THE CONSTITUTIONAL AND PROCEDURAL INTERFACE: SECTION 91 CRPC/SECTION 94 BNSS AND ARTICLE 20(3) IN THE DIGITAL AGE

Aishwarya Vucha, ICFAI Law School Hyderabad

ABSTRACT

The criminal justice architecture of modern constitutional democracies is constructed upon a precarious equilibrium. On one side rests the sovereign's imperative to investigate crime, uncover truth, and maintain social order—a duty that demands expansive procedural powers to search, seize, and summon evidence. On the opposing side stands the individual's inviolable constitutional sanctuary: the right against self-incrimination, or the privilege to remain silent in the face of accusation. In India, this conflict has historically played out in the textual and doctrinal friction between the statutory power to compel production of documents under Section 91 of the Code of Criminal Procedure, 1973 (CrPC)—now Section 94 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)—and the fundamental right enshrined in Article 20(3) of the Constitution of India.

For the better part of the twentieth century, this conflict was managed through a judicially crafted compromise known as the doctrine of "implicit exclusion." However, the dawn of the digital age has fundamentally fractured this settlement. The transition from a paper-based evidentiary regime to one dominated by silicon and cloud storage has rendered the physical-mental distinction obsolete. This paper offers an exhaustive, publication-ready analysis of this jurisprudential crisis. It integrates critical judicial precedents, including the foundational *Romesh Chandra Mehta v. State of West Bengal* regarding the definition of an "accused," the rights-expanding *Nandini Satpathy v. P.L. Dani* concerning the right to silence during interrogation, and the technologically pivotal *Ritesh Sinha v. State of U.P.* concerning biometric compulsion.

By dissecting the "Physical-Mental Divide" established in *State of Bombay v. Kathi Kalu Oghad* and expanded in *Selvi v. State of Karnataka*, this paper evaluates the constitutional validity of compelled decryption (passwords/biometrics) in the digital age. It argues that while the BNSS explicitly expands the investigative net to include "electronic communication devices," the constitutional shield of "mental privacy" remains robust,

necessitating a new judicial test that distinguishes between the *seizure* of hardware and the *compulsion* of the mental keys required to unlock it.

1. Introduction: The Jurisprudential Fault Line of the Twenty-First Century

The adversarial criminal justice system is constructed on the premise that the accused is a subject of rights, not merely an object of investigation. This premise finds its most potent expression in the common law maxim *nemo tenetur seipsum accusare*—no man is bound to accuse himself. This principle, codified in Article 20(3) of the Constitution of India, serves as a bulwark against the "Cruel Trilemma" of self-incrimination, where an accused is forced to choose between confessing (and inviting conviction), lying (and facing perjury charges), or remaining silent (and facing contempt or statutory penalties).

For decades, the Indian judiciary managed the conflict between this right and the police's investigative powers through a carefully crafted compromise known as the doctrine of "implicit exclusion." Established by the Supreme Court in the landmark decision of *State of Gujarat v. Shyamlal Mohanlal Choksi* (1965) [1], this doctrine held that while the police could search a premise for incriminating documents (where the accused remains passive), they could not summon the accused to actively produce them, as this would constitute "testimonial compulsion." This distinction between *passive submission* to a search and *active participation* in production maintained the constitutional balance in a world of tangible evidence.

However, the dawn of the digital age has fundamentally fractured this settlement. The transition from physical ledgers, bloodstained weapons, and paper diaries to encrypted cloud storage and biometric locks has rendered the physical-mental distinction obsolete. In the physical world, a document exists as a tangible object independent of the accused's will; it can be seized via a search warrant without the accused's cooperation. In the digital realm, the "document" is often encrypted, intangible, and locked behind a password or biometric barrier that exists solely within the "mind" or "body" of the accused. To access this evidence, the state requires the accused to perform a volitional act: to speak the password or place the finger on the sensor.

This requirement of active participation has reignited the constitutional debate with unprecedented intensity. Does compelling an accused to unlock a smartphone constitute "being a witness" against oneself? Or is the password merely a "key" to a digital warehouse, compellable just like a physical key to a safe? This question has created a deep schism in the Indian judiciary, with the Karnataka High Court in *Virendra Khanna* (2021) [1] advocating a

pragmatic "Key Theory" favoring investigation, and the Delhi High Court in *CBI v. Mahesh Kumar Sharma* (2022) [1] and *Sanket Bhadresh Modi* (2023) [1] championing a "Mental Privacy" approach rooted in the right to silence.

The enactment of the Bharatiya Nagarik Suraksha Sanhita (BNSS), which replaced the CrPC on July 1, 2024, has further complicated the landscape. Section 94 of the BNSS explicitly expands the summoning power to include "electronic communication, including communication devices," signaling a legislative intent to empower the state to seize digital hardware.[1] Yet, the constitutional question remains: can a statute override the fundamental right against self-incrimination?

This paper argues that the resolution lies in a nuanced synthesis of historical doctrine and modern technological reality. It traces the evolution of the "accused" status from *Romesh Chandra Mehta*, analyzes the scope of interrogation under *Nandini Satpathy*, and examines the biometric frontier opened by *Ritesh Sinha*. Ultimately, it proposes that unless the Supreme Court provides a definitive ruling, the "sanctuary of silence" is at risk of being dismantled by the exigencies of digital investigation.

2. The Doctrinal Bedrock: Statutory Mandate vs. Constitutional Shield

To understand the current crisis, one must first excavate the doctrinal foundations laid in the pre-digital era. The tension is embedded in the very text of the law and the specific definitions of who constitutes an "accused."

2.1 The Statutory Power: Section 91 CrPC and Section 94 BNSS

Section 91(1) of the Code of Criminal Procedure, 1973 (CrPC) was the primary engine of documentary investigation. It provided:

"Whenever any Court or any officer in charge of a police station considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code... such Court may issue a summons... to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it..."

The operative words were "any document or other thing" and "necessary or desirable." The

provision was facially neutral; it did not explicitly exclude the accused. The legislative logic was utilitarian: the discovery of truth requires the production of all relevant evidence, regardless of who holds it. Failure to comply attracted penalties under Section 175 of the Indian Penal Code (IPC).

The Transition to BNSS (2023): Under the new regime, Section 94 of the BNSS retains the core structure of Section 91 but introduces critical textual changes to address the digital reality. Section 94(1) empowers the court/officer to summon "any document, electronic communication, including communication devices, or other thing".[1] This explicit inclusion of "communication devices" (smartphones, laptops, tablets) serves as a statutory acknowledgement that the hardware itself is now a primary source of evidence. However, Section 94 retains the generic reference to "the person," leaving the question open: does "person" include the "accused"?

2.2 The Constitutional Immunity: Article 20(3)

Article 20(3) of the Constitution of India provides the countervailing immunity:

"No person accused of any offence shall be compelled to be a witness against himself."

This clause is the constitutional embodiment of the common law principle *nemo tenetur seipsum accusare*. It has three components:

1. **Person Accused:** The protection applies only to an individual formally accused of an offense.

2. **Compulsion:** There must be duress or coercion.

3. **To be a Witness:** The compulsion must force the accused to provide evidentiary testimony against themselves.

The interface of Section 91/94 and Article 20(3) creates the central conflict. If an accused is summoned under Section 94 BNSS to produce a smartphone containing incriminating chats (electronic communication), and they are compelled to unlock it under threat of penalty, are they being "compelled to be a witness"?

2.3 The "Formal Accusation" Threshold: *Romesh Chandra Mehta v. State of West Bengal* (1969)

A pivotal question in the application of Article 20(3) is *when* a person becomes an "accused." Does the protection start the moment a person is detained, or only when a formal charge is laid? This distinction is critical in the digital age, where pre-FIR inquiries are common. This issue was definitively settled by the Constitution Bench in **Romesh Chandra Mehta v. State of West Bengal**.[6]

In *Romesh Chandra Mehta*, the Court examined whether statements made to Customs Officers under the Sea Customs Act (and later the Customs Act, 1962) were protected by Article 20(3) and Section 25 of the Evidence Act. The appellant argued that a person detained by Customs for smuggling was effectively an "accused" and thus could not be compelled to make statements.

The Ratio: The Supreme Court rejected this broad interpretation, establishing two critical principles:

1. **Formal Accusation is Essential:** The Court held that a person does not become an "accused" for the purposes of Article 20(3) merely by being detained or interrogated during a preliminary inquiry. The protection is triggered only when there is a "formal accusation" against the person—typically the lodging of a First Information Report (FIR) or a formal complaint before a Magistrate.[9] Until that point, a person is merely a suspect or a witness.

2. **Customs Officers are Not Police Officers:** The Court ruled that Customs Officers are not "police officers" within the meaning of Section 25 of the Evidence Act. Therefore, confessions made to them are admissible, provided the person was not formally accused at the time of the statement.[11]

Implication for Digital Evidence: The *Romesh Chandra Mehta* doctrine creates a "pre-accusation window." A suspect summoned for a preliminary inquiry (before an FIR is registered) may technically be compelled to produce a device or password under Section 94 BNSS because they do not yet enjoy the shield of Article 20(3). This creates a significant potential for state overreach in the digital era, where the most incriminating evidence (the

phone) is often seized at the very threshold of investigation, before formal accusations are crystallized.

2.4 The Historical Resolution: The "Implicit Exclusion" Doctrine

The Supreme Court resolved the conflict regarding the *accused* (post-FIR) through three seminal Constitution Bench judgments in the physical era.

2.4.1 *M.P. Sharma v. Satish Chandra* (1954)

In this eight-judge bench decision, the Court examined whether search and seizure violated Article 20(3). The Court defined "to be a witness" broadly as "furnishing evidence." It held that producing documents could constitute being a witness. However, it drew a vital distinction between a **Summons** and a **Search**:

- **Summons:** Requires the volition and active cooperation of the accused. If the document is incriminating, a summons effectively compels the accused to incriminate themselves.
- **Search:** Is a state-driven process where the accused remains passive. The evidence is seized *from* them, not produced *by* them. Thus, a search does not violate Article 20(3).[1]

2.4.2 *State of Bombay v. Kathi Kalu Oghad* (1961)

This eleven-judge bench refined the definition of "witness." The Court was asked if compelling an accused to give fingerprints, handwriting samples, or measurements violated Article 20(3). The Court established the **Physical-Mental Divide**:

- **Testimonial Compulsion (Protected):** Evidence based on "personal knowledge" or the mental faculties of the accused. This is protected because it forces the accused to convey information from their mind.
- **Physical Evidence (Unprotected):** Evidence derived from the body (fingerprints, measurements, DNA). The accused is not "testifying" but merely acting as a source of material evidence. The Court held that "to be a witness" means imparting knowledge about relevant facts.[1]

2.4.3 *State of Gujarat v. Shyamlal Mohanlal Choksi* (1965)

The definitive ruling on Section 91 CrPC came in *Shyamlal*.[1] A five-judge bench held that the term "person" in Section 91 does *not* include the accused person.

- **Ratio:** The Court reasoned that applying Section 91 to an accused would inherently violate Article 20(3) whenever the document sought was incriminating. To save the section from unconstitutionality, the Court "read down" the statute.

- **The Consensus:** The police cannot issue a summons to an accused to produce incriminating documents (like a diary or ledger). They must instead use a search warrant (Section 93 CrPC) to seize them.

3. The Scope of Protection: From Physical to Mental

While *Shyamlal* insulated the accused from producing physical documents, the scope of protection *during* interrogation—where the compulsion is psychological rather than statutory—remained a battleground. This was addressed in the landmark judgment of *Nandini Satpathy*, which significantly broadened the understanding of "compulsion."

3.1 *Nandini Satpathy v. P.L. Dani* (1978): The Right to Silence During Interrogation

In **Nandini Satpathy v. P.L. Dani** [14], the Supreme Court, led by Justice V.R. Krishna Iyer, confronted the tension between the obligation to answer police questions and the right against self-incrimination. The case involved a former Chief Minister accused of corruption who refused to answer a long questionnaire during police interrogation, citing Article 20(3).

The Legal Conflict:

- **Section 161(2) CrPC:** Mandates that a person "shall be bound to answer truly all questions relating to such case put to him by such officer," *other than* questions the answers to which would have a tendency to expose him to a criminal charge.[16]

- **Article 20(3):** Protects the accused from being a witness against themselves.

The Ruling: The Supreme Court delivered a rights-expansive judgment that harmonized these provisions:

1. **Interrogation as a Protected Zone:** The Court rejected the notion that Article 20(3) applies only in the courtroom. It held that the "accused" is entitled to the right to silence even during the stage of police interrogation. The phrase "compelled to be a witness" encompasses the investigative stage.[17]

2. **The "Link in the Chain" Doctrine:** The Court ruled that the protection is not limited to confessions that directly admit guilt. It extends to any answer that might form a "link in the chain" of evidence necessary to secure a conviction. If an answer would have a "reasonable tendency" to expose the accused to a criminal charge, they have the right to remain silent.[14]

3. **Compulsion Defined Broadly:** Crucially, the Court recognized that "compulsion" isn't limited to physical torture (third-degree methods). It includes "psychological pressure," "atmospheric pressure," and environmental coercion inherent in police custody. The Court famously noted that "compelled testimony" includes evidence extracted through "psychological torture, atmospheric pressure, environmental coercion, tiring interrogative prolixity, overbearing and intimidatory methods".[17]

Relevance to Digital Evidence: *Nandini Satpathy* is the doctrinal anchor for refusing to divulge passwords. A password is purely mental knowledge. Compelling an accused to reveal it is analogous to compelling them to answer a question during interrogation. If the password unlocks incriminating data (chats, photos, logs), revealing it creates a "link in the chain" of prosecution. Under *Nandini Satpathy*, the accused has a constitutional right to refuse to provide this information if it would tend to incriminate them. The "bound to answer truly" clause of Section 161(2) (now Section 179 BNSS) explicitly contains an exception for incriminating questions, which covers passwords to incriminating devices.

3.2 *Selvi v. State of Karnataka* (2010): The Expansion of Article 20(3)

The jurisprudential landscape shifted seismically with *Selvi v. State of Karnataka* (2010).[1] The Supreme Court examined the constitutionality of narco-analysis, brain-mapping, and polygraph tests.

- **Holding:** The Court ruled that compelling an accused to undergo these tests violates Article 20(3).

- **Reasoning:** The Court held that Article 20(3) protects **"Mental Privacy."** It creates a "zone of privacy" around the accused's mind. Techniques that forcibly extract information from the mind—whether through drugs (narco) or physiological responses (polygraph)—are "testimonial compulsion."

- **Crucial Dictum:** The Court noted that even if the information extracted is used only for investigation (and not as evidence in court), the act of extraction itself violates the Constitution if it is involuntary. This directly impacts passwords, which are pieces of information stored in the mind.

4. The Digital Disruption: Mental Privacy and the Encrypted Mind

The "Shyamlal Consensus" functioned effectively when evidence was physical. A diary in a safe could be seized by breaking the safe; the accused's mind was not required. In the digital age, the safe is encrypted, and the key exists only in the accused's memory (password) or biological feature (biometric). The police can seize the phone (the safe) under Section 93/105 BNSS, but without the password, the seizure is futile.

This necessitates compelling the accused to act: to speak the password or scan the finger. This act forces a collision between the *Kathi Kalu Oghad* (physical evidence is compellable) and the modern jurisprudence of "mental privacy."

4.1 Biometrics and the Voice: The *Ritesh Sinha* Paradigm

The distinction between physical and mental evidence—and the limits of judicial power to compel evidence in the absence of legislation—was tested in **Ritesh Sinha v. State of Uttar Pradesh** (2019).[20]

The Facts: The appellant was accused of fraud involving the collection of money for police jobs. The investigation relied on a recorded phone conversation between the accused and an associate. To prove the voice on the recording was the accused's, the police sought a "voice sample." The accused refused, citing Article 20(3) and the lack of any provision in the CrPC authorizing a Magistrate to order a voice sample.

The Issues:

1. Does compelling a voice sample violate Article 20(3)?

2. Can a Magistrate order a voice sample in the absence of explicit statutory authority?

The Ruling: A three-judge bench of the Supreme Court held:

1. **Voice as Physical Evidence:** Reaffirming *Kathi Kalu Oghad*, the Court held that a voice sample is immutable physical evidence, akin to fingerprints or DNA. Providing a sample for identification purposes does not involve imparting "personal knowledge" regarding the facts of the crime. Therefore, it is **not testimonial compulsion** and does not violate Article 20(3).[20]

2. **Gap in the Law & Article 142:** The Court acknowledged a legislative gap: the CrPC (prior to the 2022 amendment) did not explicitly empower Magistrates to order voice samples. However, invoking its plenary powers under **Article 142** of the Constitution (to do "complete justice"), the Court judicially empowered Judicial Magistrates to order voice samples until Parliament enacted specific legislation.[22]

"This legislative lacuna has now been explicitly closed by Section 349 of the BNSS (formerly Section 311A CrPC). The new provision not only codifies the admissibility of 'voice samples' and 'finger impressions' but also aggressively expands the state's power by allowing Magistrates to order such samples even *without* an arrest. However, this statutory expansion creates a powerful argument by exclusion: while Parliament explicitly amended the law to compel physical attributes (voice/fingerprints), it remained silent on 'passwords' or 'decryption keys.' This legislative choice reinforces the constitutional distinction asserted in *Selvi*—that while the state may statutorily compel the body, it has not been authorized to compel the mind."

Impact on Digital Evidence: *Ritesh Sinha* complicates the digital debate. By classifying voice (a biometric) as physical and compellable, it opens the door for the state to argue that **biometric unlocking** (FaceID, Fingerprint) of smartphones is similarly compellable. Unlike a password (which is mental/testimonial), a fingerprint is physical/non-testimonial. This creates a dichotomy where a phone locked with a *passcode* might be protected under *Selvi*, but the same phone locked with a *fingerprint* might be compellable under *Ritesh Sinha*.

5. The Judicial Schism: The High Court Conflict on Digital Decryption

The tension between *Kathi Kalu Oghad/Ritesh Sinha* (physical/biometric is compellable) and *Selvi/Nandini Satpathy* (mental/silence is protected) has produced a sharp divergence in High

Court rulings regarding compelled decryption.

5.1 The Pragmatic/Key Theory: *Virendra Khanna v. State of Karnataka* (2021)

In *Virendra Khanna*, the Karnataka High Court addressed a situation where the police sought directions to compel an accused to unlock his smartphone and email accounts.[1]

- **The Ruling:** The Court held that the police can compel the accused to provide passwords and biometrics.

- **The "Key" Analogy:** The Court equated a password to a physical key. It reasoned that the password itself is not the incriminating evidence; the *contents* of the phone are. Providing the password is akin to handing over the key to a locked room during a search, which is a duty under Section 100 CrPC.

- **Biometrics as Physical Evidence:** Relying on *Kathi Kalu Oghad*, the Court categorized fingerprints and FaceID as physical evidence. Since the accused can be compelled to give a fingerprint for identification, the Court reasoned they can be compelled to give it to unlock a phone.

- **Adverse Inference:** The Court held that if the accused refuses to unlock the device, the court can draw an adverse inference against them at trial, penalizing their silence.

5.2 The Mental Privacy Theory: *CBI v. Mahesh Kumar Sharma* (2022) & *Sanket Bhadresh Modi* (2023)

The Delhi High Court and its subordinate courts have taken a diametrically opposite stance, prioritizing the "Rights-Centric" view.

5.2.1 *CBI v. Mahesh Kumar Sharma* (2022)

The Special CBI Court in Delhi explicitly disagreed with *Virendra Khanna*, declaring it *per incuriam* (bad law) for ignoring the *Selvi* judgment.[1]

- **Password as Testimonial:** The Court held that a password is "personal knowledge" residing in the mental faculties of the accused. Compelling its disclosure forces the accused to use their memory and convey information, which is pure testimonial

compulsion protected by Article 20(3).

- **Distinction from Biometrics:** The Court introduced a nuance. While *Kathi Kalu Oghad* permits taking fingerprints for *comparison* (identification), taking a fingerprint to *unlock a device* leads to the discovery of substantive evidence. Thus, the context changes the nature of the act from physical to testimonial.

5.2.2 *Sanket Bhadresh Modi v. CBI* (2023)

In this case, the Delhi High Court granted bail to an accused despite the CBI's argument that he was "non-cooperative" for refusing to share passwords.[1]

- **The Ruling:** The Court affirmed the Right to Silence. It stated that an accused "cannot be expected to sing in a tune which is music to the ears of the investigating agency." The refusal to provide passwords is a legitimate exercise of constitutional rights and cannot be a ground to deny bail. This judgment firmly places digital credentials within the protective ambit of Article 20(3).

5.3 Reaffirming *Shyamlal* in the BNSS Era: *Ram Kishan Mittal v. State of West Bengal* (2025)

The conflict persists into the era of the new criminal laws. In **Ram Kishan Mittal v. State of West Bengal** (2025) [1], the Calcutta High Court quashed proceedings where a lower court had ordered an accused to produce incriminating rent receipts under Section 91 CrPC.

- **Significance:** The Court reaffirmed the *Shyamlal* doctrine: Section 91 (and by extension Section 94 BNSS) cannot be used to compel an accused to produce incriminating material. This judgment serves as a vital contemporary precedent, confirming that the legislative changes in the BNSS have not diluted the constitutional protection.

5.4 Procedural Misuse: The "Debit Freeze" Phenomenon

The conflict also extends to the misuse of Section 91/94 for asset freezing. In **Aeronfly International v. State of Himachal Pradesh** (2024) [1], the Himachal Pradesh High Court struck down a police order that "debit froze" a company's bank accounts using Section 91.

- **The Ruling:** The Court held that Section 91 empowers the police to summon documents

(like account statements) but does not authorize them to issue prohibitory orders freezing assets. Freezing requires the strict procedure of Section 102 CrPC (Section 106 BNSS), which mandates reporting the seizure to a Magistrate. This judgment highlights how Section 91 is often weaponized as a tool of economic coercion rather than evidence gathering.

6. The Legislative Landscape: The Bharatiya Nagarik Suraksha Sanhita (2023)

The enactment of the BNSS has brought textual changes that directly impact this debate.

6.1 Section 94 BNSS: Expanding the Net

Section 94 of the BNSS replaces Section 91 CrPC. While the core structure remains, the scope is expanded. It empowers the court/police to summon: *"any document, electronic communication, including communication devices, or other thing..."*.[1]

Implications:

- **Explicit Inclusion:** The specific mention of "communication devices" attempts to settle the debate on whether a phone is a "document" or "thing." It is now a distinct statutory category.

- **The Prosecutors' View:** The state will argue that Parliament has explicitly authorized the summoning of devices, overriding the hesitation in older judgments.

- **The Constitutional Reality:** However, statutory expansion cannot negate a Fundamental Right. The limitation in *Shyamlal* was based on Article 20(3), not the text of the CrPC. Therefore, even if Section 94 allows summoning a device, Article 20(3) prevents using that power against an accused if it leads to self-incrimination. The section must be "read down" just as Section 91 was: valid for third parties, invalid for the accused regarding incriminating evidence.

6.2 Section 105 BNSS: The Videography Safeguard

Section 105 BNSS introduces a mandatory procedural safeguard: the entire process of search and seizure must be recorded through audio-video means (preferably mobile phone) and forwarded to the Magistrate without delay.[1]

- **Impact:** This provision is designed to prevent the "planting" of evidence and ensure transparency. It creates a new category of digital evidence—the search video itself.

- **The Defense Shield:** This provision will likely lead to increased litigation where the accused invokes Section 94 to summon the search video to prove procedural lapses. If the police fail to videograph the seizure of a phone, the integrity of the digital evidence extracted from it becomes suspect.

6.3 Intermediary Liability: *PhonePe Pvt Ltd v. State of Karnataka* (2025)

The interaction between Section 91/94 and digital intermediaries was clarified in **PhonePe Pvt Ltd v. State of Karnataka** (2025).[1] The Karnataka High Court dismissed PhonePe's petition challenging a Section 91 notice for user data. The Court held that intermediaries cannot claim "privacy" on behalf of users to block lawful investigations. While user privacy is important, it must yield to the statutory power of investigation when directed at a third party (the intermediary), not the accused themselves. This reinforces that *Shyamlal* protects the *accused*, not the *intermediary* holding the accused's data.

7. Comparative Constitutional Law: Global Perspectives

The Indian dilemma is not unique. Jurisdictions worldwide are grappling with the "Going Dark" problem—law enforcement's inability to access encrypted evidence.

7.1 United States: The "Foregone Conclusion" Doctrine

The Fifth Amendment to the US Constitution is textually similar to Article 20(3). The US Supreme Court in *Fisher v. United States* (1976) and *United States v. Hubbell* (2000) established the "Foregone Conclusion" doctrine.

- **The Doctrine:** The state can compel the production of documents/passwords if it can show that it already knows with "reasonable particularity" that the evidence exists, is in the accused's possession, and is authentic. In such cases, the act of production is not "testimonial" because it reveals nothing new to the government.[1]

- **Application to Passwords:** US Courts are split.

    - *11th Circuit (In re Grand Jury Subpoena):* Held that compelling decryption is

unconstitutional if the government does not know exactly what is on the drive. It is a "fishing expedition."

- *Other Courts (e.g., Massachusetts in Commonwealth v. Gelfgatt):* Have applied the doctrine to passwords, arguing that if the police can link the phone to the accused, the password is a non-testimonial key.

- **Biometrics:** A significant divergence exists where US courts often consider biometrics (fingerprints/FaceID) as non-testimonial physical evidence (similar to *Kathi Kalu Oghad*), whereas passwords are protected testimonial thoughts. This contrasts with the Indian "Mental Privacy" view in *Selvi* which offers broader protection.[1]

7.2 United Kingdom: The Statutory Override (RIPA 2000)

The UK has prioritized investigation over silence through legislation. Part III of the Regulation of Investigatory Powers Act 2000 (RIPA) (Section 49) empowers authorities to serve a notice demanding encryption keys.

- **Criminalizing Silence:** Failure to comply with a Section 49 notice is a distinct criminal offense punishable by up to two years (or five years for national security cases) in prison.[1]

- **Judicial View:** In *R v. S and A* (2008), the Court of Appeal held that this regime is compatible with the privilege against self-incrimination because the "key" exists independently of the accused's mind (as a fact), and the statute provides safeguards (the key itself cannot be used as evidence, only the decrypted data).[1] This represents a legislative "override" of the right to silence that is absent in Indian law.

7.3 Canada: The Charter Protection

Section 7 of the Canadian Charter of Rights and Freedoms protects the right to silence.

- **R. v. Shergill (2019):** The Ontario Court of Justice refused to issue an "assistance order" compelling an accused to unlock his phone. The court held that forcing the accused to provide the password would compel him to create evidence against himself (the knowledge of the password) that exists only in his mind. The court distinguished this

from existing physical evidence like DNA.[1]

7.4 European Court of Human Rights (ECHR)

The ECHR views the right to silence as implicit in Article 6 (Right to a Fair Trial).

- **Funke v. France:** The Court held that attempting to compel the production of incriminating bank statements violated the right to silence.

- **Podchasov v. Russia (2024):** The ECtHR ruled that statutory requirements for messaging apps (like Telegram) to build "backdoors" or provide decryption keys to security services violate Article 8 (Right to Private Life). The Court held that general weakening of encryption is disproportionate and endangers all users.[1] This jurisprudence aligns with the "Mental Privacy" approach of the Delhi High Court.

8. Synthesis and Conclusion: Toward a New Constitutional Test

The current legal landscape in India is fragmented. The "Shyamlal Consensus" is broken, and the High Courts are divided. The "Pragmatic" approach of *Virendra Khanna* risks eroding the constitutional core of Article 20(3) by treating the mind as a repository of keys. The "Rights-Centric" approach of *Mahesh Kumar Sharma* and *Sanket Bhadresh Modi* upholds the dignity of the individual but arguably hampers investigation in an era of ubiquitous encryption.

8.1 Proposed Doctrinal Test

To resolve this, the Supreme Court must formulate a test that synthesizes *Kathi Kalu Oghad*, *Selvi*, *Nandini Satpathy*, and the reality of the BNSS.

1. **The "Mind vs. Body" Threshold:** Is the authentication method mental (password) or physical (biometric)?

    - **Biometric:** Falls under *Kathi Kalu Oghad* and *Ritesh Sinha*. It is physical evidence. The accused can be compelled to provide a fingerprint unless the act of unlocking itself is an admission of guilt (e.g., admitting ownership of a device found in a public place).

    - **Password:** Falls under *Selvi* and *Nandini Satpathy*. It is mental content. It is *prima*

facie protected.

2. **The "Independent Existence" Factor:** Does the intelligible evidence exist independently?

   - Encrypted data is unintelligible. The "evidence" (readable files) does not exist without the password. Therefore, the password *creates* the evidence. Compelling it is creating evidence against oneself.

3. **The "Reading Down" of Section 94 BNSS:** The statute must be interpreted to allow the seizure of the device (hardware) but not the compelled disclosure of the password (mental software). The state must invest in technological capabilities (forensics) to break encryption, rather than relying on legal coercion to break the accused's silence.

8.2 Conclusion

The conflict between Section 91 CrPC (Section 94 BNSS) and Article 20(3) is not merely a procedural technicality; it is a fundamental contest over the boundaries of state power in the digital age. While the BNSS expands the state's reach into "electronic communication," the Constitution remains the supreme law. The "sanctuary of silence" guaranteed by Article 20(3), expanded by *Selvi* to include "mental privacy," and reinforced by *Nandini Satpathy* regarding interrogation, must protect the digital extensions of the human mind. Unless the Supreme Court adopts a modified "Foregone Conclusion" doctrine or overrules *Selvi*, the constitutional bar against compelling an accused to provide a password must stand. In the digital age, the right to silence effectively includes the right to encryption.

Table of Cases

Case Name	Citation	Court	Key Holding
M.P. Sharma v. Satish Chandra	AIR 1954 SC 300	Supreme Court	"To be a witness" includes document production; Search is not compulsion.
State of Bombay v. Kathi Kalu Oghad	AIR 1961 SC 1808	Supreme Court	Physical evidence (fingerprints) is compellable; Personal knowledge is protected.
State of Gujarat v. Shyamlal Mohanlal Choksi	AIR 1965 SC 1251	Supreme Court	Section 91 CrPC does not apply to the accused regarding incriminating documents.

Romesh Chandra Mehta v. State of West Bengal	(1969) 2 SCR 461; AIR 1970 SC 940	Supreme Court	"Accused" under Art 20(3) requires formal accusation (FIR/Complaint). Customs officers are not police officers.
Nandini Satpathy v. P.L. Dani	AIR 1978 SC 1025; (1978) 2 SCC 424	Supreme Court	Right to silence applies during interrogation. S. 161(2) CrPC does not compel incriminating answers.
Selvi v. State of Karnataka	(2010) 7 SCC 263	Supreme Court	Mental privacy protected; involuntary neuro-scientific tests violate Art 20(3).
Ritesh Sinha v. State of Uttar Pradesh	(2019) 8 SCC 1; AIR 2019 SC 3592	Supreme Court	Voice samples are physical evidence (not testimonial). Article 142 used to empower Magistrates to order samples.
Virendra Khanna v. State of Karnataka	2021 SCC OnLine Kar 5032	Karnataka HC	Passwords are "keys," not testimony. Accused can be compelled to unlock devices.
CBI v. Mahesh Kumar Sharma	2022 SCC OnLine Dis Crt (Del) 48	Delhi Dist. Court	*Virendra Khanna* is *per incuriam*. Passwords are mental knowledge and protected.
Sanket Bhadresh Modi v. CBI	2023 SCC OnLine Del 7837	Delhi HC	Right to silence includes refusal to share passwords; bail cannot be denied for this.
Ram Kishan Mittal v. State of West Bengal	2025 SCC OnLine Cal 6945	Calcutta HC	Reaffirmed *Shyamlal* in the context of BNSS; accused cannot be summoned for incriminating docs.
PhonePe Pvt Ltd v. State of Karnataka	2025 SCC OnLine Kar (WP 11567/2025)	Karnataka HC	Intermediaries cannot claim absolute immunity; must comply with Section 91 if specific.
Aeronfly International v. State of HP	2024 SCC OnLine HP 4099	Himachal HC	Section 91 cannot be used to "debit freeze" bank accounts; must use Section 102/106.

Works cited

1. State Of Gujarat v. Shyamlal Mohanlal | Gujarat High Court | Judgment | Law - CaseMine, accessed on January 27, 2026, https://www.casemine.com/judgement/in/560910d2e4b0149711182986

2. MR.VIRENDRA KHANNA v. THE STATE OF KARNATAKA - CaseMine, accessed on January 27, 2026, https://www.casemine.com/judgement/in/61e613409fca19546ac36187

3. Right of Self-Incrimination in Digital Age: Whether Compelled Disclosure of Password/Biometrics is Unconstitutional? - SCC Online, accessed on January 27, 2026, https://www.scconline.com/blog/post/2023/03/18/right-of-self-incrimination-in-digital-age-whether-compelled-disclosure-of-password-biometrics-is-unconstitutional/

4. Sanket Bhadresh Modi vs Central Bureau Of Investigation & Anr on 18 December, 2023, accessed on January 27, 2026, https://indiankanoon.org/doc/47054136/

5. REPORTABLE IN THE SUPREME COURT OF INDIA CRIMINAL APPELLATE JURISDICTION CRIMINAL APPEAL NO.152 OF 2013 TOFAN SINGH …Appellant, accessed on January 27, 2026, https://api.sci.gov.in/supremecourt/2012/26682/26682_2012_33_1501_24551_Judgement_29-Oct-2020.pdf

6. Romesh Chandra Mehta vs State Of West Bengal on 18 October, 1968 - Indian Kanoon, accessed on January 27, 2026, https://indiankanoon.org/doc/690751/

7. Customs Officers Not Police Officers: Admissibility of Statements Under the Customs Act - Ramesh Chandra Mehta v. State of West Bengal: Supreme Court Of India | CaseMine, accessed on January 27, 2026, https://www.casemine.com/commentary/in/customs-officers-not-police-officers:-admissibility-of-statements-under-the-customs-act---ramesh-chandra-mehta-v.-state-of-west-bengal/view

8. DISCRETION WITH REGARD TO DIFFERENT AGENCY AT PRE-TRIAL STAGE - Jetir.Org, accessed on January 27, 2026,

https://www.jetir.org/papers/JETIR2112016.pdf

9. Virbhadra Singh & Anr vs Enforcement Directorate & Anr on 3 July, 2017 - Indian Kanoon, accessed on January 27, 2026, https://indiankanoon.org/doc/43073718/

10. Safeguards under CrPC Applicable to Warrantless Arrests under Fiscal Laws, accessed on January 27, 2026, https://www.scobserver.in/supreme-court-observer-law-reports-scolr/safeguards-under-crpc-applicable-to-warrantless-arrests-under-fiscal-laws/

11. REPORTABLE IN THE SUPREME COURT OF INDIA CRIMINAL ORIGINAL JURISDICTION WRIT PETITION (CRIMINAL) NO.336 OF 2018 RADHIKA AGARWAL, accessed on January 27, 2026, https://api.sci.gov.in/supremecourt/2018/46616/46616_2018_1_1501_59928_Judgement_27-Feb-2025.pdf

12. State Of Gujarat vs Shyamlal Mohanlal Choksi And Manubhai ... on 14 December, 1964, accessed on January 27, 2026, https://app.draftbotpro.com/doc/32758508

13. Nandini Satpathy v. P.L. Dani AIR 1978 SC 1025 - Aashayein Judiciary, accessed on January 27, 2026, https://www.alec.co.in/judgement-page/nandini-satpathy-v-pl-dani-air-1978-sc-1025

14. SILENCE AS A SHIED AND INTERROGATIVE RESTRAINTS: UNDERSTANDING THE LEGAL IMPLICATIONS SET OUT IN NANDINI SATPATHY V. P L DANI De - JLRJS, accessed on January 27, 2026, https://jlrjs.com/wp-content/uploads/2024/08/91.-Deepika-Mohnani.pdf

15. Nandini Satpathy vs Dani (P.L.) And Anr on 7 April, 1978 - Indian Kanoon, accessed on January 27, 2026, https://indiankanoon.org/doc/1938988/

16. Comprehensive Commentary on Nandini Satpathy v. P.L Dani And Another: Reinforcing the Right Against Self-Incrimination in India - CaseMine, accessed on January 27, 2026, https://www.casemine.com/commentary/in/comprehensive-commentary-on-nandini-satpathy-v.-p.l-dani-and-another:-reinforcing-the-right-against-self-incrimination-in-india/view

17. Selvi & Ors vs State Of Karnataka & Anr on 5 May, 2010 - Indian Kanoon, accessed on January 27, 2026, https://indiankanoon.org/doc/338008/

18. Selvi vs. State of Karnataka - Privacy Law Library, accessed on January 27, 2026, https://privacylibrary.ccgnlud.org/case/selvi-vs-state-of-karnataka

19. Ritesh Sinha v. State Of UP, 2019 | Naya Legal, accessed on January 27, 2026, https://www.nayalegal.com/ritesh-sinha-v-state-of-up-2019

20. Ritesh Sinha v. State of Uttar Pradesh (2019) - Drishti Judiciary, accessed on January 27, 2026, https://www.drishtijudiciary.com/constitution-of-india/ritesh-sinha-v-state-of-uttar-pradesh-2019

21. Ritesh Sinha v. State Of U.P. | Allahabad High Court | Judgment | Law - CaseMine, accessed on January 27, 2026, https://www.casemine.com/judgement/in/5608edb2e4b014971111f82f

22. Ritesh Sinha vs State Of Uttar Pradesh on 2 August, 2019 - Indian Kanoon, accessed on January 27, 2026, https://indiankanoon.org/doc/18061439/

23. Mr. Virendra Khanna vs State Of Karnataka By: on 12 March, 2021 - Indian Kanoon, accessed on January 27, 2026, https://indiankanoon.org/doc/87379349/

24. CBI vs. Mahesh Kumar Sharma &Ors, accessed on January 27, 2026, https://images.assettype.com/barandbench/2022-11/3273686f-00bf-4311-8619-79a98e5831ca/CBI_v__Mahesh_Kumar_Sharma___Anr.pdf

25. Accused cannot be coerced to reveal/disclose password in regard to digital evidence while trial is ongoing: Delhi High Court - SCC Online, accessed on January 27, 2026, https://www.scconline.com/blog/post/2024/01/06/accused-cannot-be-coerced-to-reveal-password-in-regard-to-digital-evidence-while-trial-is-ongoing-dhc-legal-news/

26. Can Section 91 CrPC be invoked to compel an accused to produce incriminating material? Calcutta High Court examines - SCC Online, accessed on January 27, 2026, https://www.scconline.com/blog/post/2025/09/03/calcutta-hc-section-91-crpc-accused-incriminating-material-legal-news/

27. RAM KISHAN MITTAL vs THE STATE OF WEST BENGAL AND ORS - 2025 Supreme(Online)(Cal) 5900, accessed on January 27, 2026, https://supremetoday.ai/doc/judgement/INDCAL00000022188

28. Yamini Bhandari vs The State Of West Bengal & Ors on 11 July, 2025 - Indian Kanoon, accessed on January 27, 2026, https://indiankanoon.org/doc/80954164/

29. IN THE HIGH COURT OF HIMACHAL PRADESH, SHIMLA - LawBeat, accessed on January 27, 2026, https://lawbeat.in/sites/default/files/2024-09/Aeronfly%20International%20Private%20Limited%20vs%20State%20of%20HP%20&%20Ors.pdf

30. Bytes and Rights - Ebook | PDF | Justice | Crime & Violence - Scribd, accessed on January 27, 2026, https://www.scribd.com/document/923116163/Bytes-and-Rights-eBook

31. Confidentiality vs. Accountability: The Karnataka HC decision in the PhonePe Case, accessed on January 27, 2026, https://ssrana.in/articles/confidentiality-vs-accountability-the-karnataka-hc-decision-in-the-phonepe-case/