NFSU JOURNAL OF FORENSIC JUSTICE

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

# PASSWORDS, PRIVACY, AND SELF-INCRIMINATION: COMPELLED DECRYPTION UNDER ARTICLE 20(3) OF THE CONSTITUTION

**Samarth Udasin**

***Abstract:*** *The proliferation of encrypted digital devices in modern life has introduced complex legal challenges at the intersection of criminal investigation and constitutional rights in India. This paper critically examines whether compelling an accused to unlock or decrypt such devices—whether through alphanumeric passwords or biometric identifiers—violates the right against self-incrimination under Article 20(3) of the Indian Constitution. Drawing from key Supreme Court rulings such as Kathi Kalu Oghad, Selvi, and Puttaswamy, the paper analyzes the evolving jurisprudence distinguishing between "testimonial" and "physical" evidence. It interrogates whether unlocking a device constitutes a testimonial act by revealing mental contents or conveying control over incriminating data. The analysis further explores forensic realities, the implications of biometric authentication, and the divergent approaches taken by Indian High Courts. Comparative insights from the United States, including the "foregone conclusion" doctrine, offer additional perspective on reconciling investigative needs with individual rights. The paper concludes that compelling decryption, especially via passwords, is presumptively testimonial and constitutionally protected, while biometric access remains legally unsettled. It advocates for a robust statutory framework requiring judicial oversight, proportionality, and safeguards for digital privacy, emphasizing the urgent need for the Supreme Court to clarify this critical area of digital constitutional law.*

***Keywords:*** *Compelled decryption, Article 20(3), self-incrimination, digital privacy, biometric unlocking, password, testimonial compulsion, Indian Constitution, digital forensics, foregone conclusion doctrine.*

## I. INTRODUCTION

The advent of technology in this age has profoundly reshaped the landscape of criminal procedure and investigation in India. As every individual owns and uses encrypted digital devices such as smartphones, tablets, and computers etc. Further, this has resulted in these devices becoming involuntary repositories of a large amount of personal and potentially incriminating data. This rapid development of technology which resulted in proliferating of the digital evidences has presented a major tension between the state's legitimate interest in the crime detection and justice delivery and the fundamental rights of the individual particularly right to privacy under Article 21 and the protection against self-incrimination under Article 20(3) of the Constitution of India. Transversing through this evolving terrain demands a delicate balance to make sure that the pursuit of achieving faster, efficient and effective justice delivery does not unintentionally diminish the civil liberties. With the arrival of new criminal laws, particularly Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 and the Bharatiya Sakshya Adhiniyam (BSA), 2023 , further requires a comprehensive analysis of these foundational principles to apply them in the modern investigation environment, especially relating to seizure and access to the electronic records stored in the encrypted electronic devices.

The centre of this conflict lies at the practice of compelled decryption. This consists of the state compelling an accused person to decrypt their encrypted digital device, while this act of decrypting or unlocking can be achieved by various means. Conventionally, it involves furnishing an alphanumeric password, a sequence of characters only known to the user, which can only be recalled through his mental efforts. In the recent time with the advancements in the technology, unlocking now often requires biometric identifiers like fingerprints, facial scans, or iris scans. Irrespective of the method, compelling a person to perform this act is an "act of production". Further, this act expedites access to the device's contents which can stretch from communications and documents to location data and other digital artifacts, likely to be served as evidence. Moreover, there is an important difference that lies in whether the act of providing a password (which requires a mental recall) is fundamentally different from decrypting/unlocking (which is generally

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

treated a physical characteristic) in context of constitutional protection.

The main question that this paper aims to confront is whether compelling an accused person to unlock their digital encrypted devices (through passwords or biometrics) is violative of their fundamental right against self-incrimination given in Article 20(3) of the Constitution of India. This includes examining whether the act of unlocking or providing any means to unlock equals to being "compelled to be a witness against himself". Further, this analysis requires to deep dive into the nature of the act, of it being "testimonial" or just production of physical evidence. Moreover, this issue also elaborates by the capacity of the device to be storehouse of the person's identity and private life. Also, connected to the wider use of forensic science methods in criminal investigations. The compelling decryption is generally a prerequisite act which enables the subsequent application of forensic analysis to the device's contents. This is still a budding area of law in India which is demanding careful attention of established foundational principles in view of the modern technological advancements.

## II. ARTICLE 20(3) & THE PRIVILEGE AGAINST SELF-INCRIMINATION

The protection against self-incrimination is an essential part of the criminal justice system which is deeply rooted in the constitutional fabric of India. Understanding its structure becomes extremely important when examining the legality of the compelled decryption of the digital devices.

### A. Text, History & Constitutional Theory

The privilege against self-incrimination finds its place through Article 20(3) of the Constitution of India, which absolutely states: "No person accused of any offence shall be compelled to be a witness against himself." This fundamental right is considered as one of the indispensable rights within Parth III of the Constitution.

This doctrine finds its roots internationally by taking inspiration from the common law principles particularly those developed in England. While the history reveals a reaction against coercive methods used by the courts like Star Chambers in which individuals were compelled to incriminate themselves. On the other hand, the latin maxim "nemo tenetur seipsum accusare" meaning "a man cannot represent himself as guilty" or "no man is bound to accuse himself" embodies this fundamental principle. This protection was created to bar investigators and courts from using any kind of compulsion in place of diligent investigation to uncover evidence. The sources also mention the influence of the Fifth Amendment to the Constitution of the United States which also mentions a similar guarantee.

In the United States, the scope of the Fifth Amendment privilege concerning the production of the evidence has been subject to considerable judicial interpretation which resulted in doctrines like Act of Production Doctrine (established in Fisher v. United States ). This doctrine proposes that while the contents of a document might not be a testimonial but the act of producing the document itself can have testimonial implication such as admitting the existence, possession, or authenticity of the document. However, this has been often countered by arguably broader and older framework which extend protection to the compelled production of any incriminating evidence but not solely testimonial acts. From the perspective this paper, the application of these doctrines particularly Foregone Conclusion Doctrine, which provides that the Fifth Amendment does not protect against compelled production of evidence if the existence, possession, and authenticity of the evidence are already known to the government, rendering the act of production a "foregone conclusion" becomes important for the Indian debate on compelled decryption as it suggest similarities between the two legal systems on the right against self-incrimination.

### B. Testimonial vs. Physical Evidence

An essential difference in the Indian jurisprudence regarding Article 20(3) is between "testimonial" and "physical" evidence. The Supreme Court, in State of Bombay v. Kathi Kalu Oghad , was crucial in defining "to be a witness" under Article 20(3). The Court held that "to be a witness" is more than giving oral evidence and it means "to furnish evidence". This can be done through various modes, including producing documents or even making "intelligible gestures". However, the protection is specifically against "testimonial compulsion". The majority in Kathi Kalu Oghad drew a distinction, stating that compelling an accused to give finger impressions, palm impressions, foot impressions, or specimen handwriting or signatures, or requiring identification, does not amount to compelling him "to be a witness against himself" within the meaning of Article 20(3). This is because these acts are considered the provision of physical evidence or material evidence, not statements conveying the personal

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

knowledge of the accused. Such physical evidence "by itself" does not have a tendency to incriminate and is often used for comparison to corroborate other evidence.

This distinction was further explored and refined in Selvi v. State of Karnataka , a landmark judgment concerning the involuntary administration of techniques like polygraph, narcoanalysis, and BEAP tests. The Court in Selvi clarified that Article 20(3) protects against the forcible "conveyance of personal knowledge that is relevant to the facts in issue". It held that the results obtained from these impugned tests bore a "testimonial" character, unlike mere physical evidence, because they aimed to extract information based on the subject's personal knowledge, making them inadmissible if obtained under compulsion. The Court reiterated that the privilege applies to statements, oral or written, that convey a person's knowledge of relevant facts, which can be distinguished from providing physical material. The bar under Article 20(3) is invoked when statements are likely to lead to incrimination themselves or "furnish a link in the chain of evidence" needed for incrimination.

C. Analytical Framework for Decryption

Applying the established principles from Kathi Kalu Oghad and Selvi to compelled decryption, the core analysis hinges on whether the act of unlocking a digital device is a positive volitional act that furnishes evidence and has communicative content conveying personal knowledge.

As the act of providing a password, PIN, or pattern is often argued to involve the accused recalling and inputting information stored in their memory. This is seen as applying mental faculties and communicating knowledge (testimonial fact). It is not merely exhibiting a physical characteristic like a fingerprint. Some even argued that using biometric identifiers like fingerprints or facial scans to unlock a device to have a communicative aspect because it implicitly asserts control over the device and its contents and provides a link between the person and the data stored within.

Furthermore, the compulsion element is crucial. Article 20(3) protects against being "compelled to be a witness". The term "compulsion" in this context means duress. It is not limited to physical violence. As clarified in Nandini Satpathy v. P.L. Dani , compulsion can include "psychic torture, atmospheric pressure, environmental coercion, tiring interrogative prolixity, overbearing and intimidatory methods". The Court in Nandini Satpathy extensively examined the relationship between Article 20(3) and Section 161(2) of the Code of Criminal Procedure, 1973, concluding that they substantially cover the same area. Section 161(2) provides immunity to a person being examined by the police from answering questions that would "expose him to a criminal charge". The right to silence under both provisions extends beyond the immediate case to protect the accused from disclosure of incriminating matter related to other offences pending or imminent.

Compelling an accused to unlock a device, particularly through methods involving mental recall like passwords, under the pressure of police investigation, constitutes the necessary element of coercion to potentially invoke Article 20(3) protection. This act, by providing access to potentially incriminating data, is not merely producing physical evidence but is a step that furnishes information leading to evidence, and as such, involves communicative content related to personal knowledge or control over the device and its contents. The subsequent access to the device's contents directly flows from this compelled act, creating a strong argument that the act of unlocking itself falls within the ambit of "being a witness against himself".

## III. FORENSIC REALITIES OF DIGITAL EVIDENCE

Digital devices being present all-most everywhere in the modern life have become indispensable source of evidence in criminal investigation. However, their forensic examination presents unique challenges and considerations making it fundamentally distinct from traditional physical evidence. Understanding the technical anatomy of digital security and the practicalities of digital forensics is crucial for a proper legal analysis concerning constitutional protections.

A. Technical Anatomy of Encryption

In the modern times, electronic devices are inherently designed with the security features, the most significant being encryption. Encryption is the process of encoding data in such way that it is unintelligible without a specific key. This involves processing material using an algorithm, which typically relies on a key. Encryption can be implemented at various levels. Device-level encryption secures the entire contents of a device which makes all data inaccessible without the correct key or password. Conversely, file-level encryption protects individual files or folders within a device which requires separate keys for access.

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

While the foundational principles of cryptography include symmetric and asymmetric ciphers, hashing functions, and key stretching techniques. The central focus in the context of compelled access concerns the authentication mechanisms required to decrypt encrypted data. These mechanisms generally involve different ways like password, passcode, PIN, or biometric identifier. These serve as the "keys" that grant authorized access to otherwise inaccessible information.

B. Decryption Pathways & Forensic Feasibility

Gaining access to encrypted digital evidence can be done by several ways each of them presenting different forensic and legal implications.

Firstly, password entry, this is the most direct method which requires the user to input a memorised string of characters (password, passcode, PIN). The security of this method depends on the password's complexity. Long, complex passwords are highly resistant to brute-force attacks, which involve trying every possible combination. The technical feasibility of brute-forcing is limited by password strength and device security features that introduce delays or wipe data after repeated failed attempts. Compelling an individual to provide a password relies on their knowledge of that specific information.

Secondly, biometric unlocks, devices can also be unlocked using biometric identifiers such as fingerprints, facial scans, or iris scans. These methods rely on storing a template of the user's biometric feature and matching it against the live scan provided. While seemingly physical acts, some sources argue that using biometrics for decryption is functionally equivalent to providing a password, as both acts achieve the same outcome i.e. unlocking and accessing the device's contents. The reliability of biometrics involves considerations of false positives (incorrect match) and false negatives (correct feature not recognised). Forensically, gaining access via either method allows investigators to then extract the device's data. However, the means by which access is obtained is critical for legal analysis.

C. Forensic Best Practices

The proper forensic handling of digital evidence is paramount to ensure its integrity and admissibility. For which there are three key practices:

i. Imaging and Write-Blockers: Creating an exact duplicate or "image" of the digital media is standard practice. Forensic tools often employ "write-blockers" to prevent any alteration of the original data during the imaging process, preserving metadata and file integrity (implied by the mention of metadata alteration and hash values).

ii. Chain of Custody: Maintaining a meticulous record of who has handled the device and evidence, when, and why is essential to prove that the evidence has not been tampered with from the moment of seizure.

iii. Integrity via Hash-Value Comparison: Generating "hash values", unique digital fingerprints of the data before and after forensic procedures is a critical step to verify that the data's integrity has been maintained. Any change, however small, will result in a different hash value, indicating potential alteration.

These established procedures for handling electronic records and devices to safeguard against data leaks and breaches becomes important particularly given the sensitive nature of the data involved.

D. Legal Differentiation

The forensic processes raise critical legal questions regarding the application of Article 20(3). Does the seemingly non-invasive nature of collecting a physical characteristic like a fingerprint for identification, as deemed non-testimonial in Kathi Kalu Oghad, translate to non-testimonial status when that biometric is used to decrypt a device?

The distinction between "physical evidence" (like fingerprints for comparison) and "testimonial evidence" (conveying personal knowledge) is central. Kathi Kalu Oghad held that providing fingerprints or handwriting specimens is not testimonial because they are used for comparison and do not inherently incriminate "by itself". However, in case of compelling decryption, whether by password or biometric, provides access to potentially incriminating contents. These contents, unlike mere physical characteristics, can incriminate the accused by themselves.

The "key vs. combination" analogy, often discussed in US jurisprudence, is relevant here. Providing a key (like a physical key or arguably a fingerprint for identification) is sometimes seen as a non-testimonial act of production, merely providing access to an existing item. Revealing a combination (like a password) is seen as testimonial because it requires revealing knowledge stored in the mind. When applied to biometrics for decryption, some argue it is like providing a key. However, a counter-argument, supported by Selvi's function-based test, posits that the use of a biometric to unlock and decrypt goes beyond mere physical identification and is testimonial because it implicitly communicates possession, control, or knowledge related to the

device and its contents. It is not the biometric itself that is the evidence sought, but the access it grants to the data, and the act of providing this access is argued to involve a testimonial assertion or conveyance of information. The legal challenge lies in harmonising this functional reality with the established distinction between physical and testimonial compulsion.

## IV. INDIAN CASE-LAW & JUDICIAL TRENDS

In the nascent and rapidly evolving landscape of digital evidence, particularly concerning compelled decryption and constitutional rights, Indian jurisprudence offers a complex tapestry of judicial pronouncements. Absent explicit legislative clarity in the predecessor statutes, courts have grappled with applying traditional legal principles to novel technological challenges. While the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023, signal legislative intent to modernise, the foundational judicial interpretations under the erstwhile regime remain crucial for understanding the current trajectory and the unresolved issues. The central question is whether compelling an accused to unlock a digital device infringes the protection against self-incrimination under Article 20(3) has elicited divergent opinions, primarily from the High Courts, underscoring the imperative for authoritative guidance from the Supreme Court.

### A. Supreme Court Landmarks

Several landmark judgments of the Supreme Court, though not directly addressing digital decryption, provide the constitutional bedrock against which such actions must be assessed.

Foremost among these is K.S. Puttaswamy v. Union of India (2017) , which unequivocally recognised the Right to Privacy as an intrinsic part of the Right to Life and Personal Liberty under Article 21 of the Constitution. This seminal ruling established that any state action impinging upon privacy must satisfy a three-fold test: it must be backed by a valid law, serve a legitimate state interest, and be proportionate to the objective sought. It can be indicated that the prevention and investigation of crime is considered a "legitimate interest of the State" within the Puttaswamy framework. The Court also adopted the notion of "reasonable expectation of privacy", a concept highly relevant to the vast personal data stored on digital devices. Consequently, any compulsion to unlock a device must not only have legal backing but also be necessary and proportionate, considering the profound privacy implications of unfettered access to a device's contents.

The issue of testimonial compulsion under Article 20(3) is significantly shaped by the principles laid down in State of Bombay v. Kathi Kalu Oghad & Ors (1961) and reiterated and expanded upon in Selvi & Ors v. State of Karnataka (2010). Kathi Kalu Oghad held that compelling an accused to provide physical evidence such as thumb impressions, fingerprints, or handwriting samples for identification purposes does not amount to testimonial compulsion, as it does not involve a statement based on the accused's personal knowledge. Selvi further clarified and applied this distinction, primarily in the context of narcoanalysis, polygraphy, and brain-mapping tests, holding them to be violative of Article 20(3) if conducted without consent, as they seek to elicit information of a testimonial character. It has to be highlighted that courts grappling with compelled decryption have relied heavily on these two precedents, often drawing differing conclusions on whether providing a password or biometric is akin to a physical sample (non-testimonial) or a statement based on personal knowledge (testimonial).

Furthermore, Nandini Satpathy v. P.L. Dani (1978) is cited for clarifying the scope of the right to silence. This judgment established that the protection under Section 161(2) of the Code of Criminal Procedure, 1973 (now presumably incorporated in the BNSS) and Article 20(3) are "substantially the same". It confirms the accused's right to remain silent not only during trial but also during investigation, safeguarding them against being compelled to disclose information that could expose them to a criminal charge. This principle directly informs the debate on whether compelling decryption forces an accused to reveal potentially incriminating data.

### B. High Court Divergences

The application of these Supreme Court principles to the digital realm has resulted in conflicting judgments from various High Courts and lower courts. A prominent instance is the Karnataka High Court's decision in Virendra Khanna v. State of Karnataka (2021). The Court permitted the compulsion of an accused to provide passwords or biometrics to unlock digital devices. The reasoning employed was multi-faceted: It equated providing a password or biometric to producing a document under Section 139 of the Evidence Act, 1872, or being akin to producing a document as per Section 91 of the CrPC, neither of which were considered

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

testimonial compulsion. Drawing from Kathi Kalu Oghad, it reasoned that compelled disclosure of passcodes/biometrics was merely for identification purposes, like providing fingerprints or voice samples, and did not require the accused to make a statement exposing them to guilt. Further, it held that any privacy concerns were addressed by the state's legitimate interest in investigating crime, as recognised in Puttaswamy. The Court suggested that the evidence obtained would, in any case, need independent proof of its relevance and admissibility in court. A Kerala High Court judgment also approved compelled access to mobile phones, relying similarly on Kathi Kalu Oghad and Virendra Khanna.

However, the Virendra Khanna judgment faced criticism. As it is generally argued that its interpretation of document under Section 91 CrPC is flawed, as passwords are not physical documents but reside in the zone of mental privacy. They contend that equating passwords/biometrics to physical identification samples misinterprets Kathi Kalu Oghad, as unlocking a device provides direct access to potentially incriminating content, unlike a fingerprint which merely aids in authenticating external evidence.

Subsequently, the Delhi CBI Special Court in CBI v. Mahesh Kumar Sharma (2022) took a contrary stance, holding Virendra Khanna to be per incuriam (passed without due regard to relevant law, specifically Selvi). While not a formal overruling by a superior court, this judgment created a significant divergence. The Mahesh Kumar Sharma court drew a distinction between passwords and biometrics. It held that compelling the disclosure of a password constitutes testimonial compulsion violative of Article 20(3) because it requires the application of the accused's mental faculties and personal knowledge. However, it suggested that unlocking a phone using biometrics (like fingerprints or facial recognition) might not violate Article 20(3) because it is akin to providing physical samples. This split approach, while attempting to reconcile with the physical-evidence distinction in Kathi Kalu Oghad, has been noted for its potential inconsistency, given that biometrics often require initial password setup and both methods ultimately grant access to the same digital content.

Indian courts have displayed varied holdings regarding compelled passcodes, device seizures, and the admissibility of digital evidence like WhatsApp chats, reflecting the absence of a clear, uniform standard. While Virendra Khanna and the Kerala High Court permitted compulsion, the Delhi CBI Special Court in Mahesh Kumar Sharma did not for passwords. The Supreme Court's direction in Ajay Bhardawaj v. Union of India , requiring an accused in the GainBitcoin scam case to provide cryptowallet credentials, further illustrates judicial inclination towards compelled access in specific cases, although the sources do not detail the constitutional arguments raised or considered in that instance.

C. Thematic Insights

The application of the proportionality, necessity, and legitimacy tests derived from Puttaswamy is crucial for evaluating state intrusion into digital privacy. Courts must assess whether compelling decryption is a proportionate response to the investigative need, considering less intrusive alternatives and the potential for accessing vast amounts of irrelevant, private data. While crime investigation is a legitimate state interest, the extent and manner of data access must be justified under law.

The jurisprudence also reveals a problematic attempt to map patterns by device type and unlock method, particularly the distinction between passwords and biometrics. As highlighted by the divergent views in Virendra Khanna and Mahesh Kumar Sharma, and analyses from US courts, treating these differently creates inconsistency. The argument is made that both serve the same purpose – accessing the device's content – and drawing a constitutional line based on the mechanism (what is known vs. what is physical) is artificial and fails to protect the underlying informational privacy.

Ultimately, the judicial trend, albeit fragmented, indicates a recognition of the profound privacy implications of digital devices. Several sources argue for treating cell phones as warranting a "new zone of privacy", given their ubiquitous nature and their role as repositories of intimate personal information, arguably akin to an extension of the self or the human mind. This perspective, supported by US judgments like Riley v. California and Carpenter v. United States, suggests that the traditional frameworks for physical searches or document production are ill-suited for the digital age. The pending Ram Ramaswamy petition before the Supreme Court signifies the ongoing need for clear, harmonised guidelines that balance state investigative powers with fundamental rights in the digital age.

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

## V. INTERNATIONAL STANDARDS & COMPARATIVE JURISPRUDENCE

Exploring international perspectives provides valuable context for understanding the challenges India faces regarding electronic evidence and constitutional rights. United States jurisprudence, in particular, is frequently referenced in Indian cases and scholarly analysis due to the similarity between the constitutional protections against self-incrimination in both countries.

### A. United States

The Fifth Amendment to the US Constitution provides protection against self-incrimination, stating that no person "shall be compelled in any criminal case to be a witness against himself". This protection is similar to Article 20(3) of the Indian Constitution. For the Fifth Amendment privilege to apply, an act must be compelled, incriminating, and testimonial. The rationale often cited for this privilege is the "cruel trilemma", highlighting the injustice of forcing a witness to choose among self-incrimination, perjury, or contempt of court.

US jurisprudence has also grappled with the impact of technology on constitutional rights. Riley v. California (2014) is a significant case where the US Supreme Court held that the Fourth Amendment requires a warrant before the government searches the digital data on a cell phone incident to arrest. The Court recognised the unique nature of cell phones as indispensable devices containing vast amounts of private information and warranting a higher level of protection, viewing them as an extension of an individual's self.

The Foregone Conclusion Doctrine is an exception to the Fifth Amendment privilege that emerged from Fisher v. United States (1976). This doctrine states that if the government can show that it already knew of the existence, location, and authentication of evidence with reasonable particularity at the time it compelled its production, the act of production is a "foregone conclusion", and the Fifth Amendment privilege does not apply to that act. The US Supreme Court's decision in United States v. Doe (1984) further elaborated on the act of production doctrine and introduced the analogy of compelling a signature to access bank records being non-testimonial as it did not disclose the contents of the mind. Later, United States v. Hubbell (2000) offered another analogy, comparing compelled decryption to either producing a "combination to a safe" (testimonial) or a "key to a lock" (nontestimonial).

US courts have applied the Foregone Conclusion Doctrine differently when it comes to compelling individuals to decrypt electronic devices, leading to varying outcomes. Some courts apply the reasonable particularity standard to the underlying content sought, while others focus on whether the act of producing the password or biometric is testimonial.

### B. Lessons for India

Given the similar constitutional protections against self-incrimination, the suggestion that India could benefit from adopting principles from US jurisprudence, particularly the Foregone Conclusion Doctrine, to navigate the complexities of compelled decryption of digital devices. This could help balance individual rights against self-incrimination and privacy with the state's duty to investigate crimes.

The existing lack of regulations exposes personal data to unwarranted access. While not explicitly detailing a "warrant → hearing → immunity" structure, it is to be emphasised that the need for judicial oversight such as warrants and highlight the need for clear guidelines from the Supreme Court. The concept of immunity is related to self-incrimination; the core right being discussed. Suggested interim guidelines in the Supreme Court petition propose requiring investigators to establish the existence, basis for suspicion, and relevance of the evidence sought. This implies a move towards requiring justification and potentially a hearing or judicial review before compelled decryption.

Further, there is a call for comprehensive regulatory frameworks and a timely resolution of the legal issue by the Supreme Court. This would necessarily involve laying down clear standards for when and how decryption can be compelled, potentially distinguishing between different forms of decryption like passwords and biometrics. The Virendra Khanna case demonstrated the risks of equating physical evidence like fingerprints with digital access methods like biometrics. The adoption of principles from the Foregone Conclusion Doctrine, potentially incorporating a reasonable particularity standard, is suggested as a way to create a more defined framework.

Moreover, drawing from US cases like Riley v. California and Carpenter v. United States, the it can be argued that cell phones warrant the creation of a new zone of privacy due to their intrusive nature and the vast, retrospective data they hold. India's stance, particularly post-Puttaswamy which locates privacy under Article

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

21, and cases like Canara Bank that state privacy is attached to people, provide a foundation for this recognition.
The need for robust digital infrastructure to safeguard against data leaks and breaches, especially given the sensitive data collected under laws like the Criminal Procedure (Identification) Act, 2022 , is also a crucial consideration for India.

## VI. CONCLUSION & RECOMMENDATIONS

The legal landscape surrounding compelled decryption in India is currently in flux due to a lack of an authoritative pronouncement by the Supreme Court. Different courts have taken opposing views. The Karnataka High Court has held that compelling disclosure of passwords or biometrics does not violate the right against self-incrimination under Article 20(3), reasoning that mere disclosure is not incriminating and aligning it with permissible searches. This court also distinguished biometrics as physical evidence not requiring personal knowledge, thus not protected by Article 20(3). In contrast, the Delhi CBI Special Court disallowed compelling password disclosure, finding it directly affects the right against self-incrimination. However, this court held that unlocking a phone using fingerprint or facial recognition will not violate Article 20(3), distinguishing body measurements from testimonial acts.
Scholars argue that both passwords and biometrics used to access electronic devices should be protected under Article 20(3). They contend that these methods act as a 'vehicle' to access contents falling within the accused's personal knowledge. Compelling password disclosure involves applying mental faculties and is a “testimonial fact”. Furthermore, compelling biometrics for unlocking is seen as testimonial because of its function in producing access to information. The distinction between compelling a password versus biometrics has been called “artificial” and is criticised because the outcome i.e. unlocking the device is the same. The act of unlocking, regardless of method, is considered testimonial and potentially incriminating.
In the US, courts also disagree on how the Fifth Amendment applies to compelled decryption. The foregone conclusion doctrine is a key concept, suggesting that if the government already knows the facts that the compelled act would reveal (e.g., that the suspect knows the password), the testimonial aspect may be minimal, and the privilege may not apply. There is significant debate on whether this doctrine applies to passwords and biometrics and what the government must prove it knows. Some argue that compelled biometric decryption is testimonial, particularly because it communicates ownership or control of the device.
Therefore, while there is no uniform answer in India, there is a strong argument based on scholarly analysis and some judicial decisions that compelled password decryption presumptively violates Article 20(3), requiring a stringent justification like the US foregone conclusion doctrine. Compelled biometric decryption is on unsteady judicial ground currently, but many argue it should also be protected under Article 20(3).
The current legal uncertainty and conflicting court decisions highlight the need for significant reform.

i. There is a clear call for model legislation for the search, seizure, and examination of digital devices, aligned with fundamental rights. This legislation should mandate a “prior judicial warrant” except in emergencies. This aligns with your recommendation for a Digital Decryption Warrant regime with detailed standards, addressing the issue that existing laws like the Criminal Procedure (Identification) Act may not adequately cover digital access methods.

ii. A timely resolution by the Supreme Court of India is crucial. The Court needs to address the issue from the perspective of both self-incrimination and the right to privacy. Adopting a uniform testimonial-compulsion test that avoids arbitrary distinctions, such as the one between passwords and biometrics made by some courts, is necessary. Scholars advocate for rejecting arbitrary biometric exceptions, arguing that the method of unlocking should not determine the level of constitutional protection. Evolving a rule similar to the US foregone conclusion doctrine is suggested as a way to balance rights and investigation.

iii. Recent events have highlighted concerns about the abuse of investigative powers and the lack of safeguards during the seizure of electronic devices. There is a need for robust guidelines concerning seizure, such as providing a memo and generating hash values. While one court laid down some handling guidelines, a pending case before the Supreme Court seeks further action. Mandating the use of independent, certified labs and ensuring robust chain-of-custody and metadata integrity checks

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

aligns with the need for proper handling and preservation of digital evidence highlighted in the sources.

The issue of compelled decryption inherently involves a balancing act between the State's legitimate duty to investigate crimes and the individual's constitutional rights against self-incrimination and to privacy. Digital devices are storehouses of highly private information, and unbridled access can expose aspects of an individual's identity beyond the State's legitimate interest. Modern technology, particularly encryption, has created significant challenges for law enforcement by inserting powerful “password gates” in routine searches. The debate touches upon themes of security, surveillance, public interest, and privacy. The goal is to find a balance that allows for fair investigations without obstructing constitutional protections or forcing individuals to bargain away their rights for enhanced security. Reconciling national security imperatives with individual liberties and ensuring forensic science practices uphold fundamental rights is the central challenge.