PASSWORD AS EVIDENCE: JUDICIAL APPROACH TO PASSWORD PROTECTION AND RIGHT AGAINST SELF-INCRIMINATION IN DIGITAL WORLD

Shahnawaz Ahmad, Research Scholar, The National University of Advanced Legal Studies (NUALS), Kochi
Assistant Professor, Crescent School of Law, BSA Crescent Institute of Science & Technology, Chennai

Dr. Mini S, Professor, The National University of Advanced Legal Studies (NUALS), Kochi

ABSTRACT

This research paper deals with the correlation between the utilization of passwords as evidence and the right against self-incrimination in the digital realm, with special reference to recent issues raised by High Court of Karnataka in Virendra Khanna v. State of Karnataka and Anr. (2021) and by Rouse Avenue District Court, Delhi in Central Bureau of Investigation v. Mahesh Kumar Sharma (2022), With the growing dependence on digital platforms and devices, passwords have gained substantial significance as evidentiary elements in the criminal justice system. However, its use as evidence raises complex legal and ethical issues, particularly the right against self-incrimination.

By examining constitutional perspectives, this paper investigates the legal framework in India and analyzes constitutional provisions that safeguard the right against self-incrimination. It analyzes court rulings and interpretations regarding the compelled disclosure of passwords, aiming to strike a balance between the right of individual and state power of investigation. Landmark judicial precedents from the Supreme Court of India and various High Courts provide practical insights into the Indian scenario, enabling a comprehensive understanding of right against self-incrimination and implications pertaining to compelled password disclosure.

Policy and legislative considerations are also analyzed in this research. The effectiveness in protecting the right against self-incrimination by existing policies and guidelines in India concerning password disclosure is also examined. Additionally, the study explores potential legislative reforms and proposes possible solutions for conflict between individual rights and law enforcement interests. Finally, this research paper tries to analyze the complex relationship between passwords as evidence, the right against self-

incrimination, state power to investigate and the legal framework in India. By addressing ethical, legal, and technological realm, it offers policymakers, legal experts, and individuals dealing with the ever-changing digital world a comprehensive understanding of this complicated issue.]

Keywords: Password, Testimonial, Non- Testimonial, Evidence, Self-Incrimination, Privacy, Investigation. Digital Evidence, Privacy, Investigation.

INTRODUCTION

Passwords find a significant place in the digital realm, serving as essential tools for securing personal accounts, protecting sensitive information, and in maintaining digital privacy.[1] Concurrently, the right against self-incrimination plays a crucial role in Indian legal system, safeguarding individuals from being compelled to provide evidence against themselves. This right allows individuals the freedom to remain silent throughout investigation and avoid self-incrimination.[2]

The relevance of the right against self-incrimination is enshrined under Article 20(3) of the Constitution of India, 1950.[3] This constitutional provision guarantees individuals the right to remain silent and protection against being forced to disclose self-incriminating information. It serves as a fundamental right in the country's legal framework, ensuring that individuals are not compelled to reveal incriminating evidence against themselves.[4]

This research paper seeks to provide a comprehensive understanding of the relationship between passwords and the right against self-incrimination by examining the significance of their relevance and interaction.[5] It will analyze the legal framework in India, including constitutional provisions and constitutional court rulings that shape the boundaries of compelled password disclosure.[6] Additionally, ethical, technological, and policy implications related to passwords as evidence and the protection of the right against self-incrimination will

[1] Houser, Kimberly A., and W. Gregory Voss, 'GDPR: The end of Google and Facebook or a new paradigm in data privacy' (2018) 1 Rich. JL & Tech. 25
[2] Peyton, Antigone, 'The Connected State of Things: A Lawyer's Survival Guide in an Internet of Things World' (2016) 2 Catholic University Journal of Law and Technology, 24
[3] The Constitution of India, 1950, Art 20(3)
[4] Kumar Pandey, Pankaj, and Aqa Raza, 'Protection Against Self-Incrimination's a Fundamental Right in India: A Critical Appraisal' (2015) 42 Indian Bar Review 133, 159
[5] Guarda, N. Dalla, 'Digital Encryption and the Freedom of Self-Incrimination: Implications for the Future of Canadian Criminal Investigations and Prosecutions' (2014) 61 Crim. LQ, 119
[6] Dixon, Pam, 'A Failure to "Do No Harm"- India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the US' (2017) 4, Health and technology 7, 539, 567

be discussed in length.[7]

Through background, the research paper aims to analyze the challenges, considerations, and potential solutions associated with the use of passwords as evidence while upholding the right against self-incrimination.[8] This research paper contributes to the continuing debate over digital privacy, individual rights, and the changing nature of evidence in the digital age by contextualizing these concerns within the Indian legal and constitutional framework.[9]

UNDERSTANDING THE RIGHT AGAINST SELF-INCRIMINATION IN INDIA

Historical development and legal foundations of the right in India

The right against self-incrimination holds significant importance within India's criminal justice system and finds its basis in the Part III of Indian Constitution. Its historical development can be traced back to the formulation of Article 20(3) of the Indian Constitution, 1950.[10]

Article 20(3) of the Indian Constitution explicitly protects the right against self-incrimination, stating that *"no person accused of any offense shall be compelled to be a witness against himself."* This constitutional provision ensures that individuals have the liberty to remain silent throughout the investigation process and refrain from providing evidence that could incriminate him.[11]

While Section 161 of the Code of Criminal Procedure, 1973 expressly states that an investigating officer can question any individual who is acquainted with the facts and circumstances of the case, this provision of the Cr.P.C. cannot supersede the constitutional protections afforded to individuals under the Constitution of India.[12] The same is also mandated under section 161(2) of Cr.P.C. that one is bound to answer all questions regarding the case truthfully when put forth by investigating officer, except for questions whose answers could

[7] Cohen, Aloni, and Sunoo Park, 'Compelled decryption and the Fifth Amendment: Exploring the technical boundaries' (2018) 32, Harv. JL & Tech. 169
[8] Kerr, Orin S, 'Compelled decryption and the privilege against self-incrimination, Tex. L. Rev. 97 (2018): 767.
[9] Morrison, Caren Myers, Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment' (2012) 65, Ark. L. Rev. 133
[10] *Supra* note 4.
[11] *Id.*
[12] The Code of Criminal Procedure, 1973, S. 161

incriminate him or result in a penalty or forfeiture.[13]

The legal foundations of this right extend beyond constitutional provisions and find place in judicial decisions, including notable cases such as *Nandini Satpathy v. P.L. Dani*[14], *State of Bombay v. Kathi Kalu Oghad*[15] and *Selvi v. State of Karnataka*[16], have played a crucial role in shaping the understanding and scope of the right against self-incrimination in India.

In *Selvi v. State of Karnataka*[17] reported in 2010, the Hon'ble Supreme Court pronounced that subjecting the accused to a Polygraph Test is in violation of the 'right against self-incrimination.' This right is considered a fundamental right protected under Article 20(3) of the Constitution.

Scope and Limitations of the Right in the Context of Digital Evidence

With respect to digital evidence, the right against self-incrimination poses specific challenges and considerations for judicial system.[18] With the advancement of digital technology and the pervasive nature of digital interactions, individuals leave behind a digital trail like IP Address that can potentially be used as evidence in criminal investigations[19]. This includes information protected by passwords, such as personal communications, stored data, digital media, and online activities.[20]

The scope and limitations of the right against self-incrimination become more complex when dealing with digital evidence. Indian courts have grappled with finding a balance between upholding the right against self-incrimination and the necessity of effective law enforcement in cases involving password-protected digital evidence specially after two recent conflicting decisions one by High Court of Karnataka in *Virendra Khanna v. State of Karnataka and Anr.*[21] and other by Rouse Avenue District Court, Delhi in *Central Bureau of Investigation v. Mahesh*

[13] *Id.*
[14] *Nandini Satpathy v. P.L. Dani*, AIR 1978 SC 1025, 1978 SCR (3) 608.
[15] *State of Bombay v. Kathi Kalu Oghad*, AIR 1961 SC 1808, 1962 SCR (3) 10.
[16] *Selvi v. State of Karnataka*, AIR 2010 SC 1974, (2010) 7 SCC 263.
[17] *Id.*
[18] Soares, Nicholas, 'The Right to Remain Encrypted: The Self-Incrimination Doctrine in the Digital Age' (2012) 49, AM. Crim. L. Rev. 2001
[19] Solove, Daniel J., *The Digital Person: Technology and Privacy in The Information Age*. Vol. 1. NyU Press 2004)
[20] *Id.*
[21] *Virendra Khanna v. State of Karnataka and Anr.*, W.P. No. 11759/2020 (Decided on 12.03.2021)

Kumar Sharma[22] case.

While Indian courts have acknowledged that compelling individuals to disclose their personal information (passwords/biometric) can infringe upon their fundamental right i.e., right against self-incrimination,[23] there have been instances where courts have ordered the compelled disclosure of passwords, particularly when the password is considered a "non-testimonial" rather than testimonial in nature for the purpose of investigation only.[24]

As technology continue to evolve and legal precedents are established, the scope and limitations of the right against self-incrimination with respect to digital evidence continue to evolve.[25] It is pertinent to address the unique challenges posed by digital evidence and strike a careful balance that respects individual rights against self-incrimination while ensuring the efficient administration of justice in the digital realm.[26]

PASSWORDS AS DIGITAL EVIDENCE

a) Definition and Types of Digital Passwords

According to the National Institute of Standards and Technology (NIST), a password is "a memorized secret, consisting of a sequence of characters, used to authenticate a user to a system." This definition emphasizes that a password is a confidential and memorable secret that allows a user to prove their identity and gain access to a particular system or service.[27]

Whereas digital passwords refer to authentication credentials used to secure access to various digital platforms and services. These passwords may be in the form of alphanumeric combinations, PINs, passphrases, biometric data, or other authentication factors.[28] Digital passwords encompass a wide range of applications, including e-commerce platforms, email accounts, encrypted devices, social media profiles, online banking, and encrypted communication services. Each type of password serves as a unique identifier and a protective

[22] *Central Bureau of Investigation v. Mahesh Kumar Sharma,* 2022 SCC OnLine (Dist. Court (Del) 48, decided on 29-10-2022).
[23] *Id.*
[24] *Supra* note 22.
[25] *Supra* note 19.
[26] Kerr, Orin S, 'Compelled decryption and the privilege against self-incrimination', (2018) 97 Tex. L. Rev. 767.
[27] National Institute of Standards and Technology (NIST), US Dept of Commerce.
[28] Clarke, Nathan. Transparent user authentication: biometrics, RFID and behavioural profiling. Springer Science & Business Media, (2011).

barrier against unauthorized access.[29]

b) Evidentiary Value of Passwords in Criminal Investigations

Passwords hold significant evidentiary value in criminal investigations conducted by investigating authorities under relevant provisions of Cr.P.C.[30] They can provide crucial information regarding an individual's online activities, communication patterns, and stored data. Password-protected digital evidence can be instrumental in establishing the connection between a suspect and an alleged crime, uncovering motives, and establishing a timeline of events.[31]

Passwords lie corroborate, or challenge statements made by the accused, verify digital transactions or communications, and provide evidence of intent or involvement in criminal activities under relevant provisions of Indian Evidence Act, 1872.[32] The evidentiary value of passwords lies in their ability to unlock access to essential digital information that may be relevant to an investigation.[33]

Testimonial Nature of Password:

Some scholars are having an opinion that the results obtained from tests such as polygraph examination are "testimonial" acts that should come within the prohibition of the right against self- incrimination.[34] The outcomes yielded by polygraph tests and other lie detector test, regardless of whether they are obtained through voluntary means or not, can be considered 'testimonial'. This is because these tests serve as inductive evidence of the accused state of knowledge or belief.[35]

Similarly, disclosers of password may also be treated as "personal testimony" since they are a means for "imparting personal knowledge about relevant facts".[36] The results obtained

[29] Ombiro, Zablon BH. 'Mobile–Based Multi-Factor Authentication Scheme for Mobile Banking' (2016) PhD diss., University of Nairobi
[30] Saxena, Nidhi, and Veer Mayank, 'Forensic Hurdles in Investigating & Prosecuting Cyber-crime-An Overview', The Indian Pol. J. 96.
[31] *Id.*
[32] George, Ms Jaisy, and Ashish Deshpande, 'Impact of Technology in Investigations: The Judicial Response to Admissibility of Evidence Obtained Technologically' (2021) NVEOJ, 12023-12041
[33] *Id.*
[34] Pardo, Michael S, 'Self-incrimination and the epistemology of testimony' (2008) 30 Cardozo L. Rev. 1023
[35] *Id.*
[36] Rizzo Parse, Rosemarie, 'Truth for the moment: Personal testimony as evidence' Nursing Science Quarterly (2008) 21, 45-48.

through the involuntary administration of revealing password for investigation purposes come within the scope of "testimonial compulsion", thereby attracting the protective shield of Article 20(3) of the Constitution. Since courts in India are not having a concrete opinion that whether disclosure of password is testimonial evidence or simply an information given by an individual to facilitate the investigation process.[37]

c) Case Studies Highlighting the Use of Passwords as Evidence in India

There are several instances in India demonstrate the use of passwords as evidence in criminal investigations. For example, in *the Rhea Chakraborty case*,[38] passwords to social media accounts and digital devices played a significant role in establishing communication patterns and potential evidence related to drug consumption issues.

In the *Aarushi Talwar murder case*, passwords to email accounts and other digital platforms were crucial in unraveling the sequence of events and establishing the involvement of individuals.[39]

The High Court of Karnataka in *Virendra Khanna v. State of Karnataka and Anr*[40]. analyzed various provisions of Indian Evidence Act, 1872 and the Code of Criminal Procedure, 1973 and held Section 139 of the Indian Evidence Act states that individuals can be legally summoned to present a "document."[41] The Indian Evidence Act's Section 3 defines "evidence,"[42] which encompasses all forms of documents, including electronic records. Therefore Section 139 of Indian Evidence Act, 1872 authorizes the disclosure of electronic record and it does not violate right to privacy of individual under Article 21 of the Constitution.[43]

It further held that the disclosure of password is of the nature of giving specimen signatures or handwriting as held by the supreme court of India in *Ritesh Sinha v. State of Uttar*

[37] *Supra* note 4.
[38] Subhangi Mishra, 'Rhea Chakraborty's media trial shows Indians confuse drug addicts with criminals' *THE PRINT*, available at https://theprint.in/opinion/pov/rhea-chakrabortys-media-trial-shows-indians-confuse-drug-addicts-with-criminals/491690/ (Last visited 20 May, 2023)
[39] Outlook Web Bureau, 'Aarushi Talwar Murder Case: A Timeline Of Events' *Outlook*, available at https://www.outlookindia.com/website/story/aarushi-talwar-murder-case-a-timeline-of-events/302932 (Last visited 20 May, 2023)
[40] *Supra* note 22.
[41] Indian Evidence Act, 1872, s 139
[42] Indian Evidence Act, 1872, s 3
[43] The Constitution of India, 1950, Art 21.

Pradesh [44] that a Magistrate may order for the collection of voice sample under Section 311-A of the Code of Criminal Procedure, 1973.

In the case of *Sudhir Chaudhry v. State* (2015 SCC On Line Del 7457),[45] the learned Single Judge of Delhi High Court determined that the purpose of obtaining a voice sample is to facilitate in comparing it with a recorded conversation. The voice sample itself does not serve as testimony as it merely functions as "identification data." According to the High Court's perspective, a voice sample is not a substantive piece of evidence. The High Court dismissed the argument that the requirement to provide a voice sample violated the fundamental right guaranteed under Article 20(3) of the Constitution.[46]

In the case of Justice *Puttaswamy,*[47] the Supreme Court of India ruled that the state has legitimate interests in the prevention and investigation of crime. The request for password disclosure is made in the context of criminal investigations. Hence, the order for disclosure serves a legitimate purpose of the state. The measure is deemed proportionate as it solely aims to obtain the password to aid in the investigation process. There exists a rational nexus between the objective and the means employed to achieve it.[48]

These cases decided by different high courts and the Supreme Court of India illustrate how passwords have been utilized as evidence in India to strengthen investigations, establish connections, and construct a comprehensive narrative surrounding criminal activities.[49]

The significance of passwords as digital evidence in criminal investigations highlights the importance of acknowledging their evidentiary worth and establishing suitable legal frameworks and protocols to guarantee their admissibility and credibility in court proceedings.[50] The assessment of the evidentiary value of passwords and the establishment of guidelines should be undertaken by the Supreme Court of India, as there are currently no explicit guidelines on this subject.[51] Striking a balance between protecting digital privacy rights

[44] *Ritesh Sinha v. State of Uttar Pradesh*, (2019) 8 SCC 1.
[45] *Sudhir Chaudhry v. State,* 2015 SCC On Line Del 7457.
[46] *Id.*
[47] *Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.,* (2017) 10 SCC 1, AIR 2017 SC 4161
[48] *Supra* note 22.
[49] *Id. See also Supra* note 23.
[50] Abhishek Sharma Padmanabhan and Santhy, Dr KVK, 'A Review on the Changing Dimensions of Digital Forensics in Criminal Investigations' (2023) SVP National Pol. Aca. J.
[51] Goldstraw-White, Janice, 'Legal And Policy Framework For Digital Forensics: A Resource For Practitioners', (2022).

and utilizing passwords as evidence remains a critical consideration for parliament and the judiciary in India.[52]

CONSTITUTIONAL CONSIDERATIONS AND LEGAL FRAMEWORKS IN INDIA

a) Constitutional provisions related to the right against self-incrimination:

Constitutional provisions pertaining to the right against self-incrimination provide essential safeguards. Article 20(3) of the Indian Constitution explicitly protects individuals from being compelled to be witnesses against themselves in criminal proceedings. It asserts that ***"no person accused of any offense shall be compelled to be witness against himself."***[53] This constitutional provision emphasizes the principle that individuals have the right to remain silent and cannot be compelled to testify against their own interests. It underscores the significance given to individual rights and fair justice administration in India.[54]

Article 20(3) ensures that individuals have the freedom to exercise their right to remain silence, placing limitations on the powers of law enforcement authorities and affirming that the burden of proof lies with the prosecution.[55] While this right is not absolute and may be subject to reasonable restrictions, it is an integral part of the broader constitutional framework that upholds justice & fairness and the protection of individual rights in the criminal justice system. Other constitutional provisions, such as the right to a fair trial (Article 21),[56] protection against double jeopardy (Article 20(2),[57] and the presumption of innocence (Article 21), further contribute to this framework. Together, these provisions shape the constitutional rights, maintaining a delicate balance between the interests of justice and the rights of the accused in India.

"To be witness" as used under Article 20(3) has been defined by the Supreme Court in *State of Bombay V/s Kathi Kalu Oghad*[58] as "To be a witness" means imparting of knowledge in respect of relevant facts by means of oral statements or statements in writing, by a person who has personal knowledge of the facts to be communicated to a court or to a person holding

[52] *Supra* note 51.
[53] The Constitution of India, 1950, Art 20(3).
[54] *Id.*
[55] Munjal, Nandish, and Shivain Arora, 'I Reserve the Right to Remain Silent' (2020) 15 Supremo Amicus 217
[56] The Constitution of India, 1950, Art 21.
[57] The Constitution of India, 1950, Art 20.
[58] *State of Bombay V/s Kathi Kalu Oghad*, AIR 1961 SC 1808, para-11. See also *supra* note 16.

an enquiry or investigation."[59]

The phrase "to be a witness" typically refers to the act of providing verbal testimony in a courtroom.[60] However, legal precedent has extended the literal interpretation of this phrase to encompass a broader definition, which includes the act of providing testimony in a court or outside of it, whether in oral or documentary form, by an individual who is accused of committing an offense.[61]

The only question is whether an individual who discloses their password to facilitate an ongoing investigation would be considered as providing "testimonial evidence," and if doing so would incriminate themselves. If the answer is yes, then disclosing the password would be protected by the right against self-incrimination.[62]

Whereas the Karnataka High Court is having a contrary opinion that there is no testimony which is given by the accused by providing the said password, passcode, or biometrics by which the document is being accessed by the Investigating officer.[63] The high court substantiated it logic by citing *Kathi Kalu Oghad case,*[64] that Eleven-Judge Bench of the Supreme Court has clearly established that actions such as providing a thumb impression, palm or foot impression, fingerprints, or a written specimen, or even revealing a part of the body for identification purposes by an accused person, do not qualify as testimonial evidence. The blurry opinion of the Karnataka High Court needs to be clarified and resolved by the Supreme Court of India.[65]

b) Interpretations and Court Rulings on Compelled Password Disclosure in India

The issue of compelled password disclosure in India has been a subject of legal interpretation and court rulings. Very few cases have emerged, leading to the establishment of certain principles and guidelines regarding the compelled disclosure of passwords. The interpretation of key judgments of Supreme Court and different High Court rulings in India can

[59] *Id.*
[60] Nagareda, Richard A, 'Compulsion to Be a Witness and the Resurrection of Boyd' (1999) 74 NYUL Rev. 1575
[61] *Id.*
[62] Herrera, Adam, 'Biometric Passwords and the Fifth Amendment: How Technology Has Outgrown the Right to Be Free from Self-Incrimination' (2019) 66 UCLA L. Rev. 778
[63] *Supra* note 22.
[64] *Supra* note 16.
[65] *Supra* note 64.

provide insights into this issue. Here are some key points:

The principle of a right to remain silent during the investigation is well recognized in the Supreme Court of United States' decision in *Miranda v. Arizona*[66], which is applied worldwide, and the same principle reaffirmed by the Hon'ble Supreme Court of India in the landmark decision of *Nandini Saptapathy v. P.L. Dani.*[67]

i) **Miranda v. Arizona (1966)**[68] was a landmark decision of United States Supreme Court that addressed the issue of the Fifth Amendment right against self-incrimination during police interrogations. Here are some brief facts and analysis of the case:

In 1963, Ernesto Miranda was arrested in Arizona for kidnapping and under rape charges. During the police interrogation, iranda confessed his crimes, but he was not informed of his right to remain silent throughout investigation or to have an attorney present. Miranda's confession was used as evidence against him during the trial, and he was subsequently convicted. Miranda appealed against his conviction and argued that his confession should have been excluded because he was not advised of his rights.[69]

The Supreme Court of United States, with a 5:4 majority, ruled that the prosecution may not use statements made by a defendant in response to police interrogation unless the defendant was first informed of their right to remain silent and their right to an attorney. The Court emphasized the importance of protecting an individual's Fifth Amendment privilege against self-incrimination and the right to counsel during custodial interrogations. The Court established what is now known as the "Miranda warnings" or "Miranda rights," which require law enforcement officers to inform suspects of their rights before conducting a custodial interrogation.[70]

The Court also ruled that if a suspect indicates during the interrogation that they wish to remain silent or have an attorney present, the interrogation must cease until the suspect's rights are honored. However, the Court stated that if a suspect voluntarily and knowingly waives their Miranda rights, any subsequent statements made by the suspect can be used

[66] *Miranda v. Arizona*, 384 U.S. 436 (1966) DD 13.06.1966
[67] *Supra* note 15.
[68] *Supra* note 67.
[69] *Id.*
[70] *Id.*

as evidence.[71]

This decision established a constitutional safeguard to protect individuals from self-incrimination during custodial interrogations. The ruling led to the widespread adoption of the Miranda warnings by law enforcement agencies across the country and worldwide.[72]

ii. **M.P. Sharma vs. Satish Chandra (1954*)*[73]** established that the right against testimonial compulsion under Article 20(3) is not limited to the courtroom. It applies to all individuals who face charges that could potentially result in prosecution.

iii. **State of Bombay vs. Kathi Kalu Oghad & Others (1962*)*[74]** indicated that the act of providing information about relevant facts through oral or written statements by someone who has personal knowledge of those facts to a court or a person conducting an inquiry or investigation would fall within the scope of the right protected under Article 20(3).

iv. **Nandini Satpathy v. P.L. Dani and anr. (1978)*[75]*** a landmark decision provided an interpretation of Article 20(3) of the Constitution. The Supreme Court recognized the right against self-incrimination as a fundamental right under Article 20(3) of the Constitution. and Section 161(1) of the Criminal Procedure Code, 1973.

The former Chief Minister (CM) of Orissa was charged under various sections of the Prevention of Corruption Act, 1988 and the Indian Penal Code (IPC) by the Deputy Superintendent of Police, Vigilance, Cuttack. The charges include owning assets beyond legal income, misuse of political power, and illegal gratification leading to an increase in wealth. The appellant and others involved in the case were interrogated based on a set of written questions.[76]

However, during her interrogation, she invoked her fundamental right under Article 20(3), which is the right against self-incrimination. This right, commonly known as the right to remain silent, protects a person from being compelled to incriminate themselves in the case they are being booked. On this, she challenged the rationality of the judicial

[71] *Id.*
[72] *Id.*
[73] M.P. Sharma vs. Satish Chandra**,** 1954 SCR 1077.
[74] State of Bombay vs. Kathi Kalu Oghad & Others, 1962 3 SCR 10. *See also Supra* note 16.
[75] *Supra* note 15.
[76] *Id.*

magistrate's authority by filing a petition with the High Court under Article 226 of the Indian Constitution. However, the High Court failed to address the scope of Section 161(2) of the Criminal Procedure Code. Subsequently, the appellant appealed to the Supreme Court under Article 132(1).[77]

The court ruled that in order to invoke Article 20(3), the party making the plea must be accused of an offense and must have been compelled to answer incriminating questions. Additionally, the court stated that summoning a woman as a witness at the police station violates Section 160(1) and influences her testimony. Furthermore, Section 161(2) and Article 20(3) provide immunity to the witness from being compelled to answer incriminating questions during the investigation.[78]

This decision established a foundation for protecting individuals from being compelled to disclose their passwords if it could incriminate them.[79]

v. **Selvi vs. State of Karnataka (2010)*[80]*** in this case the Supreme Court granted permission for a special leave petition pertaining to situations where objections were raised regarding the involuntary administration of neuroscientific tests to the accused, suspects, and witnesses during the investigation. The Court deliberated on the constitutional validity of utilizing neuroscientific tests, such as narcoanalysis, BEAP or 'brain mapping,' and polygraph tests, as a means to collect evidence. The polygraph test assesses various physiological responses, including respiration, blood pressure, pulse, and galvanic skin resistance, in order to detect falsehoods or deceit.[81]

One of the issues was "Whether the involuntary administration of the impugned techniques violated the 'right against self-incrimination' enumerated in Article 20(3) of the Constitution;" the Supreme Court examined the constitutionality of different methods used to gather evidence, which included narcoanalysis, BEAP (Brain Electrical Activation Profile) or 'brain mapping,' and polygraph tests. The Court ultimately concluded that the utilization of these neuroscientific investigative techniques amounted to testimonial compulsion. Consequently, they ruled that such practices violated an accused individual's

[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Supra* note 17, AIR 2010 SC 1974, (2010) 7 SCC 263
[81] *Id.*

right against self-incrimination as guaranteed by Article 20(3) of the Constitution, as well as their right to life and personal liberty protected under Article 21.[82]

The Court ruled that the protection against self-incrimination under Article 20(3) of the Constitution should be interpreted in conjunction with various aspects of personal liberty under Article 21, including the right to a fair trial and substantive due process. This protection extends to the accused, suspects, and witnesses, and is not limited to the courtroom but applies in any case that may lead to prosecution.[83]

vi. **Virendra Khanna v. State of Karnataka (2021*),*[84]** In the present case, the petitioner faced charges under the Narcotic Drugs and Psychotropic Substances Act (NDPS), 1985, and the Foreigners Act, 1946. The police seized the petitioner's mobile phone, laptop, and other items and requested the petitioner to provide the passwords for his electronic devices and email account. The petitioner refused to disclose the passwords. Subsequently, the police filed two applications before the trial court. The first application sought permission to conduct a polygraph test on the petitioner without his consent to determine the password. In the second application, the police requested an order to compel the petitioner to disclose the password. The trial court granted both applications. The petitioner challenged these orders before the High Court.[85]

The High Court ruled that the order permitting the administration of the polygraph test was overturned. However, the Court rejected the appeal against the order for passcode disclosure, stating that Article 20(3) of the Indian Constitution does not protect passcode disclosure as a right. The Court analyzed the distinction between testimonial and non-testimonial (physical) evidence to establish its reasoning.[86]

vii. **CBI v. Mahesh Kumar Sharma (2022),*[87]** Delhi Special CBI Court received an application requesting the disclosure of the passcode for a computer that had been confiscated from the accused. The prosecution relied on the Karnataka High Court's decision in *Virendra Khanna v. State of Karnataka*[88] as a supporting precedent. The

[82] *id.*
[83] *Id.*
[84] *Supra* note 22, 2021 SCC On Line Kar 5032,
[85] *Id.*
[86] *Id.*
[87] *Supra* note 23, 2022 SCC On Line Dist. Court (Del) 48, *decided on 29-10-2022.*
[88] *Supra* note 22.

opposition to the application argued that there is no specific provision for the disclosure of passcodes and that the trial court does not possess inherent authority to order the unlocking of phones or computers. It was argued that Article 20(3) prohibits the compelled extraction of passcodes since it would constitute testimonial evidence. Additionally, it was contended that the judgment in *Virendra Khanna v. State of Karnataka*[89] is per incuriam, or in error, in light of the *Selvi*[90] judgment.

The court held that compelling a witness to disclose a password or security pattern is a violation of Article 20(3) of the Indian Constitution. The court also deliberated on the distinction between testimonial and non-testimonial evidence in its ruling.[91]

The court also noted that the accused's password is not needed for comparison or identification purposes, making it protected personal information that resides within the individual's mental faculty. Therefore, requiring the disclosure of the passcode would violate Article 20(3). Referring to the ruling in the *Selvi case*,[92] the court further emphasized that procedures such as narcoanalysis or lie detector tests involve personal knowledge of the accused and cannot be conducted without their consent. Similarly, the disclosure of a passcode entails revealing personal knowledge, and thus an accused cannot be compelled to disclose it.[93]

viii. Commonwealth Of Pennsylvania V. Joseph J. Davis (2019):[94] the Supreme Court of Pennsylvania ruled that:

"...regarding the scope of the Fifth Amendment, we determine that requiring someone to provide a password to access a computer, which is considered an act of production, is considered testimonial. To put it simply, the act of revealing a computer password involves verbal communication rather than just a physical action that would not be considered testimonial. Unlike a handwriting sample, blood drawing, or voice exemplar, a password has no physical form. Since a password is something that is memorized, disclosing it

[89] *Id.*
[90] *Supra* Note 17.
[91] *Supra* note 23.
[92] *Supra* note 91.
[93] *Supra* note 88.
[94] *Commonwealth Of Pennsylvania V. Joseph J. Davis* No. 56 MAP 2018 Appeal from the Order of the Superior Court dated November 30, 2017, at No. 1243 MDA 2016, affirming the Order of the Court of Common Pleas of Luzerne County, Criminal Division, dated June 30, 2016, Nos. CP-40-CR291-2016 and CP-40-MD-11-2016, decided on Nov 20, 2019.

means revealing the contents of one's mind. A computer password is intentionally personalized and unique, serving the purpose of keeping the information within it confidential and protected from discovery."[95]

Further the court held that "In accordance with previous rulings of the United States Supreme Court, we conclude that the Commonwealth is essentially seeking the electronic equivalent of a combination to a wall safe - the passcode to unlock the appellant's computer. The Commonwealth is not seeking the password as an end in itself, but rather as a means to access the withheld files. Therefore, compelling the production of a computer password requires the appellant to recall the contents of their mind, and the act of production implies factual assertions that may be used against them. Hence, we affirm that compelling the appellant to reveal a computer password is considered testimonial in nature."[96]

The topic requires the formulation of new principles to respect the constitutional ban on self-incrimination while allowing impartial investigations. Since the Supreme Court couldn't establish self-incrimination standards for mobile phones in the 1960s, the *Kathi Kalu Oghad*[97] case cannot serve as a benchmark for passcode-related self-incrimination today.

The Supreme Court must consider self-incrimination and the right to privacy, as accessing an individual's mobile phone without limits may compromise privacy beyond the State's investigative interest. A timely resolution is crucial, balancing individual rights and the State's duty to investigate crimes.[98] The "foregone conclusion" doctrine in the US, an exception to the rule against self-incrimination, could be a valuable model for the Indian Supreme Court to develop a similar rule, striking a balance between individual rights and the State's investigative responsibilities.[99]

c) Legal Standards and Tests Applied by Indian Courts in Determining the Violation of the Right against Self-Incrimination

[95] *Id.*
[96] *Id.*
[97] *Supra* note 65.
[98] Bennett, Colin J., Rebecca A. Grant, and Colin John Bennett, eds. Visions of privacy: Policy choices for the digital age. *University of Toronto Press*, 6 (1999).
[99] Alito Jr, Samuel A, 'Documents and the Privilege Against Self-Incrimination' (1986) 48 U. Pitt. l. Rev. 27

Indian courts utilize specific legal standards and tests to determine whether the right against self-incrimination has been violated or not. These standards and tests help to assess the admissibility of evidence and the extent to which the right has been infringed. The following are standards and tests:

i. **Compulsion Test:** This test examines whether the accused has been compelled, either through coercive pressure, legal means or to provide incriminating evidence. Evidence of compulsion may indicate a violation of the right under Article 20(3).[100]

ii. **Testimonial Nature Test:** Indian courts differentiate between testimonial and non-testimonial evidence in many cases.[101] The testimonial nature test evaluates whether the compelled evidence relates to the accused's personal knowledge, communication, or mental faculty. If the evidence is deemed testimonial in nature, it falls under the protection of the right against self-incrimination.[102]

iii. **Voluntariness Test:** The voluntariness test assesses whether the accused has provided evidence with free consent, without coercion or inducement.[103] If evidence has been obtained involuntarily, undue influence or through improper means, it may be considered a violation of the right against self -incrimination.[104]

iv. **Balancing Test:** Indian courts employ a balancing test to weigh the interests of justice against the rights of the accused of self- incrimination. This test evaluates the necessity and proportionality of compelling evidence, considering factors such as the severity of the offense, the relevance of the evidence, and the impact on the fairness of the trial.[105]

v. **Physical Facts Test:** In cases involving compelled password disclosure, courts may consider the distinction between testimonial and non-testimonial evidence. The physical facts test determines whether the compelled evidence pertains to disclosing

[100] Behura, Aditi, and Ashray Behura, 'Voice Recordings and the Right against Self-Incrimination' (2021) 8 GNLU L. Rev. 392.
[101] Bhalotia, Kartikey Sanjeev, and Divyansh Pareek, 'Biometric encryption of smartphones: a charted ship in the ocean of adversarial system?' (2021) 29, no. 2 Int. J. l. and Inf. Tec. 154-168.
[102] Fox, Dov, 'The right to silence as protecting mental control' (2009) 42 Akron L. Rev. 763
[103] White, Welsh S, 'What is an involuntary confession now' (1997) 50 Rutgers L. Rev. 2001
[104] Barrio, Adrian J. 'Rethinking Schneckloth v. Bustamonte: Incorporating Obedience Theory into the Supreme Court's Conception of Voluntary Consent' (1997) U. Ill. L. Rev. 215
[105] Dolinko, David, 'Is there a rationale for the privilege against self-incrimination' (1985) 33 UCLA L. Rev. 1063

a "physical fact" rather than revealing the accused's personal knowledge or mental faculty.[106] If the evidence is deemed a physical fact, like biometric, finger print etc. it may not be protected by the right against self-incrimination.[107]

These legal standards and tests guide Indian courts in determining whether the right against self-incrimination has been violated or not. By applying these tests, courts seek to strike a balance between protection of individual rights and the fair administration of justice. It is important to note that the application of these standards may vary based on the facts & circumstances of each case, and the interpretation and application of the right against self-incrimination need to evolve through case law.[108]

BALANCING RIGHTS AND LAW ENFORCEMENT INTERESTS IN INDIA

In the context of compelled password disclosure and the right against self-incrimination, striking a balance between individual rights and interests of State is very important. Indian courts recognize the need to uphold the rights of individuals while ensuring effective law enforcement. Here are some key considerations in balancing these interests:

i. **Protection of Fundamental Rights:** Indian courts prioritize safeguarding fundamental rights, including the right against self-incrimination and the right to privacy. These rights are enshrined in the Constitution and serve as essential pillars of the Indian legal framework. Courts carefully assess the potential infringement on these rights when considering prosecution demands for compelled password disclosure.[109]

ii. **Public Interest and Safety:** The interests of the state, public safety, and the prevention of crime are prime considerations. Courts recognize that compelling password disclosure may be necessary in certain heinous cases to uncover evidence, investigate crimes, and ensure the security of the public. The gravity of the offense

[106] Engel, Joshua A, 'Rethinking the application of the fifth amendment to passwords and encryption in the age of cloud computing' (2011) 33 Whittier L. Rev. 543.
[107] *Id.*
[108] Kerr, Orin S. 'Compelled decryption and the privilege against self-incrimination' (2018) 97 Tex. L. Rev. 767
[109] Sripati, Vuayashri. 'Toward fifty years of constitutionalism and fundamental rights in India: Looking back to see ahead (1950-2000)' (1998) 14 Am. U. Int'l L. Rev. 413

and the potential harm to society are weighed against the accused's rights.[110]

iii. **Proportionality:** The rights of individuals with law enforcement interests requires a proportionate balancing approach.[111] Courts examine whether the requested compelled disclosure is proportionate to the nature and severity of the offense being investigated or not. Disproportionate or excessive demands for password disclosure may be deemed a violation of individual rights to privacy and liberty.[112]

iv. **Necessity and Alternatives:** Indian courts consider whether compelling password disclosure is extremely necessary and explore alternative methods of getting evidence. They assess whether other investigative methods or sources of evidence could reasonably achieve the same outcome without infringing upon the right against self-incrimination and right to privacy. The burden rests on the prosecution to demonstrate the requirement of compelled password disclosure.[113]

v. **Safeguards and Judicial Oversight:** To ensure a fair balance, the constitutional courts may issue some guidelines and exercise judicial oversight. This includes assessing the legality of requests for compelled password disclosure, scrutinizing the scope and purpose of such demands, and imposing conditions or limitations on their implementation. Judicial supervision helps prevent abuse of process and ensures compliance with constitutional rights in tune with right against self-incrimination.[114]

Balancing rights of accused and interest of state in India is a delicate task undertaken by the judiciary. By considering fundamental rights, public interest, proportionality, necessity, alternatives, and implementing safeguards, courts strive to maintain a harmonious equilibrium among the individual rights and interest of state.[115]

[110] Solove, Daniel J, 'A taxonomy of privacy' (2006) Uni. of Penns. l. rev., 477-564
[111] Arai-Takahashi, Yutaka. 'The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR' (2002) Intersentia NV
[112] *Id.*
[113] Marcella Jr, Albert, and Doug Menendez, *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes. (*Auerbach Publications, 2010)
[114] *Supra* note 22.
[115] Thomas, Tracy A, 'Proportionality and the Supreme Court's jurisprudence of remedies' (2007) 59 Hastings LJ 73

a) Arguments for compelling password disclosure in India

i. **Enhanced Investigation and Prosecution:** The compulsion to disclose passwords of a device can significantly improve the effectiveness of investigations and prosecutions in the digital realm.[116] Access to these devices, encrypted data, and online accounts can provide crucial information and evidence to prosecution that may give a lead for uncovering the truth and bringing offenders to justice.[117]

ii. **National Security and Public Safety:** Compelling password disclosure becomes essential in cases involving national security threats, sovereignty, or potential harm to public safety.[118] By gaining access to encrypted data and protected accounts, prosecution can identify and prevent activities related to terrorism, cybercrimes, and other serious offenses that may pose risks to the national security. Compelling passwords in such situations would serve the larger objective of safeguarding national security.[119]

iii. **Preservation of Evidence:** Password-protected devices and accounts may contain information & evidence that could be tampered with, deleted, or destroyed by the accused if left inaccessible.[120] Compelling password disclosure allows for the preservation of critical information before it is irretrievably lost. Timely access to passwords would prevent the destruction of evidence and ensure a fair and thorough investigation.[121]

iv. **Overcoming Technological Barriers:** The encryption technologies and robust security measures have created challenges for the state in accessing essential evidence.[122] Compelling password disclosure provides a legal backup to overcome these technological barriers and gain access to relevant information. Without the

[116] Kerr, Orin S, 'Searches and seizures in a digital world' (2005) Har. L. Rev. 531-585
[117] Carrier, Brian, and Eugene H. Spafford, *'Getting physical with the digital investigation process'* (2003) 2 Int. J. dig. evi. 21-20.
[118] Wachtel, Michael, 'Give me your password because congress can say so: An analysis of fifth amendment protection afforded individuals regarding compelled production of encrypted data and possible solutions to the problem of getting data from someone's mind' (2013)14 Pitt. J. Tech. L. & Pol'y 44
[119] Lewis, James A., Denise E. Zheng, and William A., *Carter. The effect of encryption on lawful access to communications and data* (Rowman & Littlefield, 2017)
[120] Gershowitz, Adam M, 'Password protected-can a password save your cell phone from a search incident to arrest' (2010) 96 Iowa L. Rev. 1125
[121] Boddington, Richard, *Practical digital forensics* (Packt Publishing Ltd, 2016)
[122] Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider, *IoT Privacy and security: Challenges and solutions* (Applied Sciences 10, 4102, 2020)

power to compel passwords, certain crimes may go unpunished due to the inherent difficulties in accessing encrypted data.[123]

v. **Balancing Individual Rights and Collective Interests:** While acknowledging the importance of the right against self-incrimination under Article 20(3), it is necessary to strike a balance with public interests, such as the need to investigate, prevent crimes and bring the culprit to the justice.[124] Compelling password disclosure in a controlled, judicious, and regulated manner ensures the protection of individual rights while upholding the interests of society and maintaining law and order in the country.[125]

It is important to consider the above points for compelling password disclosure in the light of constitutional provisions, legal framework, and principles of proportionality, necessity, and procedure established by law.[126] Courts play an important role in carefully balancing these arguments against individual rights and liberty and ensuring that any compelled password disclosure is justified in the eye of law, and respects constitutional right against self- incrimination and right to privacy.[127]

b) Arguments against compelled password disclosure based on the right against self-incrimination in India:

i. **Safeguarding Individual Rights:** Compelling individuals to disclose their passwords infringes upon their fundamental right as enshrined under the constitution. Forcing individuals to reveal the password which may be incriminating information undermines their right to remain silent.[128]

---

[123] *Id.*
[124] Stuntz, William J, 'Self-incrimination and Excuse' (1988) 88 Colum. L. Rev. 1227
[125] Dolinko, David, 'Is there a rationale for the privilege against self-incrimination' (1985) 33 UCLA L. Rev. 1063
[126] Moerel, Lokke, and Corien Prins, 'Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things'(2016) *Available at* SSRN *2784123*
[127] Fortini, Cristiana Maria Pinto E. Silva, and Mariana Magalhães Avelar, *Access to Information and Its Disclosure,* (THE Right of Access to Public Information: An International Comparative Legal Survey, 543-569, 2018)
[128] Lemus, Efren, 'When Fingerprints Are Key: Reinstating Privacy to the Privilege Against Self-Incrimination in Light of Fingerprint Encryption in Smartphones' (2017) 70 SMUL Rev. 533 *See also* Sarmah, Aditya, 'Privacy and the Right against Self-Incrimination: Theorising a Criminal Process in the Context of Personal Gadgets' (2016) 3 CALJ 28.

ii. **Upholding the Presumption of Innocence:** Compelled password disclosure is against the principle of "innocent until proven guilty." By demanding passwords, individuals are presumed to have committed an offence and compelled to assist in their own prosecution, undermining the very basic principle of presumption of innocence. This practice shifts the burden of proof onto the accused to prove their innocence and violates principles of fair trial.[129]

iii. **Respecting the Right to Privacy:** Compelled password disclosure is a violation of an individual's right to privacy, which is closely related with the right against self-incrimination. Passwords are employed to secure personal information and communications at the same time it does fall in the mental faculty of individuals.[130]

iv. **Potential for Abuse and Overreach:** Compelled password disclosure carries the risk of potential abuse by police authorities or investigating officer. Without proper guidelines, compelled passwords may be misused for purposes beyond the scope of the investigation including blackmailing etc., leading to unwarranted intrusion into an individual's private life and an infringement upon their right to privacy.[131]

v. **Technological Constraints and Ineffectiveness:** It is assumed that individuals possess control over all passwords to their digital devices or accounts. Whereas individuals may genuinely forget their passwords or may lack access due to some technical limitations. In such instances, compelling password disclosure becomes impractical and may result in adverse opinion about individuals or may be punished for their inability to comply with a demand which is beyond their control.[132]

It is very important to consider these arguments against compelled password disclosure within the constitutional rights framework, the presumption of innocence, and right to privacy. Striking an appropriate balance between law interest of state and the preservation of individual rights is vital to uphold a fair and

[129] Glynn, Findlay, *Access to Electronic Information: How the Requirements of Modern Day Criminal Investigation and Prosecution Have Unduly Limited Citizens'* (Criminal Procedure Rights, 2018)
[130] Goldman, Kara, 'Biometric passwords and the privilege against self-incrimination' (2015) 33 Cardozo Arts & Ent. LJ 211
[131] Iyengar, Prashant, 'IP Addresses and Expeditious Disclosure of Identity in India' (2013) 9 Indian JL & Tech. 45
[132] Bonneau, Joseph, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano, 'The quest to replace passwords: A framework for comparative evaluation of web authentication schemes' In *2012* IEEE symposium on security and privacy, pp. 553-567. IEEE

equitable trial procedure in India.[133]

c) Analysis of Indian court decisions and precedents in balancing rights and law enforcement interests

Courts in India have faced the complex task of finding a middle ground between individual rights, particularly the right against self-incrimination, and the interests of the state. We have very few instances which directly deal with compelled password discloser. Through a detailed court decision and precedent by the Supreme Court of India we may develop a framework for achieving this delicate balance.[134]

The following analysis examines significant court rulings and their impact on the equilibrium between individual rights and law enforcement interests in India.

i. **Justice K.S. Puttaswamy (Retd.) v. Union of India (2017):*[135]*** In this landmark judgement, the Supreme Court of India recognized the right to privacy as a fundamental right protected by the Constitution. The ruling highlighted the importance of individual privacy in the digital era and laid the precedent for dealing with the interplay between privacy rights and law enforcement concerns.[136]

ii. **Selvi v. State of Karnataka (2010):*[137]*** The Supreme Court of India in this judgement established safeguards for the admissibility of evidence obtained through compelled statements. It ruled that forced self-incriminating statements, including the disclosure of passwords hit by Article 20(3) of the constitution and, would be deemed inadmissible unless provided with free consent. This judgment emphasized the need to protect individual rights against self- incrimination and set boundaries on compelled disclosures.[138]

iii. **Shreya Singhal v. Union of India (2015):*[139]*** I n this case, the Supreme Court struck

[133] Dulay, Nicole Bernadette M, 'The Right to Speak in Code: A Balancing of State Interest and the Right to Encrypted Speech' (2019)2 U. Asia & Pacific LJ 131
[134] Brady, Scott, 'Keeping secrets: a constitutional examination of encryption regulation in the United States and India' (2012) 22 Ind. Int'l & Comp. L. Rev. 317
[135] *Supra* note 48, (2017) 10 SCC 1, AIR 2017 SC 4161.
[136] *Id.*
[137] *Supra* note 17.
[138] *Id.*
[139] Shreya Singhal v. Union of India**,** AIR *2015* SC 1523, [Writ Petition (Criminal) No. 167 of 2012]

down Section 66A of the Information Technology Act, 2000 which allowed for the arrest of individuals for posting "offensive" content online including social media. The court upheld the significance of freedom of speech and expression and established a precedent for balancing interests of state with constitutional rights.[140]

Overall, Indian courts including Supreme Court of India have shown a commitment to uphold individual rights while recognizing the importance of interests of state.[141] They have stressed the need for proportionality, guidelines, and consensual disclosures, ensuring that the balance between rights against self-incrimination and law enforcement remains intact.[142]

GUIDELINES FOR PROSECUTION AND COURTS IN INDIA ON HANDLING PASSWORD DISCLOSURE CASES:

When it comes to handling cases involving password disclosure, it is essential to establish clear guidelines for law enforcement agencies and courts by the Supreme Court or by Parliament. The following guidelines aim to ensure a balanced approach that respects privacy rights & rights against self- incrimination while enabling effective law enforcement:

a) Legal Procedures in tune with Article 21:

i. Law enforcement agencies should strictly adhere to the procedures outlined under Section 91, 92, 93, 94 and 100 of Cr.P.C. while seeking password disclosure.[143]

ii. Obtain proper authorization as mandated under Code of Criminal Procedure, 1973 such as search warrants or court orders, based on credible evidence and reasonable information received.[144]

iii. Respect the principles of procedure established by law, including providing notice to the affected individuals, allowing them an opportunity of being heard, and ensuring the

[140] *Id.*
[141] Cassels, Jamie, 'Judicial activism and public interest litigation in India: Attempting the impossible?' (1989) 37 The American J. Compr. l. 495-519
[142] *Supra* note 23.
[143] The Code of Criminal Procedure, 1973, s 91, 92, 93, 94 & 100.
[144] *Id.*

right to be represented by an advocate of his choice.[145]

b) Proportionality and Necessity:

i. Seek password discloser only in extremely necessary cases, considering the nature and severity of the offense.[146]

ii. Prioritize alternative investigative methods and exhaust all reasonable efforts for getting desired information before resorting to compelling password disclosure from an individual.[147]

iii. Avoid indiscriminate requests for password disclosure that may infringe on constitutional right to privacy without adequate justification.[148]

c) Preservation and Protection of Privacy:

i. Take appropriate steps to ensure the preservation and protection of individuals' right to privacy during the process of password disclosure.[149]

ii. Prevent unauthorized access, use, or disclosure of password-protected information.[150]

iii. Minimize the collection and retention of personal information including passwords to the extent necessary for the specific investigation only.[151]

d) Expertise and Training:

i. State should Provide specialized training and guidance to law enforcement

[145] The Constitution of India, 1950, Art 20, 21 & 22.
[146] Siponen, Mikko, Wael Soliman, and Anthony Vance, 'Common misunderstandings of deterrence theory in information systems research and future research directions' (2022) 53, 1 ACM SIGMIS Database: the DATABASE for Advances in Information Systems 25-60
[147] *Supra* note 95.
[148] Stratton, Sara E, 'Passwords Please: Rethinking the Constitutional Right to Informational Privacy in the Context of Social Media' (2013) 41 Hastings Const. LQ 649
[149] Sorensen, Shannon, 'Protecting children's right to privacy in the digital age: Parents as trustees of children's rights' (2016) 36 Child. Legal Rts. J.156
[150] Koushik, P., A. M. Chandrashekhar, and Jagadeesh Takkalakaki, 'Information security threats, awareness and cognizance' (2015) 2 IJTRE 9
[151] Krishnamurthy, Balachander, and Craig E. *Wills. Characterizing privacy in online social networks* (In Proceedings of the first workshop on Online social networks, 37-42, 2008)

agencies including police, forensic expert, and legal professionals on handling password disclosure cases.[152]

ii. Develop an expertise agency which effectively navigates the technical aspects and complexities of password-protected information in the court of law.[153]

e) Collaboration and Information Sharing:

i. Relevant agencies and departments involved in password disclosure cases may foster collaboration and information sharing among themselves.[154]

ii. Promote coordination between technology experts, law enforcement agencies, legal professionals, and to ensure effective handling of password related cases.[155]

f) Transparency and Accountability:

i. Keep accurate records of password disclosure requests, including the reasons, procedures to be followed, and outcomes.[156]

ii. Establish mechanisms for accountability and review of internal and external oversight to ensure law enforcement agencies are complying with the established guidelines.[157]

CONCLUSION

In conclusion, this research paper has explored the topic titled ***"Password as Evidence: Judicial Approach to Password Protection and Right Against Self- Incrimination in Digital World "*** with a specific focus on the Indian court's decision on balancing approach between

[152] Reyes, Anthony, Richard Brittson, Kevin O'Shea, and James Steele, *Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors* (Elsevier, 2011)
[153] Kanta, Aikaterini, Iwen Coisel, and Mark Scanlon, *A survey exploring OPEN-SOURCE Intelligence for smarter password cracking,* (Forensic Science International: Digital Investigation 35, 301075, 2020)
[154] Adams, Anne, Martina Angela Sasse, and Peter Lunt, *Making passwords secure and usable, In People and computers XII: proceedings of HCI'97*, (Springer London, 1-19, 1997)
[155] Hinduja, Sameer, 'Perceptions of local and state law enforcement concerning the role of computer crime investigative teams' (2004) 27, 3 Policing: An International Journal of Police Strategies & Management 341-357
[156] Salem, Maha, Gabriella Lakatos, Farshid Amirabdollahian, and Kerstin Dautenhahn, 'Would you trust a (faulty) robot? Effects of error, task type and personality on human-robot cooperation and trust' (2015) In Proceedings of the tenth annual ACM/IEEE international conference on human-robot interaction, 141-148
[157] Walker, Samuel, 'Police accountability' (2001) Belmont, CA: Wadsworth 199-214

rights of individual and interest of State. The study has provided an in-depth analysis of the challenges, significance, and implications of passwords as evidence with respect to the right against self-incrimination as guaranteed under article 20(3) of the Constitution of India, 1950.[158]

Passwords play a critical role in the digital realm as they are protection against gaining access to personal and sensitive information. They have become very crucial sources of evidence in criminal investigations, offering valuable information into individuals' online activities and accounts. However, compelling individuals to disclose their passwords raises issues concerning the right against self-incrimination, which is protected under Article 20(3) of the Indian Constitution.[159]

Throughout this research paper, the historical development, and legal foundations of the right against self-incrimination in India as well as of USA have been examined. The interpretation and application of this right by the Supreme Court of India, Karnataka High Court and Delhi District Court have been discussed, emphasizing the need to strike a delicate balance between privacy rights and interest of the state.[160]

The interpretation of different court rulings has been discussed in detail with a view to giving a clear picture of compelled password discloser. The arguments for and against compelled password disclosure in India have been evaluated with key highlights, considering the implications for privacy rights and law enforcement objectives.[161]

Moving forward, it is important to acknowledge the ongoing implications and challenges that passwords as evidence and the right against self-incrimination pose in the different Indian courts. Continuous evaluation and adaptation to technological advancements and evolving legal & constitutional frameworks will be necessary to strike an appropriate balance between privacy rights and prosecution by the state for compelled password discloser.[162]

The highest court in Pennsylvania has ruled that *"the compelled recollection of Appellant's*

[158] *Supra* note 4.
[159] *Id.*
[160] *Supra* note 64, 65, 69, 74, 75, 81, 85, 86 & 95.
[161] *Supra* note 118 to 134.
[162] Broucek, Vlastimil, *Forensic computing: exploring paradoxes: an investigation into challenges of digital evidence and implications for emerging responses to criminal, illegal and inappropriate on-line behaviours*, (PhD diss., University of Tasmania, 2009)

password is testimonial in nature, and, consequently, privileged under the Fifth Amendment to the United States Constitution."[163] Similarly different state's Supreme Courts of United States said compelling a password from a suspect is a violation of the Fifth Amendment, a constitutional protection that protects suspects from self-incrimination.[164]

Unlocking a phone through facial recognition or fingerprint scanning is not equivalent to disclosing a password verbally.[165] As the law develops, the grey area surrounding this issue will become more defined over the time. Currently, privacy remains compromised, and there is a violation of the right against self-incrimination.[166]

[163] *Supra* note 95.
[164] Rangaviz, David Rassoul, 'Compelled decryption & state constitutional protection against self-incrimination' (2020) 57 Am. Crim. L. Rev. 157
[165] Carnes, Brittany A*,* 'Face ID and Fingerprints: Modernizing Fifth Amendment Protections for Cell Phones' (2020) 66 Loy. L. Rev. 183
[166] DeCew, Judith Wagner, *In pursuit of privacy: Law, ethics, and the rise of technology* (Cornell University Press, 1997)