TC 08

4TH SURANA AND SURANA AND CUSAT SCHOOL OF LEGAL STUDIES

DR. A T MARKOSE MEMORIAL TECHNOLOGY LAW MOOT COURT COMPETITION, 2024

BEFORE

THE HON'BLE SUPREME COURT OF INDICA

—— IN THE MATTER BETWEEN ——

WRIT PETITION (CIVIL) NO. _____ OF 2024

C.G. CAR COMPANY AND OTHERS …**PETITIONERS**

V.

UNION OF INDIA ….**RESPONDENT**

CLUBBED WITH

SUO MOTU TRANSFER PETITION NO. _____ OF 2024

MR. IAN ….**PETITIONER**

V.

STATE OF ANTARTAKA …**RESPONDENT**

ON SUBMISSION TO THE HON'BLE SUPREME COURT OF INDICA

(UNDER ARTICLE 32 AND 139A OF THE CONSTITUTION OF INDICA)

MEMORANDUM ON BEHALF OF RESPONDENT

—— DRAWN AND FILED ON BEHALF OF RESPONDENT ——

TABLE OF CONTENTS

INDEX OF AUTHORITIES

I. CASES:

1. State of Bombay v. Kathi Kalu Oghad, 1961 SCC OnLine SC 74.

2. Selvi v. State of Karnataka, (2010) 7 SCC 263.

3. State v. Diamond 905 N.W.2d 870 (Minn. 2018).

4. Virendra Khanna v. State of Karnataka, (2021) SCC OnLine Kar 5032.

5. State of U.P. v. Sunil, (2017) 14 SCC 516.

6. Ritesh Sinha v. State of UP, (2019) 8 SCC 1.

7. A.K. Gopalan v. State of Madras, (1950) SCC 228.

8. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

9. Gobind v. State of MP, (1975) 2 SCC 148.

10. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 30.

11. Vinit Kumar v. CBI, 2019 SCC OnLine Bom 3155.

12. Bharat Shantilal Shah v. State of Maharashtra, 2003 SCC OnLine Bom 1361.

13. National Human Rights Commission v. State of Arunachal Pradesh, (1996) 1 SCC 742.

14. Om Kumar v. Union of India, (2001) 2 SCC 386.

15. State of M.P. v. Laxmi Narayan, 2017 SCC OnLine SC 1799.

16. Gaurav Kumar Bansal v. Union of India, (2015) 2 SCC 130.

17. Swaraj Abhiyan v. Union of India, (2016) 7 SCC 498.

18. Pt. Parmanand Katara v. Union of India, AIR 1989 SC 2039.

19. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

20. Mahender Chawla and Others v. Union of. India, (2019) 14 SCC 615.

21. Bharat Shantilal Shah v. State of Maharashtra, 2003 SCC OnLine Bom 1361

22. Kerala State Beverages (M&M) Corp. Ltd. v. PP Suresh, (2019) 9 SCC 710

23. Internet Freedom Foundation v. Union of India, WP(C) No. 44/2019.

24. National Human Rights Commission v. State of Arunachal Pradesh, (1996) 1 SCC 742.

25. Indian Express Newspapers v. Union of India, (1985) 1 SCC 641.

26. Praveen Arimbrathodiyil v. Union of India, WP(C) 9647/2021.

27. Shrillekha Vidyarthi v. State of UP, AIR 1991 SC 537.

28. Ranjit Thakur v. Union of India, (1987) 4 SCC 611.

29. Sandeep Subhash Parate v. State of Maharastra (2006) 1 SCC 50.

30. Coimbatore Distt. Central Co-operative Bank v. Employees Association, (2007) 4 SCC 669.

31. Chintaman Rao v. State of MP, AIR 1951 SC 118; VG Row v. State of Madras, AIR 1952 SC 196.

32. State of MP v. Laxmi Narayan, 2017 SCC OnLine SC 1799.

33. Directorate of Film Festivals v. Gaurav Ashwin Jain, 2007 (4) SCC 737.

34. Anuj Garg v. Hotels Association of India, (2008) 3 SCC 1, 19.

35. Sahara India Real Estate Corporation Ltd v. SEBI, (2012) 10 SCC 603

36. PP Enterprises v. Union of India, AIR 1982 SC 1016.

37. MRF Ltd v. Inspector Kerala Government, (1998) 8 SCC 227.

38. Binoy Viswam v. Union of India, (2017) 7 SCC 59.

39. Gaurav Kumar Bansal v. Union of India, (2015) 2 SCC 130.

40. Swaraj Abhiyan v. Union of India, (2016) 7 SCC 498.

41. Joseph Shine v. Union of India, (2019) 3 SCC 3

42. Umesh Kumar v. State of Andhra Pradesh, (2013) 10 SCC 591

43. Dnyaneshwar v. State of Maharashtra, (2019) SCC Online Bom 4949.

44. Bachan Singh v. State of Punjab, AIR 1980 SC 89.

45. Summer v. Shuman, 55 US Law Week 4931 (1987).

46. Mithu v. State, AIR 1983 SC 473.

II. STATUTES:

1. The Constitution of Indica, 1950.

2. The Indican Penal Code, 1860.

3. The Information Technology Act, 2000.

4. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

5. The Central Goods and Services Act, 2017.

6. The Consumer Protection Act, 2019.

7. The Indican Telegraphs Act, 1885.

8. The Credit Information Companies Regulation Act, 2005.

III. BOOKS:

1. Ruma Pal, ‘Indian Constitutional Law’ (2010).

2. Bhimrao Ramji Ambedkar, ‘The Constitution of India’ (2019).

3. Granville Austin, ‘The Indian Constitution’ (1966).

4. Shikher Deep Aggarwal & Kush Kalra, ‘Commentary on the Information Technology Act’.

IV. <u>LEGAL DATABASES:</u>

1. www.scconline.com

2. www.manupatra.com

3. www.lexisnexis.com

STATEMENT OF JURISDICTION

The Respondent submits to the inherent jurisdiction of the Hon'ble Supreme Court of Indica arising by virtue of Article 32 along with 139A of the Constitution of Indica to hear and adjudicate over the present Writ Petition clubbed with the Suo Motu Transfer Petition in the case of ***C.G. Car Company and others v. UOI***.

The present memorial puts forth the facts, arguments, and laws in the present case.

STATEMENT OF FACTS

BACKGROUND

- **Location and Demographics**: The Republic of Indica, a democratic country in Southern Asia, is the world's most populous democracy, characterized by its pluralistic, multilingual, and multi-ethnic society.
- **Legislative Developments**: Indica enacted the Information Technology Act in 2000, amended in 2008, and introduced the National Information and Technology Policy in 2015, reflecting its commitment to regulating technological advancements.
- **State of Antartaka**: A leading state in Indica, particularly noted for its IT sector in Singaluru, which is likened to the Silicon Valley of Indica.

INCIDENT AND INVESTIGATION

- **Discovery of a Crime Scene**: On August 13, 2022, a family traveling to Sundarpur National Park discovered a body next to a Trudi car on State Highway No. 106. The victim was identified as Mr. Anand, a Vice President at MATT Private Limited.
- **Preliminary Findings**: Anand's death was suspected to be a homicide with a bullet wound to the head. No forceful entry was detected in or around his car. Simultaneous to the incident, Indica enforced rules under the IT Act, mandating approval and key sharing for cryptographic tools usage.
- **Primary Suspect**: Mr. Ian, an individual who frequented the same café as Anand and drove through the incident area at an unusual time, became the primary suspect. Ian's car, equipped with blockchain and encrypted data, became a focus for potential evidence.

LEGAL PROCEEDINGS

- **High Court**: Mr. Ian's legal challenge in the High Court of Antartaka addressed the alleged infringement of privacy and self-incrimination rights under the Constitution of Indica.
- **Supreme Court**: The Supreme Court consolidated Ian's case with a writ petition by CG Car Company, questioning the constitutional validity of mandatory cryptographic key sharing under the IT Act.

STATEMENT OF ISSUES

I. Whether Section 69 of the Information Technology Act, 2000 is constitutionally valid?

II. Whether governmental control over the use of cryptographic techniques is too restrictive in nature?

SUMMARY OF ARGUMENTS

Issue I: Whether the Section 69 of the Information Technology Act, 2000 is constitutionally valid?

The counsel for the Respondent argues the validity of Section 69 of the Information Technology Act, 2000 and addresses specific sub-issues. *Firstly*, it is contended that Section 69 does not violate the right against self-incrimination, as the act of providing an encryption key is deemed non-testimonial and falls outside the scope of compelled testimony. *Secondly*, it is asserted that Section 69 includes reasonable safeguards, citing provisions in the Information Technology Rules of 2009 that ensure proper oversight and data protection. *Thirdly*, the counsel contends that Section 69 does not impose unreasonable restrictions under Article 19, aligning with permissible limitations for national security and public order outlined in Article 19(2). Lastly, the argument emphasizes the crucial role of Section 69 in national security, drawing parallels with legal precedents related to surveillance, especially in cases involving serious offenses like murder. The counsel asserts that the surveillance is justified and necessary in the context of the ongoing murder investigation.

Issue II: Whether governmental control over the use of cryptographic techniques is too restrictive in nature?

The Respondent’s Counsel argues that the government’s control over cryptographic techniques, specifically compelled decryption for Mr. Ian, is justified within constitutional and legal frameworks. Stressing the state’s obligation to maintain public order and national security, the Counsel asserts the necessity of decryption for crime prevention. The Doctrine of Proportionality is invoked to justify government actions, ensuring a balance between individual rights and collective security. Emphasizing the government’s duty to fulfil constitutional obligations and protect citizens, the argument considers the negative and affirmative duties involved. References to legal principles and cases, including Maneka Gandhi, Article 19(6), and the Doctrine of Proportionality, support the legitimacy of decryption powers. The Counsel contends that the measures taken by the Investigation Authority are proportionate, safeguarding public safety and facilitating effective crime investigation. The overall stance advocates for a balanced approach that respects individual rights while addressing broader concerns of public safety and security within the framework of Section 69 of the IT Act, 2000.

ARGUMENTS ADVANCED

ISSUE I: WHETHER SECTION 69 OF THE INFORMATION TECHNOLOGY ACT IS CONSTITUTIONALLY VALID?

¶ 1. The counsel respectfully asserts validity of Section 69 of the IT Act,[1] confidently affirming that its legal standing will be substantiated through: [**1.1]** *Section 69 of the IT Act*[2] *does not violate Petitioner's fundamental right against Self Incrimination,*[3] **[1.2]** *Section 69*[4] *consist of safeguards that render it constitutional* **[1.3]** *Article 19 of Indican Constitution*[5] *provides for certain reasonable restrictions and Section 69*[6] *does not impose any unreasonable restriction and it is an essential legislation.*

1.1. Right against self-incrimination and privacy concerns of Mr. Ian.

¶ 2. The right against self-incrimination was essentially laid down to ensure that "No person accused of any offence shall be compelled to be a witness against himself."[7] Further, cases such as ***Selvi v. State of Karnataka***[8] elaborated on the same.

1.1.1 The Act of giving an encryption key is not testimonial in nature:

¶ 3. The counsel humbly submits that self-incrimination does not include the mechanical process of acquiring documents or evidence. In ***State of Bombay v. Kathi Kalu Oghad***,[9] SC held that Article 20(3)[10] is designed to protect individuals from self-incrimination. In this context, Self Incrimination refers to conveying information based on personal knowledge that could implicate oneself. This means that when personal knowledge is involved of the person only then Right against Incrimination is applicable as it constitutes testimony. It does not extend to the mere act of presenting documents in court that might shed light on the case without the accused making a personal statement based on their own knowledge.[11]

¶ 4. This means that in the present case the information that the investigation authority sought to retrieve from the Petitioners did not involve personal information, i.e., the private key for

[1] Information Technology Act 2000, s 69.
[2] ibid.
[3] Constitution of Indica, art 20(3).
[4] ibid.
[5] Constitution of Indica, art 19.
[6] Information Technology Act 2000, s 69.
[7] Constitution of Indica, art 20(3).
[8] Selvi v. State of Karnataka, (2010) 7 SCC 263.
[9] State of Bombay v. Kathi Kalu Oghad, 1961 SCC Online SC 74.
[10] Constitution of Indica, art 20(3).
[11] State of Bombay v. Kathi Kalu Oghad, 1961 SCC Online SC 74.

decryption.[12] The information is only to allow the investigation agency to conduct their investigation. The counsel further submits that the Right against self-incrimination, in both the jurisdictions Indica as well as the U.S., means to be protected only against self-incriminating "testimonial evidence" and not against "non-testimonial evidence." In the present scenario, the Petitioners were asked to produce "non-testimonial evidences".

¶ 5. Drawing from ***Kathi Kalu case***,[13] the Court observed that as the Petitioners are not responding to any questions that might implicate them in a crime, a request for a password, passcode, or biometric would not constitute testimonial compulsion. Password disclosure by biometrics is like providing voice, fingerprint, thumb impression, clothing samples, or chemical samples, which are physical evidence and do not constitute forced testimony. This case further helped in differentiating between testimonial and non-testimonial evidence. Testimonial evidence is one where the witness is made to reveal the contents of his/her mind in the form of substantial oral or written statements. On the other hand, non-testimonial evidence is one where the witness only lays a foregone conclusion in the sense that there is no statement made but things like blood samples, voice samples, signature specimens, fingerprints, body measurements, and in respect of the current case *passwords, private keys, etc. are obtained.*

¶ 6. What differentiates the two is that these non-testimonial pieces of evidence have no independent incriminatory nature, but simply aid the agencies in investigating and connecting the dots. In the present case, it can very well be seen that the information sought by the investigating authority comes under the purview of a non-testimonial piece of evidence that would help the authority reach the crux of the matter.

¶ 7. The counsel deems it necessary to refer to the case of ***State v. Diamond***,[14] the Supreme Court clarified that since the compelled act of providing fingerprints merely demonstrated Diamond's physical characteristics and did not involve communicating factual assertions from Diamond's mind, the act of providing a fingerprint to unlock a cellphone was not considered a testimonial communication protected by the Fifth Amendment. Drawing parallels to the present case, the Petitioners act of decrypting the private key does not violate the Right against Self Incrimination.

1.1.2. Compelled Decryption in the present case does not amount to Self-Incrimination:

[12] Moot Proposition ¶ 18.
[13] State of Bombay v. Kathi Kalu Oghad, 1961 SCC Online SC 74.
[14] State v. Diamond 905 N.W.2d 870 (Minn. 2018).

¶ 8. The Counsel humbly submits that the High Courts of Karnataka and Kerala are the ones to have dealt with the issue of forced decryption at some length. One of them is the case of ***Virendra Khanna v. State of Karnataka***.[15] In a case before the High Court of Karnataka involving the Narcotic Drugs and Psychotropic Substances Act, 1985,[16] the court had to determine the validity of a trial court order compelling the accused to provide passwords for his smartphone and email account to the investigating agency. Further, in the case of ***State of Uttar Pradesh* v. *Sunil***,[17] the court held that any person can be directed by the court to give his foot-prints or specimens of a similar nature, such as signatures, handwriting samples, etc., for corroboration of evidence, but the same cannot be considered as violation of the protection guaranteed to him under Article 20(3) of the Indican Constitution and also was of the view that they are not incriminating by themselves if they are used for the purpose of identification or corroboration with facts or materials that the investigators are already acquainted with. The petitioners have been directed by the appropriate competent authority to present evidences thus not violating their rights. The same was further held regarding voice samples in ***Ritesh Sinha* v. *State of Uttar Pradesh***.[18]

¶ 9. The High Court concluded that requiring the accused to disclose passwords or fingerprints did not violate the right against self-incrimination or the right to privacy. (*a*) The court argued that a password or fingerprint qualifies as a "document," and Section 139 of the Indican Evidence Act, 1872[19] allows the summoning of an accused to produce such a document. (*b*) It stated that a password or fingerprint functions as an "identification mark," and Section 54-A of the Criminal Procedure Code ("**CrPC**")[20] permits the disclosure of such identification marks by the accused. (*c*) The court reasoned that disclosing a password is like providing specimen signatures or handwriting, and therefore, such disclosure can be ordered under Section 311-A of the CrPC.[21] The court emphasized that providing access to a passcode or email account does not constitute testimonial compulsion since the information accessed still needs to be proven and established in court following the applicable rules of evidence.

¶ 10. In the present case the information sought from Mr. Ian does not compel the accused to give up any information which is self- incriminatory in nature because passwords as mentioned

[15] Virendra Khanna v. State of Karnataka, (2021) SCC OnLine Kar 5032.
[16] Narcotic Drugs and Psychotropic Substances Act 1985.
[17] State of UP v. Sunil, (2017) 14 SCC 516.
[18] Ritesh Sinha v. State of UP, (2019) 8 SCC 1.
[19] Indican Evidence Act 1872, s 139.
[20] Code of Criminal Procedure 1973, s 54-A.
[21] ibid s 311-A.

above qualifies as a document and it functions as an identification mark and Section 54A of CrPC[22] under the Indican Evidence Act,1872 which allows the summoning of an accused to produce the same. Further, in the case of ***Ajay Bhardwaj v. Union of India***[23], the SC directed the accused to share the username and password of his crypto wallet with the Enforcement Directorate for the purpose of carrying out a proper investigation. Throughout the course of the case, the SC did not discuss the constitutional guarantee of the right against self-incrimination, which essentially shows that there was no such breach in demanding such information as the information would not amount to personal knowledge and would help the investigation process.

¶ 11. In light of the cases and arguments mentioned above, the Counsel for the Respondent humbly submits that the mere requirement of giving up the private key, which recorded information about driving and vehicle conditions, including braking, acceleration, and other related data, and also about the vehicle's features such as charging events and status, the enabling/disabling of various systems, diagnostic trouble codes, speed, direction, location,[24] etc., is not self-incriminatory in nature as it does not covered under the testimonial compulsion. It is crucial to be submitted to the investigating authority for decoding the murder.

¶ 12. It is also submitted that even though the law intends to protect an accused person from the hazards of self-incrimination, it cannot put obstacles in the way of efficient and effective investigation into the crime and in bringing criminals to justice and that the Investigation Authorities were well within their rights in seeking such information.

1.2. Section 69 consists of reasonable safeguards that render it constitutional.

¶ 13. The counsel respectfully argues that Section 69[25] cannot be deemed unconstitutional on the grounds of conferring arbitrary powers to the government concerning monitoring, decrypting, or intercepting information. The contention is that historical instances of declaring an act unconstitutional usually stem from the undue and capricious authority it bestows on one party. However, while Section 69 of the Information Technology Act[26] empowers investigative authorities, it imposes specific limitations on the exercise of such powers.

¶ 14. The Counsel would like to submit that even while acknowledging the potential invasion of privacy resulting from access to personal content on a smartphone or email account, the Court had further imposed a duty on investigating officers not to disclose, make public, or use

[22] ibid s 54A.

[23] Ajay Bhardawaj v. Union of India, Writ Petition (Criminal) No 231 of 2019. (Ongoing case in SC)

[24] Moot Proposition ¶ 16.

[25] Information Technology Act 2000, s 69.

[26] ibid.

personal details/data found on such devices or emails in court proceedings without the written permission of the Court in this particular case which clearly ensures that any kinds of information acquired in such a manner requires the approval of the court to be further used as an evidence which clearly is one of the key safeguards provided to the accused.

¶ 15. Additionally, In the context of intercepting, monitoring, or decrypting information, several safeguarding measures are in place, as outlined in the Information Technology Rules of 2009 (hereinafter referred to as "***2009 Rules***").[27]

¶ 16. Prohibition without Authorization: Rule 24 of the 2009 Rules[28] prohibits unauthorized interception, monitoring, or decryption of information from computer resources. Individuals engaged in unauthorized surveillance with malicious intent face punishment under this Rule.

¶ 17. Approval by Review Committee: Rule 22 of 2009 Rules[29] requires that each case of surveillance authorized by the competent authority must undergo review by a committee meeting every two months. Committee's approval is necessary for interception, monitoring, or decryption of information, preventing unchecked power for authorized agencies.

¶ 18. Prohibition of Information Disclosure: Rule 25 of the 2009 Rules[30] ensures the non-disclosure of intercepted, monitored, or decrypted information. Once lawfully obtained by an authorized agency, information should only be used for intended purpose as it is confidential.

¶ 19. Destruction of Recorded Information: Rule 23 of the 2009[31] Rules stipulates that information obtained must be permanently removed from all sources within six months after fulfilling its intended purpose. Retention is allowed only if the authorized agency deems the information useful for its functions.

¶ 20. Recording Reasons for Surveillance: Section 69(1) of the IT Act[32] mandates the recording of reasons before obtaining information from any computer resource. Before directing an agency to intercept, monitor, or decrypt information, the government or its appointed officers must record the reasons for conducting surveillance on such information. Thus, the Petitioners are given sufficient safeguards while decryption is done lawfully.

1.3. Article 19 provides for certain reasonable restrictions and Section 69 does not impose any unreasonable restrictions.

[27] Information Technology Rules 2009.
[28] ibid rule 24.
[29] ibid rule 22.
[30] ibid rule 25.
[31] ibid rule 24.
[32] Information Technology Act 2000, s 69(1).

¶ 21. The counsel respectfully submits that the claims of CG Car Company, where in Section 69 of the IT[33] act is claimed of being violative of the Constitution of Indica should not be upheld due to the presence of the reasonable restrictions under Article 19(1)(a)[34] which guarantees that the Fundamental Rights are not absolute. Article 19(2)[35] allows restrictions in the interest of the nation's sovereignty and integrity, national security, friendly relations with foreign nations, public order, decency, or morality, or in relation to contempt of court, defamation, or incitement to an offense.

¶ 22. The case of ***A.K. Gopalan v. State of Madras***[36] was one of the many cases that upheld the validity of these restrictions, wherein *Justice Das* expressed the view that reasonable restrictions on the enjoyment of fundamental rights are necessitated by the need to prioritize certain broader societal interests over individual liberty in specific circumstances. Further, as mentioned in the previous argument ***K.S. Puttaswamy v. UOI***,[37] the Court had upheld that disclosure of passwords in criminal investigation is covered under "legitimate interests of State." This shows in the present situation of Petitoner's the exception carved for prevention and investigation of crime is a legitimate State interest.

¶ 23. In the case of State of ***MP & ANR v. Gobind***,[38] the court applied the *compelling state interest test,* a concept first established in American legal precedent. The court held that an individual's right to privacy must give way to a stronger state interest, and for the state's interest to prevail, it must be compelling in nature. Under section 69 of IT Act, 2000,[39] government is empowered only under the following circumstances to authorize agencies to intercept, monitor, or decrypt information in certain conditions namely: for protection and preservation of sovereignty and integrity of nation; for maintaining good ties with other nations, to ensure public order; for preventing commission of offences related to above-mentioned areas & for investigation of any offences. The counsel humbly submits that the situations wherein Section 69[40] can be imposed are highly like the reasonable restrictions under Article 19[41] this shows that Section 69[42] is well within the constitutional limits.

1.3.1. Section 69 is an essential legislation for ensuring national security.

[33] Information Technology Act 2000, s 69.
[34] Constitution of Indica 1950, art 19(1)(a).
[35] Constitution of Indica 1950, art 19(3).
[36] A.K. Gopalan v. State of Madras, (1950) SCC 228.
[37] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[38] Gobind v. State of MP, (1975) 2 SCC 148.
[39] Information Technology Act 2000, s 69.
[40] ibid.
[41] Constitution of Indica 1950, art 19.
[42] Information Technology Act 2000, s 69.

¶ **24.** The counsel for the Respondent submits that Section 69[43] derives its legal reasoning from the Telegraphs Act. It is the *grundnorm* source law on electronic surveillance is Section 5(2) of the Indican Telegraph Act, 1885[44] **("Telegraph Act")** read with the Telegraph Rules, 1951.[45] This law allows interception and disclosure of telecom messages *"*on the occurrence of any public emergency or in the interest of public safety". While the telegraph law is an old legislation, Section 5(2)[46] was formulated in 1972 to facilitate surveillance by way of telephone tapping. In 1996, a case was brought by the ***People's Union for Civil Liberties v. Union of India***[47], which challenged the Indican Government's telephone tapping activities and the SC was of the view that telephones may not be tapped except in the interest of national security, public order, investigation of crime and similar objectives, under orders made in writing by the Minister concerned or an officer of rank to whom the power in that behalf is delegated.

¶ **25.** The counsel submits that the same legal reasoning was adapted for surveilling computer records in later laws as well. Section 69 of the Information Technology Act, 2000 ("**IT Act**")[48] mirrored Section 5(2) of the Telegraph Act,[49] the Information Technology Rules[50], 2009 allowed data access on the same basis. Since all these laws have the very same basis and have been evolved from time to time, the counsel submits that it is in no way unconstitutional. Further, the clear requirement of national security has been upheld to be one of the situations where surveillance has been allowed, and in the present case, due to the issue involving murder, there is a clear question of security.

¶ **26.** The counsel asserts that the discovery of a bullet wound on Mr. Anand's body unmistakably indicates that the assailant was in possession of a firearm, which makes it an issue of national security and public safety. The counsel would also like to refer to the Bombay High Court in **Vinit *Kumar v. CBI***,[51] relying on the ***PUCL Ruling***[52] and the ***K.S. Puttaswamy ruling***[53] that illegal tapping of the telephone conversation was held to be violative of the right to privacy and the grounds for issuance of an access order under Section 5(2)[54] was held not

[43] Information Technology Act 2000, s 69.
[44] Indican Telegraph Act 1885, s 5(2).
[45] Indican Telegraph Rules, 1951.
[46] ibid.
[47] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 30.
[48] Information Technology Act 2000, s 69.
[49] Indican Telegraph Act 1885, s 5(2).
[50] Information Technology (Procedures and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009.
[51] Vinit Kumar v. CBI, 2019 SCC OnLine Bom 3155.
[52] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 30.
[53] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[54] Indican Telegraph Act 1885, s 5(2).

for public safety and does not denote a risk for people at large. However, in the present case, as mentioned above, there is a question of the safety of the public at large. The counsel for the Respondent argues that in all the above-mentioned situations, surveillance without the knowledge of the accused is held to be allowed, further it also allows tapping into the private conversations of people and in the present case, Mr. Ian is merely asked to provide an encryption key to knowing his whereabouts and is in no way violative of his privacy.

ISSUE II: WHETHER GOVERNMENTAL CONTROL OVER THE USE OF CRYPTOGRAPHIC TECHNIQUES IS TOO RESTRICTIVE IN NATURE?

¶ 27. The Counsel for Respondent humbly submits before the Hon'ble Court that governmental control over the use of cryptographic techniques is not too restrictive in nature.[55] Compelled decryption is the most important self-incrimination issue of the digital age.[56] The Government is justified in decrypting Mr. Ian's data for investigating the crime and ordering CG Car Company to provide access to private key based[57] on: **[2.1.]** *constitutional and legal framework for decryption powers,* **[2.2.]** *balancing national security and fundamental rights,* and **[2.3.]** *the evidence obtained should be admissible because of its purpose and the validity it upholds.*

2.1. Constitutional and Legal Framework for Decryption Powers.

¶ 28. "Police" and "Public Order" are State subjects under the Seventh Schedule to the Indican Constitution,[58] and therefore, it is the primary duty of the State Governments to prevent, detect, register, and investigate crime and prosecute the criminals.[59] Central Government, however, supplements the efforts of the State Governments by providing them with financial assistance for the modernization of their Police Forces in terms of weaponry, communication, equipment, mobility, training, and other infrastructure under the Scheme of Modernization of State Police Forces. While Mr. Ian asserts his right to privacy, it is essential to recognize the State's legitimate interest in national security.[60]

¶ 29. In the ***Bharat Shantilal Shah case***,[61] the court emphasized the State's duty to ensure public order and national security, even if it infringes on individual rights.[62] Decryption is a

[55] Moot Proposition ¶ 21.

[56] David Rassoul Rangaviz, 'Compelled Decryption & State Constitutional Protection Against Self-Incrimination,' (2020) 57(157) American Criminal Law Review.

[57] Moot Proposition ¶ 21.

[58] Constitution of Indica 1950, schedule VII.

[59] Mahender Chawla v. Union of India, (2019) 14 SCC 615.

[60] Moot Proposition ¶ 21.

[61] Bharat Shantilal Shah v. State of Maharashtra, 2003 SCC OnLine Bom 1361.

[62] Gopalan v. State of Madras, AIR 1950 SC 27.

tool to prevent and investigate crimes, ensuring the safety of citizens.[63] In the present case, it emphasizes the importance of effective tools for law enforcement agencies to maintain public order and investigate crimes.[64] The government, in advocating for the decryption of cryptographic keys, asserts the necessity of striking a balance between national security imperatives and individual rights.[65] This argument draws parallels with cases such as ***National Human Rights Commission v. State of Arunachal Pradesh***,[66] where the court recognized the State's duty to protect citizens from threats posed by private actors. The Counsel humbly submits that in the realm of cybersecurity, decoding cryptographic keys becomes essential to pre-empt and counter potential threats to national security.[67] By allowing the government access to encrypted information, citizens indirectly contribute to the collective responsibility of safeguarding the nation against malicious activities.[68]

2.2. Doctrine of Proportionality and balancing national security and individual rights.

¶ 30. The Counsel humbly submits that the "Doctrine of Proportionality"[69] that was laid down to ensure that the Govt does not take any unnecessary measures to obtain results and that the step taken by government authorities[70] proportionally aligns with the goals that it seeks to achieve is highly relevant in the present case to prove the constitutionality of Section 69[71] and the actions of the Investigation Authority.

¶ 31. The counsel would like to refer to the case of ***Om Kumar v. Union of India***[72] to prove the relevance of this particular doctrine to the case in hand. The Supreme Court in this case acknowledged that Indican courts, since 1950, have consistently applied the principle of proportionality when assessing the constitutionality of legislative actions that impact the fundamental freedoms enumerated in Article 19(1)[73] of the Indican Constitution.[74] The Supreme Court found that government measures affecting basic freedoms[75] (Articles 19 and

[63] Kerala State Beverages (M&M) Corp. Ltd. v. PP Suresh, (2019) 9 SCC 710.
[64] KE v. Sadashiv Narayan Bhalerao, AIR 1947 PC 82.
[65] Internet Freedom Foundation v. Union of India, WP (C) No. 44/2019.
[66] National Human Rights Commission v. State of Arunachal Pradesh, (1996) 1 SCC 742.
[67] Indian Express Newspapers (Bombay) Private Limited v. Union of India, (1985) 1 SCC 641
[68] Praveen Arimbrathodiyil v. Union of India, WP(C) 9647/2021.
[69] Shrillekha Vidyarthi v. State of U. P, AIR 1991 SC 537.
[70] Omkumar v. Union of India, AIR 2000 SC 3689.
[71] Information Technology Act 2000, s 69.
[72] Om Kumar v. Union of India, (2001) 2 SCC 386.
[73] Constitution of Indica, art 19(1).
[74] Ranjit Thakur v. Union of India, (1987) 4 SCC 611.
[75] ibid art 19.

21)[76] in Indica have always been judged on the doctrine of proportionality criteria, even when the doctrine of proportionality is not clearly expressed.[77]

¶ 32. It is humbly submitted by the counsel for the Respondent that one of the most important essentials of this doctrine is that the measures used must be in strict sense, the measure must be proportionate,[78] involving a net gain when weighing the reduction in the enjoyment of the right against the level to which the legitimate interest is advanced.[79] According to Aharon Barak, the former president of the SC of Israel in his "Proportionality and Principled Balancing paper"[80] proportionality *stricto sensu* requires a balancing of the benefits gained by the public and the harm caused to the right of the accused and in the present case the benefits and interests of the public overrides the rights granted to the accused,[81] i.e., Mr. Ian under Article 19.[82]

¶ 33. It is to be kept in mind that a murder is considered to be a crime against the society as upheld in the case of In ***Laxmi Narayan case***,[83] where in the SC noted that crimes like murder and attempt to murder would be considered heinous and serious offences, and that they should be prosecuted as crimes against society rather than against the individual, this means that there is an inherent essence of the fact that the interests and rights of the public[84] overrides the interests and rights granted to an individual[85] when it comes to serious and heinous cases such as murder or attempt to murder.

The Counsel would like to submit that the measures taken by the investigation authority was purely taken to reach to the crux of the matter and accessing the Private Key which provides details of the whereabouts of the suspect on the day of the crime[86] and this in no way breaches the fundamental right of the accused and the measures adopted by the Govt clearly is in proportion with the greater good of the society.[87]

2.2.1. Balancing National Security and Individual Rights:

[76] ibid art 21.
[77] Sandeep Subhash Parate v. State of Maharastra (2006) 1 SCC 50.
[78] Coimbatore Distt. Central Co-operative Bank v. Employees Association, (2007) 4 SCC 669.
[79] Chintaman Rao v. State of MP, AIR 1951 SC 118; VG Row v. State of Madras, AIR 1952 SC 196.
[80] Aharon Barak, 'Proportionality and Principled Balancing. Law and Ethics of Human Rights' (2010) 4 (1) Law & Ethics of Human Rights.
[81] Modern Dental College and Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353.
[82] Constitution of Indica, art 19.
[83] State of M.P. v. Laxmi Narayan, 2017 SCC OnLine SC 1799.
[84] Directorate of Film Festivals v. Gaurav Ashwin Jain 2007 (4) SCC 737.
[85] VG Row v. State of Madras AIR 1952 SC 196 [15].
[86] Moot Proposition.
[87] Anuj Garg v. Hotels Association of India, (2008) 3 SCC 1, 19.

¶ **34.** The government, in advocating for the decryption of cryptographic keys, asserts the necessity of striking a balance between national security imperatives and individual rights.[88] This argument draws parallels with cases such as ***National Human Rights Commission v. State of Arunachal Pradesh***,[89] where the court recognized the State's duty to protect citizens from threats posed by private actors. In the realm of cybersecurity, decoding cryptographic keys becomes essential to pre-empt and counter potential threats to national security.[90] By allowing the government access to encrypted information, citizens indirectly contribute to the collective responsibility of safeguarding the nation against malicious activities.[91]

2.2.2. Fulfilling Statutory and Constitutional Obligations:

¶ **35.** In Supreme Court's view in interpreting the duty of the Government, it had passed judgments in ***Gaurav Kumar Bansal v. Union of India***[92] and ***Swaraj Abhiyan v. Union of India***,[93] the Respondent contends that, similar to the obligations cited in these cases, it has a constitutional and statutory duty to protect citizens.[94] The duty to decrypt cryptographic keys aligns with the affirmative duty imposed on the State to carry out its obligations under the law, especially when private actors may pose a threat to the rights and liberties of individuals.[95] In essence, failure to decode keys in situations of potential harm could be construed as a breach of the government's duty to protect its citizens.[96]

¶ **36.** Drawing from the analysis of the court in the provided text, the government emphasizes the negative duty imposed by Article 21[97] – not to deprive a person of life and personal liberty except in accordance with the law.[98] However, it underscores that this negative duty coexists with an affirmative duty to carry out obligations under statutory and constitutional law.[99] The decryption of cryptographic keys, when warranted by security concerns, becomes a proactive step in fulfilling this affirmative duty. This approach aligns with the principle that the government must act to prevent private actors from infringing on the rights of citizens, as

[88] Sahara India Real Estate Corporation Ltd v. SEBI, (2012) 10 SCC 603.
[89] National Human Rights Commission v. State of Arunachal Pradesh, (1996) 1 SCC 742.
[90] PP Enterprises v. Union of India, AIR 1982 SC 1016; Mohd Hanif Quareshi v. State of Bihar, AIR 1958 SC 731; MRF Ltd. v. Inspector Kerala Government, (1998) 8 SCC 227.
[91] Binoy Viswam v. Union of India, (2017) 7 SCC 59.
[92] Gaurav Kumar Bansal v. Union of India, (2015) 2 SCC 130.
[93] Swaraj Abhiyan v. Union of India, (2016) 7 SCC 498.
[94] In re: Special Courts Bill, AIR 1978 SC 478.
[95] Joseph Shine v. Union of India, (2019) 3 SCC 3.
[96] Tom Hickman,'The Substance and Structure of Proportionality' (2008) Public Law 694, 714-16.
[97] Constitution of Indica, art 21.
[98] Francis Coralie Mullin W. v. Administrator, Union Territory of Delhi, AIR 1981 SC 746.
[99] Hussainara Khatoon v. State of Bihar, A.I.R. 1979 S.C. 1369.

established in various cases, including ***Pt. Parmanand Katara v. Union of India***,[100] In the present scenario, the CG Car Company was asked to provide access to the private key which balances the affirmative duty of the Company along its obligation to carry out statutory obligations of the Act. The Investigating authorities seek to fulfill state-activities and surveillance through these means.[101]

¶ 37. Article 19(6)[102] of Indican Constitution explicitly allows for the imposition of reasonable restrictions on the freedom of trade, business, or profession in the interest of the general public.[103] This provision acknowledges that certain limitations are essential for larger welfare of society.[104]

¶ 38. ***Maneka Gandhi v. Union of India***[105] case expanded the scope of Article 21[106] (Right to Life and Personal Liberty) and emphasized that any law restricting personal liberty must be just, fair, and reasonable. The principle established here underscores the idea that reasonable restrictions are permissible if they meet the criteria of fairness and justice.

¶ 39. A legislation or a government action may have a direct effect on a Fundamental Right, although its subject matter may be different. No law or action will expressly say that it violates a right guaranteed. That is why the courts must protect fundamental rights by considering the scope and provisions of the Act and its effect on fundamental rights. The "effect" test has been applied by the Supreme Court in the ***Maneka Gandhi case***.[107] The object of all freedoms and restrictions is to reach social order or maintenance of public order which was done in the case of Mr. Ian and C.G Car Company. No freedom can be absolute or completely unrestricted. Accordingly, under Art. 19(2),[108] the State may make a law imposing "reasonable restrictions" on the exercise of the right to freedom of speech and expression "in the interests of," the security of the State, friendly relations with the foreign States, public order, decency, morality, sovereignty and integrity of Indica, or *"in relation to the Contempt of Court, defamation or incitement to an offence."* Restrictions in Article 19 (2)[109] are all conceived in the national interests or in the interests of the society.

[100] Pt. Parmanand Katara v. Union of India, AIR 1989 SC 2039.
[101] Moot Proposition ¶ 18.
[102] Constitution of Indica, art 19(6).
[103] Umesh Kumar v. State of Andhra Pradesh (2013) 10 SCC 591.
[104] Dnyaneshwar v. State of Maharashtra (2019) SCC Online Bom 4949.
[105] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[106] Constitution of Indica, art 21.
[107] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[108] ibid art 19(2).
[109] ibid art 19(6).

¶ 40. In ***Express Newspapers v. Union of India***,[110] it was held by the Supreme Court that there ought to be a reasonable balance between the freedoms enshrined under Article 19(1)[111] and the social control permitted by clauses (2) to (6). In addition to this, the restriction imposed shall have a direct or proximate nexus with the object sought to be achieved by the law. There is credible information suggesting that Ian's data might contain evidence related to criminal activities, seeking the private key could be considered a reasonable step in the investigation process. It aligns with the broader concept of justice, ensuring that individuals involved in criminal activities are held accountable for their actions. In the context of cryptographic keys, the government's access to such keys can be seen as a reasonable restriction justified by the need for national security and public safety. Complying with the principles in ***Maneka Gandhi case***[112], any action that curtails personal liberty must be balanced with the broader public interest. Decrypting Ian's data may be justified if it serves the larger purpose of ensuring public order, safety, and justice. The principle of balancing individual rights with the collective well-being of society is crucial in determining the reasonableness of such actions.

¶ 41. Section 16 read along with Section 69 of the IT Act, 2000[113] and the accompanying regulations of the IT Act, 2000 underscores the government's commitment to accountability and transparency in the use of decryption powers. By mandating the submission of cryptographic algorithms to the "Authority on Control and Regulation of Cryptography" and requiring prior approval for their use, the government establishes a procedural framework that acts as a safeguard against arbitrary or unchecked decryption. This ensures that the exercise of decryption powers is subject to a structured process, preventing potential misuse and upholding the principles of due process. The creation of "Authority on Control and Regulation of Cryptography" adds an additional layer of oversight to the process. The Authority, is a body with the expertise to evaluate cryptographic tools, acts as a check on the government's exercise of decryption powers. Its role in approving the use of cryptographic algorithms provides a safeguard against arbitrary or unwarranted requests for decryption. An independent entity contributes to a balanced approach that considers both individual rights and state interests.

¶ 42. For CG Car Company, complying with decryption requirements aligns with national interests, ensuring that its technologies do not compromise security and do not affect the

[110] Express Newspapers (P) Ltd. v. Union of India, (1986) 1 SCC 133.
[111] ibid art 19(1).
[112] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[113] Information Technology Act 2000, s 69.

reputation and business stakes of the company. This is an indigenous exercise of power and will not be exercised unless a significant reason mandates it.

¶ 43. In light of the Respondent's contention, the Respondent asserts that the decryption of cryptographic keys is not an arbitrary intrusion but a targeted measure to prevent potential harm. The duty to protect citizens extends to safeguarding their interests in the digital realm. The government contends that ensuring the safety and security of individuals, businesses, and the nation as a whole necessitates the ability to decode encrypted communications when authorized by law. This approach mirrors the court's decisions in cases where the State's intervention was deemed necessary to prevent harm to individuals or communities.

2.3. The Standard for Testing Violations When Others Fundamental Rights Are Affected.

¶ 44. The Counsel for Respondent humbly submits that in accordance with the ***K.S. Puttaswamy case***, national security objectives and crime control are deemed as legitimate state objectives.[114] Section 5 of the Indican Evidence Act 1872 is commonly recognized as the statutory foundation for the principle that evidence obtained unlawfully can be deemed admissible when it is of public concern.[115] Several government officials have highlighted the challenges posed by encryption in mitigating the risks of terrorism, dissemination of false information, and offenses against women and children.[116] After the India-Pakistan conflict in Kargil in 1999, the Kargil Review Committee observed that insufficient focus and resources were allocated to the cultivation of encryption and decryption capabilities.[117] The committee further underscored the growing dependence of organized crime and anti-national elements on encrypted communications.[118]

¶ 45. In 2015, the Indican government published a preliminary version of the National Encryption Policy for public feedback. In the preamble of the draft policy, emphasis was placed on the significance of safeguarding internet transactions, while concurrently addressing the needs of national security agencies and Law Enforcement Agencies (LEAs)[119] defines "key" as a "sequence of symbols that controls the operation of a cryptographic transformation (e.g.

[114] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[115] Indican Evidence Act 1872, s 5.
[116] Bedavyasa Mohanty, 'Encryption Policy 2.0, Securing India's Digital Economy' (2017) ORF Special Report.
[117] Bachan Singh v. State of Punjab, AIR 1980 SC 89.
[118] Dr. Farooq Ahmad, *Cyber Law in India* (4th edn, 2011) 33.
[119] Information Technology (Certifying Authorities) Rules 2000, schedule V.

encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification."[120]

2.3.1. *The Heinous Crime which was committed violates the Fundamental Rights vested to the other citizens of the State:*

¶ 46. As per the Intermediary Rules, the Intermediary is mandated to identify the initial originator and is not obligated to divulge the substance of any electronic message or any other details pertaining to the first originator or other users.[121] Similarly, CGCC is not requested to enclose data with the necessary information but the initial originator of the messages. It must be pointed out that the Joint Cipher Bureau of the Government of Indican has jurisdiction over issues of public key and private key management, production of customized cryptographic products, etc.[122] However, the Bureau serves mostly as an arm of the Indican Army as it provides it with tactical cryptographic equipment and the management thereof.[123]

¶ 47. Recently, the Madras High Court *suo motu* took up a public interest litigation concerning a matter where a boy committed suicide under the influence of an online game. Most of the participants receive a link to participate in this game by way of WhatsApp, which uses end-to-end encryption. Such encryption ensures complete anonymity of users, leaving the law enforcement agencies with little evidence to prosecute crime and prevent terrorism.[124] The High Court expressed a concern that such applications could also pose a threat to national security, as the source of the messages and the sender of invitation to participate in the online game, in the present case, remains untraceable.[125]

¶ 48. Thus, the Counsel humbly submits that the rights of CGCC must be protected, there must be reasonable restrictions vested in the government, and the control can nowhere be deemed invalid.

[120] Draft National Encryption Policy 2015.

[121] 'NIST Cryptographic Standards and Guidelines Development Process' (*National Institute of Standards and Technology*, 2016).

[122] Summer v. Shuman, 55 US Law Week 4931 (1987).

[123] G.S. Bajpai, *On Cyber Crime and Cyber Law* (2011) 538, 551.

[124] Mithu v. State, AIR 1983 SC 473.

[125] Registrar (Judicial) v. Secretary to Government, Suo Moto WP (MD) No. 16668 of 2017.

PRAYER

Wherefore, considering the facts stated, questions presented, pleadings advanced, and authorities cited, counsels for the Respondent pray that this Hon’ble Court may be pleased to adjudge and declare that:

1. Section 69 of the Information Technology Act, 2000 is constitutional.
2. The Governmental control over the use of cryptographic techniques is reasonably restrictive in nature.

The Hon’ble Court, being satisfied, may also make any such order as it may deem fit in the light of Justice, Equity, and Good conscience.

All of which is most humbly prayed.

ON BEHALF OF THE RESPONDENT.

PLACE: ___________ Sd/

DATE: ____________ Counsel for the Respondent