework; and Part VIII concludes with recommendations.

II. STATUTORY ARCHITECTURE: WHAT CHANGED AND WHY IT MATTERS

A. BNSS Section 94: The Compulsion Engine

Section 94 of the BNSS empowers a court, or an officer-in-charge of a police station, to issue a written order requiring any person to produce a document or thing expressly including electronic communications believed to be necessary for an investigation, inquiry, trial, or other proceeding.[12] Non-compliance is punishable as an offence. The provision is the direct successor to Section 91 of the erstwhile Code of Criminal Procedure, 1973,[13] but the BNSS

[11]Fisher v. United States, 425 U.S. 391 (1976).
[12]BNSS § 94, supra note 2.
[13]Code of Criminal Procedure, 1973, § 91 (India) (repealed and replaced by Bharatiya Nagarik Suraksha Sanhita, 2023, § 94).

makes explicit what the CrPC left to judicial interpretation: that "document" and "thing" extend to electronic communications and, by implication, the devices that store or transmit them.

Constitutional issue this creates: Section 94 speaks of compelling the production of a device or communication. It does not, on its face, address whether the person subject to the order can be compelled to provide the credential required to render that device's contents intelligible. A locked smartphone produced under Section 94 remains functionally inert without a password, PIN, or biometric input. The provision is silent on this second-order compulsion leaving it unclear whether Section 94 authorizes only physical production or extends to compelling the act of decryption itself.

B. BNSS Section 96: The Coercive Backstop

Where the court has reason to believe that a person to whom a Section 94 order is or would be addressed will not comply, Section 96 permits the issuance of a search warrant instead, authorizing search and seizure of the document or thing directly.[14] This shifts the mechanism from cooperative production to state-executed seizure.

Constitutional issue this creates: Section 96 resolves the compulsion problem for physical seizure of a device but does not resolve it for the device's contents where those contents are encrypted. Seizing a locked phone under a Section 96 warrant still leaves the investigating agency dependent on either forensic decryption tools or the accused's cooperation. The statute thus creates a practical incentive for investigating agencies to seek the credential directly from the accused a scenario examined through decided cases in Parts III and IV below without any statutory guidance on the constitutional limits of doing so.

C. BSA Sections 62–63: Admissibility, Not Compulsion

Section 63 of the BSA (read with Section 62, the enabling clause) governs the admissibility of electronic records as documentary evidence, replacing Sections 65A and 65B of the Indian Evidence Act, 1872.[15] It requires a certificate identifying how the electronic record was produced and confirming the proper functioning of the device involved, and where the record is produced from a device other than one regularly used to produce such records an additional

[14]BNSS § 96, supra note 3.
[15]Indian Evidence Act, 1872, §§ 65A–65B (India) (repealed and replaced by Bharatiya Sakshya Adhiniyam, 2023, § 63).

certificate authenticating the record, including its hash value, from an expert.[16]

Constitutional issue this creates: Section 63 governs the evidentiary status of a record once it has been obtained. It presupposes that access has already occurred and says nothing about how that access was procured. This creates the analytical seam this paper relies on: Sections 94 and 96 BNSS govern the moment of compulsion, while Section 63 BSA governs what happens afterward. A court applying Section 63 to admit the contents of a decrypted phone is not thereby ruling on whether the decryption itself was constitutionally compelled yet in practice, as the case law shows, courts asked to enforce Section 94 orders have had to grapple with the Article 20(3) question with no statutory signpost from either code.

D. IT Act Section 69: The Parallel Track

Section 69 of the Information Technology Act, 2000, separately empowers the Central or State Government to direct any agency to intercept, monitor, or decrypt information transmitted through a computer resource, and imposes a duty on the subscriber or person in charge to extend "all facilities and technical assistance" when called upon.[17] This operates independently of BNSS Sections 94/96 and is triggered by executive direction rather than judicial or investigative order in the course of a specific criminal proceeding.

Constitutional issue this creates: Section 69's "technical assistance" language is broad enough to potentially encompass compelled disclosure of a password or decryption key, again without addressing Article 20(3). Because it operates on a separate statutory track from the BNSS, an investigating agency theoretically has two independent legal bases to seek device access raising a further question about whether this parallel structure allows circumvention of whatever constitutional limit eventually applies to BNSS-based compulsion.

E. Synthesis

Taken together, these four provisions reveal a statutory architecture built for a pre-encryption world, retrofitted onto smartphones and cloud-linked devices without confronting the constitutional question they generate. BNSS Sections 94 and 96 compel production; the IT Act's Section 69 compels technical assistance; and BSA Section 63 governs what may be done

[16]BSA §§ 62–63, supra note 4.
[17]Information Technology Act, 2000, § 69 (India).

with whatever is obtained yet none of the three asks whether the specific act of supplying a password, pattern, or biometric credential is itself testimonial. This is not an oversight the legislature can be faulted for in isolation: the CrPC provisions BNSS Sections 94 and 96 replace were drafted for physical documents and objects, where the accused's state of mind was rarely in issue. Applying that same framework to a credential that exists only in the accused's memory is where the constitutional seam opens up and it is this seam, rather than any single provision, that Part III now examines through the Kathi Kalu Oghad–Selvi relationship.

III. THE TESTIMONIAL/PHYSICAL EVIDENCE LINE CONFRONTING KATHI KALU OGHAD DIRECTLY

A. The Actual Kathi Kalu Oghad Test

The eleven-judge bench in State of Bombay v. Kathi Kalu Oghad[18] is frequently summarized as drawing a line between "physical" and "testimonial" evidence. This is imprecise. The Court's actual reasoning was narrower and more demanding: an accused becomes a "witness" against himself, within the meaning of Article 20(3), only through a positive volitional act that furnishes evidence by imparting personal knowledge relevant to a fact in issue. Specimen handwriting, signatures, and thumb impressions were held not to attract Article 20(3) not because they are "physical" in some abstract sense, but because they convey no knowledge held by the accused they merely provide a sample for comparison, functionally no different from the accused's outward appearance being observed by a witness. The accused giving a thumb impression does not tell the investigating agency anything he knows; he merely makes available a physical characteristic that exists independent of, and is unaffected by, what he knows or believes.

This precision matters because it changes what the Virendra Khanna court needed to establish, and did not. If the correct question under Kathi Kalu Oghad is whether the act imparts personal knowledge, then the relevant inquiry for a password is not "is a password like a fingerprint" but "does supplying a password communicate something the accused knows." Framed this way, the answer is not obviously favorable to the Virendra Khanna holding.

B. The Selvi Extension and the Concept of Mental Privacy

[18]Kathi Kalu Oghad, supra note 7.

Selvi v. State of Karnataka,[19] decided by a three-judge bench, extended the Kathi Kalu Oghad framework to techniques narcoanalysis, polygraph examination, and Brain Electrical Activation Profile testing that involve no traditional "communication" at all, yet the Court held these violate Article 20(3) because they involve the involuntary extraction of personal knowledge from a person's mind. The Court's introduction of "mental privacy" as an organizing concept confirms that the constitutional inquiry tracks the source of the evidence the accused's own mind rather than the form in which it is extracted, whether verbal, physical, or physiological.

Selvi is therefore best read not as a departure from Kathi Kalu Oghad but as its logical extension: both cases ask whether the evidentiary act draws on the contents of the accused's mind. Read together, they yield a single underlying test evidence is testimonial, and therefore protected, when it requires the accused to draw on personal knowledge to produce it, regardless of the mechanism used to extract that knowledge.

C. Applying the Test to Passwords, Patterns, and Biometrics

A password or alphanumeric passcode is, on this reading, a paradigm case of testimonial evidence. It exists nowhere except in the accused's memory; producing it necessarily requires the accused to recall and communicate something he alone knows. It is functionally indistinguishable from being asked to state a fact from memory the very act Kathi Kalu Oghad treated as testimonial, and Selvi confirmed remains testimonial regardless of the extraction method.

A pattern lock sits in the same category: the sequence exists only as a memorized motor routine, and its disclosure requires the accused to draw on that memory.

Biometric credentials present a genuinely harder case, and this paper does not treat them as automatically falling into either category. A fingerprint or facial scan is, in the narrow Kathi Kalu Oghad sense, a physical attribute rather than a piece of knowledge the accused need not "know" or "recall" anything to provide it. But this framing was developed for identification and comparison purposes, not for using a physical attribute as the specific key to unlock a device containing potentially incriminating content. Compelling a fingerprint for comparison against a crime-scene print is a different act, constitutionally, from compelling a fingerprint for

[19]Selvi, supra note 8.

the specific purpose of decrypting a phone even though the physical act performed by the accused may look identical. This distinction between the nature of the act and the evidentiary purpose it serves is underdeveloped in existing Indian case law and is where this paper's proposed graded framework (Part VII) does its central work.

D. Where This Leaves Virendra Khanna

Virendra Khanna's reasoning that a password functions like a document or object under Section 139 of the Indian Evidence Act, 1872[20] does not engage with the Kathi Kalu Oghad/Selvi personal-knowledge test at all. Section 139 addresses whether a person producing a document under summons thereby becomes a "witness" for cross-examination purposes; Kathi Kalu Oghad itself clarified that Section 139 is not a guide to the constitutional meaning of "witness" under Article 20(3), which must be understood in its natural sense. Virendra Khanna's reliance on Section 139 to resolve an Article 20(3) question therefore rests on a provision the Supreme Court had already cautioned against using for that exact purpose a point subsequently recognized, in substance, by two later tribunals returning directly to Selvi's mental-privacy framework instead: a Special CBI Court in CBI v. Mahesh Kumar Sharma & Ors.[21] and the Delhi High Court in Sanket Bhadresh Modi v. CBI.[22]

IV. THE HIGH COURT SPLIT EMPIRICAL MAPPING

A. Table of Decisions

Case	**Court & Level**	**Date**	**Holding**	**Reasoning**
Virendra Khanna v. State of Karnataka, W.P. No. 11759/2020	Karnataka High Court (single judge, Govindaraj, J.)	12 Mar 2021	Accused CAN be compelled to disclose password	Treated password disclosure as akin to production of a document/object under S.139, Evidence Act, 1872; found no Article 20(3)

[20]Indian Evidence Act, 1872, § 139 (India).
[21]CBI v. Mahesh Kumar Sharma & Ors., Spl. Case (Spl. CBI Ct., Rouse Avenue Dist. Cts., Delhi, order dated Oct. 29, 2022) (India) (Naresh Kumar Laka, Spl. J.).
[22]Sanket Bhadresh Modi v. CBI, Bail Appln. (Del. H.C. order dated Dec. 18, 2023) (India) (Jasmeet Singh, J.).

				violation
CBI v. Mahesh Kumar Sharma & Ors.	Special CBI Court, Rouse Avenue, Delhi (trial court)	29 Oct 2022	Accused CANNOT be compelled to disclose password	Relied on Article 20(3) and S.161(2) CrPC; held IO may still access data via specialized forensic agency without accused's cooperation
Sanket Bhadresh Modi v. CBI	Delhi High Court (Jasmeet Singh, J.)	18 Dec 2023	Accused CANNOT be coerced to disclose password	Made in a bail application; grounded in Article 20(3); held investigating agency cannot expect accused to “sing in a tune which is music to their ears”

B. Assessing Whether a Genuine Split Exists

A rigorous reading requires distinguishing precedential weight rather than treating all three decisions as equivalent. Virendra Khanna[23] is the only High Court decision squarely deciding the Article 20(3) question as its central issue, in a writ petition brought for that purpose. Mahesh Kumar Sharma[24] is a trial-court order, carrying persuasive rather than binding authority, though notable for directly engaging Selvi-style reasoning rather than Kathi Kalu Oghad. Sanket Bhadresh Modi,[25] while delivered by the Delhi High Court, arose in a bail application the Article 20(3) finding, though clearly stated, was not the central relief sought and may be characterized as obiter rather than a considered holding on the constitutional question.

This paper's position is therefore not that a settled, binding High Court split exists in the formal

[23]Virendra Khanna, supra note 6.
[24]Mahesh Kumar Sharma, supra note 21.
[25]Sanket Bhadresh Modi, supra note 22.

sense of two coordinate benches squarely disagreeing on ratio. Rather, what exists is a consistent pattern of disagreement in reasoning and outcome across every court that has confronted the question post-2020 one High Court permitting compulsion via Kathi Kalu Oghad/Section 139 reasoning, and two subsequent tribunals (one trial court, one High Court) rejecting compulsion via Selvi-style reasoning, without either of the latter two decisions directly overruling or even engaging Virendra Khanna. This pattern real disagreement without resolution is arguably a more precise and more troubling description of the current state of the law than a simple "split," because it means the governing precedent for any given accused currently depends on which forum hears the matter, with no mechanism yet forcing convergence.

C. Why the Divergence Is Doctrinally Predictable

The divergence traces directly to the analytical error identified in Part III: Virendra Khanna resolved the question through Section 139 of the Evidence Act[26] a provision Kathi Kalu Oghad itself cautioned was not a guide to the constitutional meaning of "witness." Mahesh Kumar Sharma and Sanket Bhadresh Modi, by returning to Article 20(3) and, implicitly, the Selvi personal-knowledge framework, arrive at the opposite conclusion because they are, in effect, asking the correct doctrinal question. The disagreement is not a matter of judicial discretion or differing values it reflects two different doctrinal starting points, one of which, per Part III's analysis, is more faithful to Kathi Kalu Oghad and Selvi properly understood. This is the paper's central empirical finding supporting the case for a definitive graded test rather than continued forum-dependent adjudication.

V. THE FOREGONE CONCLUSION PROBLEM

A. The Doctrine and Its Origins

The strongest available argument against this paper's proposed protection for passcodes comes not from Indian law but from the United States. In Fisher v. United States,[27] the Supreme Court held that a compelled act of production does not violate the Fifth Amendment privilege against self-incrimination where the act's testimonial component "add[s] little or nothing to the sum total of the Government's information" because the government already independently knows

[26]Evidence Act § 139, supra note 20.
[27]Fisher, supra note 11.

what the act would reveal, the incidental testimony implicit in the act is a "foregone conclusion." United States v. Hubbell[28] refined this into an operative test: the government must demonstrate, with reasonable particularity, prior knowledge of the existence, possession, and authenticity of the material sought before the doctrine can apply.

Applied to compelled decryption, the argument runs as follows: when the state already knows an individual controls a specific device and can operate it, requiring that individual to enter a passcode reveals nothing beyond the fact that the passcode is known to them a fact the state already presumes. On this reasoning, compelling passcode entry does not violate the privilege because the "testimony" implicit in the act adds nothing to what the government already knows.

B. The Doctrine Has Split American Courts, Not Resolved Them

Despite its apparent simplicity, the foregone conclusion doctrine has produced sharp disagreement even within the U.S. system whose Fifth Amendment jurisprudence generated it. The Massachusetts Supreme Judicial Court in Commonwealth v. Jones[29] and the New Jersey Supreme Court in State v. Andrews[30] applied the doctrine to compel passcode disclosure. The Pennsylvania Supreme Court in Commonwealth v. Davis[31] and the Indiana Supreme Court in Seo v. State[32] reached the opposite conclusion, holding that compelled passcode disclosure remains privileged and declining to extend the foregone conclusion doctrine to this context at all.

This split matters for the present argument in two ways. First, it demonstrates that even courts operating within the doctrine's home jurisdiction cannot agree on its proper scope in the digital context. Second, the U.S. Supreme Court itself has never extended the foregone conclusion doctrine beyond business records of the kind at issue in Fisher and Hubbell, expressly flagging "special problems of privacy" where more personal material its own example was a diary is involved. A smartphone, holding the functional equivalent of an individual's diary, correspondence, financial records, and private communications combined, sits closer to the category the U.S. Supreme Court has itself declined to extend the doctrine to than to the

[28]United States v. Hubbell, 530 U.S. 27, 45 (2000).
[29]Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019).
[30]State v. Andrews, 234 A.3d 1254 (N.J. 2020).
[31]Commonwealth v. Davis, 220 A.3d 534 (Pa. 2019).
[32]Seo v. State, 148 N.E.3d 952 (Ind. 2020).

corporate records at issue in Fisher. This is reinforced by Riley v. California,[33] where the Court held that cell phones differ "in both a quantitative and a qualitative sense" from other physical objects a person might carry a holding about Fourth Amendment doctrine, but one whose reasoning about the distinctive character of digital devices applies with equal force to the Fifth Amendment question addressed here.

C. Why Article 20(3) Provides Weaker, Not Stronger, Grounds for Importing the Doctrine

Even setting aside the doctrine's contested status in its own jurisdiction, this paper argues it should not be imported into Article 20(3) analysis, for a reason specific to Indian doctrine rather than a general skepticism of American law. The foregone conclusion doctrine is a creature of the U.S. "act of production" framework, which asks whether the act of producing something is testimonial a framework concerned with what the act itself implicitly asserts, independent of the content ultimately produced. Selvi, by contrast, locates the constitutional harm in the involuntary extraction of the contents of the accused's mind the violation is complete at the point personal knowledge is compelled out of the accused, regardless of whether the government could have obtained the same result through other means. Under this reasoning, whether the government "already knew" the accused could access the device is beside the point: the constitutional injury identified in Selvi is the compelled extraction itself, not the marginal evidentiary value of what is extracted. A doctrine built to measure incremental evidentiary contribution does not sit naturally alongside a doctrine built to protect the inviolability of the accused's mind.

D. The United Kingdom's Alternative Model

The United Kingdom takes a different approach entirely, one that avoids the foregone conclusion inquiry by making non-disclosure itself a distinct criminal offence rather than treating disclosure as compellable evidence. Section 49 of the Regulation of Investigatory Powers Act, 2000, empowers specified authorities to serve a notice requiring disclosure of a key or password to protected information, subject to necessity and proportionality requirements; Section 53 makes knowing failure to comply, without reasonable excuse, a separate offence punishable by up to two years' imprisonment (five years in cases involving national security or child indecency).[34] This model sidesteps the self-incrimination question by

[33]Riley, supra note 9.
[34]RIPA §§ 49, 53, supra note 10.

structurally decoupling the request for the password from the criminal proceeding the password might incriminate the accused in. Whether this structure is itself compatible with a right against self-incrimination is a separate and unresolved question in UK law, but it illustrates that the American path is not the only model available to Indian lawmakers considering a legislative fix.

E. Conclusion on the Foregone Conclusion Problem

The strongest counter-argument to this paper's proposed graded framework does not, on close examination, defeat it. The foregone conclusion doctrine remains contested in its jurisdiction of origin, has never been extended by the U.S. Supreme Court to material as personal as smartphone contents, and rests on a theory of constitutional harm incremental evidentiary contribution that is foreign to the mental-privacy rationale Selvi has already established as the operative Indian standard. This paper therefore treats the foregone conclusion doctrine as inapplicable to passcode disclosure under Article 20(3), while acknowledging, per Part III, that biometric credentials may warrant separate treatment precisely because they do not implicate the same act-of-memory concern.

VI. APPLIED CASE STUDY: PMLA/ED DIGITAL SEIZURE PRACTICE

A. The Section 50 Framework and Vijay Madanlal's Narrow Holding

Section 50 of the PMLA empowers ED officers to summon any person to give evidence or produce records, and compels the summoned person to state the truth, with Section 63 of the Act penalizing refusal to answer.[35] In Vijay Madanlal Choudhary v. Union of India,[36] a three-judge bench upheld this framework against an Article 20(3) challenge but on a narrower ground than is often assumed in commentary. The Court did not hold that Article 20(3) has no application to PMLA proceedings; it held that ED officers are not "police officers" for the purposes of the constitutional provision, and that a person summoned under Section 50 is not necessarily an "accused" at the point of summons, since the provision operates as an inquiry rather than an investigation.

B. Why This Reasoning Does Not Resolve the Digital Disclosure Question

[35]Prevention of Money Laundering Act, 2002, §§ 50, 63 (India).
[36]Vijay Madanlal Choudhary v. Union of India, 2022 SCC OnLine SC 929 (India).

This reasoning, while sufficient to dispose of the oral-statement challenge in Vijay Madanlal, does not straightforwardly extend to compelled digital disclosure, for two reasons this paper considers significant.

First, Vijay Madanlal's holding depends on the summoned person's status as a non-accused witness at the time of the Section 50 order. Once a person is formally arrested[37] a common sequence in ED practice, where device seizure typically accompanies or follows arrest that person is unambiguously an "accused" for Article 20(3) purposes, and Vijay Madanlal's rationale for excluding Article 20(3) protection no longer applies on its own terms. The Supreme Court's later recognition in Prem Prakash v. Union of India[38] that Section 50 statements made while an accused is in custody are inadmissible if incriminating confirms that the Court itself treats the protection as reviving once custodial/accused status attaches. Compelled device disclosure sought from an arrested PMLA accused therefore falls outside the specific carve-out Vijay Madanlal created, and squarely within the Kathi Kalu Oghad–Selvi framework developed in Part III.

Second, and more fundamentally, Vijay Madanlal addressed compelled oral statements, not compelled disclosure of a memorized credential to unlock a device. Even if an ED officer could validly compel truthful answers from a non-accused witness under Section 50, extending that same logic to compel a passcode which, per Part III, is testimonial regardless of the answerer's formal procedural status would require treating "stating the truth about a fact" and "producing the specific memorized key that unlocks one's own device" as equivalent acts. This paper argues they are not: the former is compelled testimony about external facts, permissible against a non-accused witness in limited circumstances; the latter is compelled extraction of a fact that exists only within the person's own mind about their own device, which is precisely the harm Selvi identifies regardless of the summoned person's formal label.

C. Applying the Graded Framework to an ED Seizure Scenario

Consider a representative scenario: the ED, investigating a scheduled offence generating proceeds of crime, arrests an accused and seeks access to a seized smartphone believed to contain financial records and communications relevant to the alleged laundering. Applying the

[37]Bharatiya Nagarik Suraksha Sanhita, 2023, § 19 (India) (power of arrest, applicable to arrests carried out by the Enforcement Directorate under its own statutory arrest power in conjunction with the Prevention of Money Laundering Act, 2002).
[38]Prem Prakash v. Union of India Through the Directorate of Enforcement, 2024 INSC 637

framework proposed in Part VII: if the device is protected by a passcode or pattern, the accused's Article 20(3) protection attaches directly, since the accused's formal status leaves no room for Vijay Madanlal's non-accused carve-out and the compelled entry is a paradigm case of testimonial extraction under Selvi. If the device is protected by biometric authentication, the ED would need to independently establish, before a magistrate, a proportionality justification for compelling that specific biometric act analogous to the judicial-authorization requirement already familiar from the search-warrant procedure under BNSS Section 96. If the ED instead seeks to compel disclosure of a hardware security key or a recovery phrase stored in a separate physical token, this paper's framework treats that as never compellable absent independent corroborating evidence the accused controls the device's contents, since compelling production of the token itself does not require the accused to draw on memory at all.

D. The Live, Unresolved Status of the Underlying Question

This scenario is not hypothetical. A writ petition currently pending before the Supreme Court challenges the constitutional validity of Sections 50 and 63 of the PMLA directly on Article 20(3) and Article 21 grounds.[39] While that petition does not squarely raise the digital-disclosure question addressed in this paper, its pendency confirms that the boundaries of Vijay Madanlal's holding remain actively contested before the apex court, and reinforces this paper's broader argument that the interaction between PMLA enforcement practice, the BSA-BNSS compulsion framework, and Article 20(3) is an open question awaiting either legislative clarification or a properly framed test case.

VII. THE PROPOSED GRADED FRAMEWORK

A. Preliminary Framing

The analysis in Parts III through VI supports a single underlying conclusion: the constitutional treatment of compelled digital disclosure cannot be resolved by a single rule applied uniformly across passwords, patterns, biometrics, and hardware keys, because these mechanisms differ in whether they require the accused to draw on personal knowledge. What follows is offered as a proposal for further scrutiny, not as a settled doctrinal conclusion its purpose is to give the Kathi Kalu Oghad–Selvi personal-knowledge test, developed in Part III, an operative form capable of guiding investigating agencies and courts applying BNSS Sections 94 and 96 in

[39]Dr. Govind Singh v. Union of India & Ors., W.P. (Crl.) No. 65 of 2023 (S.C. Mar. 28, 2023) (notice issued).

practice.

B. Tier One: Passcodes and Patterns Per Se Testimonial

A passcode, PIN, or pattern lock exists only in the accused's memory. Producing it necessarily requires the accused to recall and communicate a fact known only to them, satisfying Kathi Kalu Oghad's "positive volitional act... imparting personal knowledge" test directly, and falling within the mental-privacy protection Selvi extended to non-verbal extraction of mental contents. This paper proposes that disclosure of this category be treated as per se testimonial and therefore protected under Article 20(3), regardless of the investigating agency's independent knowledge that the accused can access the device for the reasons given in Part V, the foregone conclusion doctrine's incremental-evidentiary-value inquiry does not track the harm Selvi identifies. The protection proposed here does not prevent the state from seeking the device's contents through other lawful means, including forensic decryption, but it forecloses compelling the accused personally to supply the memorized credential.

C. Tier Two: Biometric Credentials Conditionally Compellable

Biometric unlocking fingerprint or facial recognition does not require the accused to draw on memory in the same sense; the physical attribute exists independent of the accused's mental processes, placing it closer to the Kathi Kalu Oghad line proper. But Part III's analysis identified a complication Kathi Kalu Oghad did not contemplate: a biometric credential used specifically to unlock a device, rather than merely for identification or comparison, functions as the practical equivalent of a key to potentially incriminating content, and the accused's compelled cooperation still carries an implicit assertion of possession and control over that content.

This paper proposes that biometric compulsion be permitted only upon prior judicial authorization, supported by a proportionality showing along the lines developed in Justice K.S. Puttaswamy v. Union of India[40] requiring the investigating agency to demonstrate a legitimate investigative aim, a rational connection between the biometric compulsion sought and that aim, absence of a less intrusive alternative, and safeguards against overbroad access to the device's full contents once unlocked. This tracks the existing statutory logic of BNSS Section 96, which already requires a magistrate's involvement where voluntary compliance is doubted, and would

[40]Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).

extend a comparable judicial check to the specific act of biometric compulsion rather than leaving it to unilateral investigative discretion.

D. Tier Three: Hardware Security Keys and Recovery Phrases Never Compellable Absent Independent Corroboration

Hardware security tokens and recovery phrases occupy a distinct category: unlike a memorized passcode, a hardware key is a physical object capable of seizure through ordinary search and seizure procedure without requiring the accused to communicate anything. Where such a token can be independently located and seized, no compulsion of the accused's knowledge is necessary at all, and this paper proposes that agencies be required to pursue that route rather than compelling the accused to identify, retrieve, or explain the token's location or function since doing so would reintroduce the same personal-knowledge extraction this framework otherwise seeks to prevent. Compulsion in this category should be treated as impermissible unless the state can independently corroborate, through evidence other than the accused's own statements, both the existence of the specific key and its connection to the device in question a standard deliberately more demanding than the U.S. foregone conclusion inquiry rejected in Part V, precisely because this paper does not treat incremental evidentiary value as the relevant constitutional metric.

E. Anticipated Objections

Two objections merit direct engagement. First, investigative delay: requiring judicial authorization for biometric compulsion, and independent corroboration for hardware-key compulsion, will necessarily slow certain investigations, particularly in economic-offence cases where digital evidence is time-sensitive. This paper's response is that BNSS Section 96 already imposes an analogous judicial checkpoint for search warrants generally, without having been shown to cripple investigations under the erstwhile CrPC; extending a comparable, time-bound authorization procedure to biometric compulsion specifically is a marginal addition to an existing institutional practice rather than a novel bottleneck.

Second, risk of evidence destruction or loss: investigating agencies may argue that delay pending judicial authorization risks remote wiping or destruction of device contents. This concern is real but addressable through existing procedural tools including ex parte interim orders for physical seizure of the device (which this framework does not restrict) pending a separate judicial determination on compelled biometric unlocking, and forensic isolation techniques (e.g., Faraday enclosures) already used in Indian digital-forensics practice to prevent remote access during the interval between seizure and authorization.

F. Summary of the Proposal

Credential Type	Constitutional Treatment	Basis
Passcode / pattern	Per se testimonial; not compellable	Kathi Kalu Oghad–Selvi personal-knowledge test
Biometric (fingerprint/facial)	Compellable only with prior judicial authorization + proportionality showing	Puttaswamy proportionality standard; analogy to BNSS S.96
Hardware key / recovery phrase	Not compellable absent independent corroboration of existence and connection to device	Physical seizure alternative available; rejection of foregone-conclusion reasoning (Part V)

VIII. CONCLUSION AND RECOMMENDATIONS

A. Summary of Argument

This paper began from a narrow but consequential observation: the BSA-BNSS framework, effective from 1 July 2024, expanded the state's practical capacity to compel production of digital devices without addressing whether the specific act of unlocking such a device is itself testimonial compulsion under Article 20(3). Part II located the precise statutory seam where this question arises. Part III argued that this seam has gone unresolved because courts confronting it have not consistently applied the correct doctrinal test properly read, Kathi Kalu Oghad and Selvi together ask whether a compelled act requires the accused to draw on personal knowledge. Part IV's survey found that Indian courts confronting compelled disclosure since

2020 have not converged on an answer. Part V considered and rejected the importation of the American foregone conclusion doctrine. Part VI showed that PMLA/ED practice sits uneasily within the narrow carve-out Vijay Madanlal Choudhary created for non-accused witnesses. Part VII proposed a graded three-tier framework as a response to this doctrinal landscape, offered for further scrutiny rather than as a settled position.

B. Legislative Fix or Judicial Test Case

Two institutional paths could resolve the uncertainty this paper has documented, and this paper does not treat them as mutually exclusive. The first is legislative: Parliament could amend the BNSS, or issue rules under it, expressly addressing compelled digital disclosure for instance, by incorporating a version of the graded framework proposed in Part VII directly into Section 94, or by adopting a UK-style structural approach under which non-disclosure is treated as a separate offence rather than compelled testimony, as discussed in Part V. The second is judicial: the Special Leave Petition connected to Virendra Khanna, and the pending writ petition challenging Sections 50 and 63 of the PMLA, both currently before the Supreme Court, present opportunities for the Court to resolve the underlying Article 20(3) question directly, provided the specific digital-disclosure issue is squarely framed before it.

C. Recommendations

First, any future amendment or judicial clarification of BNSS Section 94 should expressly distinguish between compelling production of a device and compelling disclosure of the means to access it, rather than treating "production" as implicitly encompassing both.

Second, given the doctrinal clarity Selvi already provides on mental-privacy grounds, courts confronting compelled-disclosure disputes in the interim would be better served applying the personal-knowledge test articulated in Part III directly, rather than reasoning by analogy to Section 139 of the Indian Evidence Act, 1872, a provision Kathi Kalu Oghad itself cautioned against using for this purpose.

Third, given the frequency with which this question arises in PMLA/ED practice specifically, the Enforcement Directorate's internal guidelines on digital seizure would benefit from express reference to the accused/non-accused distinction Vijay Madanlal actually drew, to avoid the risk flagged in Part VI of that judgment's narrow holding being applied more broadly than its reasoning supports.

D. Closing Observation

The BSA and BNSS were enacted to modernize a criminal justice framework built for an earlier evidentiary era. Whether they succeed in that aim, with respect to digital evidence specifically, will depend less on the text of Sections 94, 96, and 63 themselves than on whether courts and legislators confront directly the question this paper has sought to frame precisely: not whether digital devices can be seized they plainly can but whether the accused's own mind can be compelled to open the door.