

THE K.K. LUTHRA MEMORIAL MOOT COURT, 2027

MOOT PROPOSITION

I. Background and the Parties

1. The Republic of Solenia is a federal parliamentary democracy in the common-law tradition; it tries criminal cases by judge and not by jury. Its capital, Mirena, is a Territory administered directly by the Federal Government directly. Sentinel Lab is a small not-for-profit digital newsroom in Mirena that specialises in data-driven investigative journalism focusing largely on illegal breaches of privacy and surveillance. It was founded in 2016 by Mr. Sam Liu, a reporter of long standing, and is funded by reader subscriptions, domestic donations, and two project grants from the Halden Media Trust, an overseas philanthropy that supports independent journalism across the region.
2. Between 2014 and 2023, the Government of Solenia built and expanded “CitiCore”, a national digital-identity and welfare-delivery platform that links the biometric, demographic and bank-account records of close to 300 million residents and is used to disburse pensions, rations and subsidies. CitiCore is administered by the Digital Governance Authority (“**the DGA**”), a statutory body, and was developed and maintained under a chain of contracts awarded to Meridian Systems Limited (“**Meridian**”), one of the country’s largest technology contractors.
3. From August 2024 onwards, Sentinel Lab published a four-part investigation titled “The Citizen for Sale”. The first three parts reported that successive CitiCore contracts had been renewed without competitive bidding and that billings by Meridian had been inflated by about forty per cent. Backed by screenshots of internal records, these reports published in three instalments were widely republished and circulated and provoked a significant public outcry against the Government, with questions raised in the press, social media along with mounting calls and public protests for an independent inquiry. The fourth and final part published in November 2024 went further: it revealed that a working extract of the live CitiCore database complete with names, addresses, biometric reference numbers and welfare-payment histories was available in the public domain, circulating and being accessed outside authorised channels, and it reproduced a redacted sample of that database. The DGA and Meridian denied every allegation and called the documents fabricated.

II. The Complaint and the Case

4. On 6 February 2025, the DGA lodged a written complaint with the Federal Investigation Agency (“**the Agency**”), the principal federal agency for investigating corruption, economic and

organised crime. The complaint claimed that a copy of the live CitiCore database had been unlawfully extracted and removed, that the breach had exposed the personal data of millions of residents of Solenia to unauthorised use and misuse, and that those responsible for custody of the data had accepted money for providing the data. It also enclosed that an internal audit was undertaken by the DGA after the reports appeared, recording that in October 2024, some weeks before publication of the fourth instalment, bulk export of data had been run from a data-centre workstation using the credentials of one Ms. Shauna Singha, a database administrator employed by Meridian at the primary CitiCore facility situated at Downtown Mirena.

5. On 12 February 2025, the Agency registered Case Information Report No. 17 of 2025 (“**the CIR**”) [**Annexure 1**] for offences under the Solenian Penal Code, 2023 [criminal breach of trust, dishonestly receiving stolen property and criminal conspiracy read with Sections 43, 66 and 70 of the Digital Information and Services Act, 2009 (unauthorised access to, and theft of data from, a protected computer resource)]. The CIR named Ms. Singha and “other unknown persons” as the perpetrators of the crime.
6. The investigation that followed proceeded on the theory that Ms. Singha had exported the database and sold it to Mr. Liu; that Mr. Liu had solicited and paid for the data, partly out of the Halden grant; and that the database had thereafter been passed on further. Mr. Liu maintains that he is a journalist who received documents from a confidential source in the public interest. He claimed journalistic privilege, and stated that he paid no one for the data received and published by Sentinel Lab; that he has never communicated with Ms. Singha, and that the CIR and investigation was a device to unmask his sources and to comb through years of his unrelated journalistic work.

III. The Search, the Seizure and the Arrest

7. Shortly before dawn on 2 April 2025, the Agency simultaneously searched Sentinel Lab’s office and Mr. Liu’s home. The search of the home was carried out without a warrant. The Investigating Officer, Assistant Director Gus Kazan, recorded in writing, before entering, his grounds for proceeding under Section 185 of the Solenian Criminal Procedure Code, 2023 (“**the Code**”) that the data sought was volatile and could be wiped if the search were delayed to obtain a warrant. Two residents of the neighbourhood were called to witness the search. The audio-video recording of the search required to be done during the search by the Code was made only in part: it began after the devices had already been gathered from the study, did not capture the search or the seizure of the devices, and was never forwarded to the jurisdictional Court.

8. From Mr. Liu's study, the Agency seized a mobile phone, a laptop computer and an external hard drive, each entered in a seizure memo [**Annexure 2**] drawn up at the spot and signed by the two witnesses. Nothing incriminating was found on his person. The mobile phone was locked by a swipe pattern; the laptop by a password and a fingerprint sensor; and the hard drive was encrypted. The Agency did not invoke Section 69 of the Digital Information and Services Act, the provision that allows a designated authority to direct a person to assist in decrypting information, and proceeded instead under its general powers of search and seizure.
9. Mr. Liu was arrested by the Agency that evening and produced the next day before the the Special Court (Economic Offences), Mirena. He was remanded to the Agency's custody for five days and thereafter to judicial custody. In its first remand application the Agency stated, on the strength of the internal audit, that "encrypted chats between the accused and Ms. Singha, and a data folder containing the October 2024 export on the accused's sealed laptop and external hard drive" were central to the case and needed to be accessed; and that the mobile phone, though of peripheral significance, would contain corroborative material.

IV. The Attempt to Access the Devices, and the Direction

10. The three devices were sent to the Agency's forensic unit. Its examiners tried to extract the contents using digital-forensic tools available to the Agency, but could not: Mr. Liu had hardened the devices with additional security (strong encryption, a non-standard lock, and a setting that would erase the data after a number of failed attempts) which the tools could not bypass. Without the pattern, the password and the decryption key, the devices could not be opened.
11. On 9 April 2025, the Agency applied to the Special Court for two orders: first, that Mr. Liu be directed to furnish the pattern, the password and the biometric required to unlock and decrypt the three devices, under Section 94 of the Code (production of documents and devices likely to contain digital evidence), Section 349 of the Code (specimen signatures, handwriting, finger impressions and voice samples), Section 5 of the Solenian (Identification) Act, 2022 and the inherent power of the court; and second, that the Agency be permitted to subject Mr. Liu to scientific investigative techniques, including narco-analysis, to aid the investigation [**Annexure 3**]. Mr. Liu opposed the first direction in writing [**Annexure 4**].
12. By a reasoned Order dated 28 April 2025 [**Annexure 5**], the Special Court (a) directed Mr. Liu to unlock and decrypt the devices; and (b) permitted the Agency to conduct narco-analysis of Mr. Liu, subject to his consent recorded before a Designated Magistrate and to the safeguards governing such tests under the Code. The Order recorded, as the foundation for both directions,

the Agency's assertion that the laptop and the external hard drive held the Singha chats and the October export.

13. On 5 May 2025, Mr. Liu declined to unlock or decrypt the devices, maintaining his objection. He consented, however, to the narco-analysis, and his consent was recorded before a Designated Magistrate [**Annexure 6**]. During the test, in a drug-induced and semi-conscious state, Mr. Liu described the pattern of the mobile phone and the password of the laptop, and disclosed the key that decrypted the hard drive. Using information given by Mr. Liu, the Agency unlocked and decrypted all three devices.

V. The Search of the Devices

14. Once unlocked, the devices were examined by the Agency's forensic unit through July-August 2025, which made complete bit-for-bit mirror images of all three but generated and recorded no hash value (so that the integrity of the images could not afterwards be verified); and retained both the originals and the images. The internal authorisation under which the forensic search was carried out described its purpose in a single line: "to examine the seized devices for material relevant to the CIR" [**Annexure 7**].
15. The examination did not bear out the Agency's stated grounds. No communication of any kind between Mr. Liu and Ms. Singha was found on any of the three devices; and neither the laptop nor the external hard drive held any data folder or any copy of the CitiCore data. The laptop held drafts of unpublished articles, Sentinel Lab's correspondence with lawyers, and Mr. Liu's personal and financial records; the external hard drive, for which the Agency had pressed hardest, held nothing but Mr. Liu's archive of source material for unrelated stories.

What the examination did recover lay on the mobile phone, the device the Agency had described as peripheral. It recovered a set of messages exchanged between Mr. Liu and Ms. Amy Budan (a privacy activist residing outside of Solenia and former colleague of Ms. Singha at a previous job), a person not named in the CIR. In the messages exchanged in July 2024, Mr. Liu asked for "the full dump", talked of settling a figure and confirmed a payment. The examination also recovered a folder holding a copy of the entire CitiCore database — its contents genuine and current, but its file metadata showing that it had been generated on 12 September 2024, some weeks before the October 2024 export recorded in the internal audit, and from a facility other than the primary CitiCore facility in Downtown Mirena. Among the messages was a link to a cloud-storage account. Using a login the Agency found stored on the unlocked mobile phone, and without any

separate warrant, officers signed into that account and downloaded a second, complete copy of the database.

The Agency's supplementary note records that the internal audit's finding of an October 2024 export on Ms. Singha's credentials stands; that no export of any kind has been traced to September 2024; and that the CIR names "other unknown persons" besides Ms. Singha.

16. The same examination ranged across each of the three devices. The Agency's report and the investigation book (maintained by investigators) listed, catalogued and in places reproduced Mr. Liu's correspondence with some forty confidential sources relating to unrelated stories; his privileged exchanges with Sentinel Lab's lawyers about this very investigation; drafts of unpublished articles; his medical records and family photographs; and his banking and tax files. None of this was screened out before examination, none was placed before any independent authority, and none has been returned or deleted — the mirror images remain in the Agency's hands. The catalogued material came overwhelmingly from the laptop and the external hard drive, the two devices which held nothing relevant to the CIR at all. Within weeks, the name of one of Mr. Liu's sources, a hospital employee with no connection to CitiCore, surfaced in a rival outlet. This source was subsequently prosecuted on charges (unrelated to the present prosecution) which Mr. Liu asserts are fabricated, and is currently on trial.

VI. The Charge and the Impugned Order

17. The Agency filed its final report in September 2025. At the hearing of arguments on indictment before the Special Court, the prosecution relied on the recovered messages, both copies of the database and the cloud-account material. Mr. Liu contended that this material, being the fruit of an unlawful compulsion to unlock his devices and of an unconstitutional, unparticularised and procedurally defective search, could not be looked into even for the purpose of framing the indictment, and that, leaving it out of account, no criminality was made out against him.
18. By Order dated 16 January 2026, the Special Court rejected the contention and formally indicted Mr. Liu for offences under the Penal Code and the Digital Information and Services Act [Annexure 8].

VII. The Proceedings before the High Court

19. Mr. Liu moved the High Court of Mirena under Articles 226 and 227 of the Constitution by Writ Petition (Criminal) No. 88 of 2026. He challenges the Order of 28 April 2025 directing him to unlock the devices and permitting the narco-analysis; the use against him of the material obtained

as a result of disclosure of the pattern, password and decryption key obtained during the narco-analysis; the search and indefinite retention of the data; and the Order of 16 January 2026 framing charges. He seeks a declaration that the direction to unlock, the use of the narco-analysis material, and the search violated Articles 20(3), 21, 19(1)(a) and 14; the quashing of the indictment; the return and destruction of the mirror images and of all irrelevant and privileged material; a direction that the impugned material not be used against him.

- 20.** The Republic of Solenia and the Agency resist the Petition. They contend that the accused consented to the narco-analysis before a the Designated Magistrate; that what a person reveals in a voluntary test may be acted upon and any fact thereby discovered proved; that the search and seizure conformed to the Code; that reasons to believe have to be judged on the material available at the time of their formation and not by what the search ultimately yielded, the audit having afforded the basis; that the devices were in any event lawfully seized under a validly registered CIR which named “other unknown persons”; and that the September extract and the Budan material therefore fall within its compass; that at the stage of indictment the court looks to see if the allegations are with basis or not .
- 21.** The High Court has admitted the petition and listed it for final hearing on the questions set out below.

QUESTIONS FOR DETERMINATION

- A.** Whether an accused can be compelled, by an order of a Court or by a direction of an investigating agency, to furnish the password, passcode, pattern or biometric to unlock a seized digital device?
- B.** Whether the pattern, password and decryption disclosed by an accused during narco-analysis, even if administered with consent, are protected by Articles 20(3) and 21 of the Federal Constitution and if so, are liable to be excluded from use against him in any investigation or legal proceeding; and whether the results of narco-analysis are admissible in evidence, or are no more than an aid to investigation, at common law?
- C.** Whether search and seizure of the devices, and the subsequent examination, copying, retention and use of their contents, were lawful regard being had to:
- i.** the sufficiency of the grounds recorded under Section 185 of the Code;
 - ii.** the recovery of material which did not correspond to that stated in the reasons to believe;
 - iii.** the audio-video record that was made only in part and never forwarded to the jurisdictional Court;

- iv. the absence of any hash value or comparable safeguard for the integrity of the mirror images;
 - v. the download, without a fresh warrant, of a further copy of the database from a cloud account using stored credentials; and,
 - vi. the unscreened examination and indefinite retention of privileged and manifestly irrelevant material, including the accused's confidential journalistic sources, his communications with counsel, and his personal records?
- D.** If the search and seizure were to be found to be unlawful in any of these respects, what would be the consequence for the material so obtained?
- E.** Whether the material obtained or derived from the narco-analysis and the search of the devices, including the data accessed by means of the credentials disclosed under the narco-analysis, can be relied upon to frame indictment against the accused, and whether, at the stage of indictment, the Court is required to address the admissibility and the tainted character of such material?

THE K.K. LUTHRA MEMORIAL MOOT COURT, 2027

NOTES FOR COUNSEL AND ANNEXURES

NOTES FOR COUNSEL

1. The Constitution of Solenia is *pari materia* with the Constitution of India; in particular, Articles 14, 19, 20, 21, 226 and 227 bear the same numbering and content. The Solenian Penal Code, 2023, the Solenian Criminal Procedure Code, 2023, and the Solenian Evidence Act, 2023, are *pari materia* with the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023, respectively. The Solenian (Identification) Act, 2022 is *pari materia* with the Criminal Procedure (Identification) Act, 2022, and the Digital Information and Services Act, 2009 is *pari materia* with the Information Technology Act, 2000.
2. Counsel may rely, as persuasive authority, on the jurisprudence of any common-law jurisdiction, and on the decisions of international and regional courts and tribunals.
3. Counsel for the Petitioner will argue Writ Petition (Criminal) No. 88 of 2026 (Mr. Sam Liu). Counsel for the Respondents will argue for the Union of Solenia and the Federal Investigation Agency.
4. The record is closed. Teams may raise any ground of law arising from the stated facts, including grounds not expressly pleaded, but may not introduce facts that are not borne out by the record. Where a fact is disputed on the record each side may rely on its own version.
5. It may be assumed that — (a) the offences under investigation are punishable with imprisonment of seven years or more; that the three devices belong to Mr. Liu; (b) the narco-analysis was administered with the accused's consent recorded before a Magistrate and in accordance with the applicable guidelines. What legal effect flows from that consent is a matter for argument; (c) electronic data is capable of being 'property' and 'stolen property' under the Penal Code; (d) the maintainability of the Writ Petition is not in issue; and, (e) the constitutional validity of the Solenian (Identification) Act, 2022 and of the Digital Information and Services Act, 2009 is not in issue, and counsel need not address it.
6. The courts referred to in this Proposition are to be understood as follows — the “Special Court (Economic Offences)” is a Court of Sessions presided over by a Special Judge, designated to try the economic offences in question; it exercises the powers of a Court of Sessions and, for the purposes of the pre-trial orders in this Proposition, the powers of a Magistrate. A “Designated Magistrate” is a Judicial Magistrate nominated to record the consent to, and to oversee the

safeguards attending, a narco-analysis. In descending order, the hierarchy is: the High Court of Mirena; the Special Court (Economic Offences), being a Court of Sessions; and the Court of Judicial Magistrate. Nothing turns on the nomenclature, which follows the corresponding Indian scheme.

7. Nothing in this Proposition is based on any real person, entity, agency or event. Any resemblance is purely coincidental.

ANNEXURE 1

Case Information Report

Gist of information: On the complaint of the Digital Governance Authority it is alleged that a working extract of the live CitiCore resident database (personal, biometric and welfare-payment data of approximately 300 million residents) was unlawfully exported and removed from the CitiCore data centre. An internal audit discloses that on or about 14 October 2024 a bulk export was executed from Workstation DC-7 using the credentials of the accused Singha. It is alleged that the accused, in conspiracy with persons presently unknown, dishonestly extracted the said data and parted with it for monetary consideration, thereby causing wrongful loss to the Authority and wrongful gain to themselves. An offence investigable without a Court order is made out.¹ Registered and taken up for investigation.

Investigation entrusted to: G. Kazan, Assistant Director (sd/-).

¹ An offence “investigable without a Court order” is one which the Agency is empowered to investigate on its own authority, without the prior order of a Court, and in respect of which an officer may arrest without warrant.

ANNEXURE 2**Search-cum-Seizure Memo**

Authority to search: This search is undertaken without a warrant. The grounds for proceeding under Section 185 of the Code have been reduced to writing prior to the search and are placed on the case file, namely that:

- i. the digital material sought is volatile and liable to be destroyed or remotely wiped if the search is postponed to obtain a warrant;
- ii. the laptop and the external hard drive hold chats between Mr. Liu and Ms. Singha, as also the October data export;
- iii. the mobile phone, though of peripheral significance, may contain corroborative material which would aid the investigation.

Note: The audio-video recording of the proceedings was made on the mobile telephone of HC Patel. It commenced at 06:18 hrs, after the devices had been collected from the study, and does not capture the search or the seizure of the devices.

Articles seized:

Item	Description	Lock / condition
1	One mobile telephone (black), recovered from the study desk	Locked by swipe pattern
2	One laptop computer (silver), recovered from the study desk	Password-protected; fingerprint sensor enabled
3	One external hard drive (grey), recovered from the desk drawer	Encrypted

The above articles were sealed in the presence of the witnesses. Hash values to be generated on forensic imaging at the laboratory. No incriminating article was recovered from the person of Mr. Liu.

Signatures: Witnesses (sd/-); Asst. Director G. Kazan (sd/-); S. Liu — declined to sign, copy received.

ANNEXURE 3

Application by the Agency for a Direction to Unlock and for a Narco-Analysis (extract)

In the Special Court (Economic Offences), Mirena

Federal Investigation Agency v. Shauna Singha & Anr. — arising from CIR No. 17 of 2025

Application dated 9 April 2025 under Sections 94 and 349 of the Code, Section 5 of the Solenian (Identification) Act, 2022 and the inherent powers of this Court, seeking a direction to the accused Sam Liu to unlock and decrypt the seized devices, and permission to subject him to a narco-analysis.

Grounds (in brief):

- (a) The mobile telephone, laptop and hard drive seized on 2 April 2025 are admittedly the property of the accused Liu and are believed to contain the communications and the data folder central to the investigation.
- (b) The Agency's forensic unit has been unable to open the devices with the digital-forensic tools available to it, the accused having secured them with encryption and a data-wipe protocol. The pattern, password and key are known only to the accused, and the investigation is brought to a standstill.
- (c) Furnishing a pattern, password or fingerprint is a purely mechanical, identificatory act, analogous to giving a specimen signature, thumb impression or voice sample, and conveys no statement of guilt. It does not attract Article 20(3).
- (d) In the alternative, a narco-analysis conducted with the accused's consent is a recognised, legitimate aid to investigation, and any fact discovered in consequence of what the accused states may be proved in accordance with law.

Prayer: The accused Liu be directed to furnish the pattern, password and biometric necessary to unlock and decrypt the three devices; and that the Agency be permitted to subject the accused to narco-analysis, subject to his consent and to the applicable guidelines.

ANNEXURE 4

Reply and Objections of the Accused Sam Liu (extract)

Reply dated 22 April 2025. The accused opposes the application on the following grounds:

- (a)** A pattern or password exists only in the accused's mind. To compel him to disclose it is to compel testimony from his own mind, squarely within the protection of Article 20(3); it is not the giving of a physical specimen.
- (b)** Compelling the accused's fingerprint to unlock the same device is, in substance and effect, no different: it is used not for identification or comparison, but to open the entire archive of his life and work, and is therefore equally testimonial.
- (c)** No statute confers the power sought. Section 349 of the Code lists specimen signatures, handwriting, finger impressions and voice samples — not passwords. Section 94 cannot be directed against an accused. The Solenian (Identification) Act, 2022 permits the taking of "measurements", which do not include passwords.
- (d)** The devices contain the unpublished work and the confidential source communications of a working journalist, protected by Article 19(1)(a), and his most private personal data, protected by Article 21. Compelled access would have a chilling effect on a free press.

The accused adds that, while he objects to being compelled to unlock the devices, he does not object to undergoing a narco-analysis of his own volition.

ANNEXURE 5**Order of the Special Judge dated 28 April 2025 (extract)**

“... Heard. The short question is whether the accused can be directed to unlock the seized devices. In my view he can. A password or a swipe pattern is, in principle, no different from a specimen signature, a thumb impression or a voice sample — it is a key that opens a device, not a statement admitting guilt. Furnishing such a key is not ‘being a witness’ within Article 20(3). The same applies, a fortiori, to a fingerprint, which is a physical characteristic the investigating agency may in any event lawfully take.

The devices are admittedly those of the accused. The existence, ownership and possession of the devices being beyond dispute, the act of unlocking adds nothing to the prosecution’s knowledge and is a foregone conclusion. The privacy of a person under investigation is not absolute; it must yield to the compelling public interest in investigating a breach of the personal data of millions of citizens, especially in light of the assertion of the Agency that the laptop and external hard drive hold chats between accused persons Mr. Liu and Ms. Singha as well as an export of the CitiCore database taken during October 2024.

The application is allowed. The accused Liu shall furnish the pattern, password and biometric necessary to unlock and decrypt the three devices. The Agency is further permitted to conduct a narco-analysis of the accused, subject to his consent recorded before a Magistrate and to the applicable guidelines, a voluntary test being a legitimate aid to investigation. Ordered accordingly.”

ANNEXURE 6

Narco-Analysis — Consent and Proceedings Memo dated 5 May 2025 (extract)

The accused Sam Liu, having declined to unlock or decrypt the seized devices notwithstanding the Order dated 28 April 2025, appeared and stated that he was willing to undergo a narco-analysis. His consent was recorded before the Magistrate; he was informed of the nature and consequences of the test. He was afforded access to counsel.

The narco-analysis was conducted at the Federal Forensic Science Laboratory under sedation. In the course of the test, in a semi-conscious state, the accused uttered the swipe pattern of the telephone and the password of the laptop, and stated the key to the encrypted hard drive. The proceedings were video-recorded. On the strength of what the accused had said, the Investigating Officer thereafter unlocked and decrypted the three devices.

G. Kazan, Assistant Director, Investigating Officer (sd/-).

ANNEXURE 7

Digital Evidence Examination Report dated 21 August 2025 (extract)

Imaging: Complete bit-for-bit mirror images were created of all three devices. No hash value was generated or recorded at the time of imaging; the integrity of the images cannot, therefore, be independently verified. Originals and images are retained by the Unit.

Scope of examination: Pursuant to an internal authorisation ‘to examine the seized devices for material relevant to the case’, the entire contents of each device were examined. The categories of data extracted and catalogued in the report and case diary are tabulated below.

Category of data extracted	Relevance to CIR No. 17/2025
Messages with A. Budan (Oct–Dec 2024) from S Liu’s phone; folder ‘CC-dump’ containing a copy of the CitiCore database	Relied upon
Cloud-storage link in the messages; second full copy of the database downloaded from the linked account using stored credentials	Relied upon
Correspondence with ~40 confidential sources on unrelated stories from S Liu’s laptop	Not connected to the case
Emails with Sentinel Lab’s lawyers concerning this investigation from S Liu’s laptop	Privileged; not connected to the offence
Drafts of unpublished articles; medical records; family photographs; banking and tax files from S Liu’s laptop	Not connected to the case
Source material for other stories from S Liu’s external hard drive	Not connected to the case

Note: No material was segregated prior to examination, and no independent examiner was associated. The mirror images, including the categories shown as not connected to the case, remain with the Unit.

ANNEXURE 8**Order of the Special Judge dated 16 January 2026 on Charge (extract)**

“... The accused contends that the messages, the database and the cloud material, being the fruit of the narco-analysis and of an unlawful and procedurally defective search, cannot be looked into even at this stage, and that without them no charge can be framed. I am unable to agree. At the stage of charge the Court has only to see whether the material on record discloses a prima facie case and grave suspicion against the accused, presuming that material to be true; it is not the stage to test the admissibility of evidence or the manner of its collection, which are matters for the trial. The accused having consented to the narco-analysis, the facts discovered in consequence of what he stated appear, prima facie, capable of being proved. In any event, the test of admissibility is the relevance of the material, not the mode of its collection, and our Courts have not adopted the doctrine of the fruit of the poisonous tree; the alleged lapses in the audio-video recording and in the noting of the hash value, if established, go to the weight of the evidence at trial. On the material placed by the prosecution — supported by the audit of the bulk export from Ms. Singha’s workstation — a prima facie case is disclosed. Charges shall be framed against the accused accordingly.”
