TEAM CODE: TL - 18

4TH SURANA & SURANA AND CUSAT SCHOOL OF LEGAL STUDIES, DR. A T MARKOSE MEMORIAL TECHNOLOGY LAW MOOT COURT COMPETITION, 2024

IN THE HON'BLE SUPREME COURT OF INDICA

UNDER ARTICLE 32 AND 139-A OF THE CONSTITUTION OF INDICA

WP NO._ OF 2023

CG CAR COMPANY AND OTHERS

(PETITIONER)

V.

UNION OF INDICA

(RESPONDENT)

MEMORIAL ON BEHALF OF THE PETITIONER

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Anr	Another
v.	Versus
Hon'ble	Honourable
Ors.	Others
AIR	All India Report
SC	Supreme Court
SCC	Supreme Court Cases
SCR	Supreme Court Report
Art.	Article
Const.	Constitution
HC	High Court
Sec.	Section
No.	Number
Edn.	Edition
cd.	Code
cl.	Clause
&	And
IT Act	Information Technology Act, 2000
DPDP Act	The Digital Personal Data Protection Act, 2023
Anr	Another
v.	Versus
Hon'ble	Honourable
Ors.	Others

INDEX OF AUTHORITIES

BOOKS

1. M P Jain, *Indian Constitutional Law* (7th edition, LexisNexis 2018) 533-549
2. Mahendra P. Singh, *V. N. Shukla's Constitution of India*, (11th edition, Eastern Book Company 2008) 160
3. H. M. Seervai, *Constitutional Law of India: A Critical Commentary* (Volume 1, 4th edition, Universal Law Publishing Co. Pvt. Ltd 1991) 435-440
4. Dr. L. M. Singhvi & Jagadish Swarup, *Constitution of India* (Volume 1, 3rd edition, Thomson Reuters 2013) 986
6. Dr. Durga Das Basu, *Commentary on the Constitution of India* (Volume 2, 8th Edition, LexisNexis 2007) 1464-1475
7. H. K. Saharay, *The Constitution of India An Analytical Approach* (4th Edition, Eastern Law House 2012) 274-281
8. Mamta Rao, *Constitutional Law* (Eastern Book Company pvt. ltd. 2021) 35
9. C.K. Takwani, *Textbook on Constitutional Law of India* (Whytes & co. 2021) 599

CASES

1. *Supreme Court of India v Subhash Chandra Agarwal*, [2020] 5 SCC 481
2. *District Registrar and Collector v Canara Bank*, [2005] 1 SCC 496
3. *K.S. Puttaswamy [Privacy-9J.] v Union of India*, [2017] 10 SCC 1,
4. *District Registrar and Collector v Canara Bank*, [2005] 1 SCC 496
5. *Mukesh Singh v State [NCT of Delhi],* [2020] 10 SCC 120
6. *Vinay Tyagi v Irshad Ali*, [2013] 5 SCC 762
7. *Shatrughan Chauhan v Union of India*, [2014] 3 SCC 1
8. *State of W.B. v Committee for Protection of Democratic Rights*, [2010] 3 SCC 571
9. *H.N. Rishbud v State of Delhi*, AIR 1955 SC 196
10. *Niranjan Singh v State of U.P*., 1956 SCR 734
11. *Paramjit Singh v State of Punjab*, [2007] 13 SCC 530
12. *Rekha v State of Maharashtra*, [2010] 15 SCC 725
13. *Union of India v T. Nathamuni*, [2014] 16 SCC 285

14. *M.P. Sharma v Satish Chandra,* [1954] 1 SCR 1077
15. *Maneka Gandhi v UOI* [1978] AIR 597
16. *R.M. Malkani v State of Maharashtra*, [1973] 1 SCC 471
17. *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, [2020] 7 SCC 1, [64]
18. *V Narayanan v District Collector*, 2018 SCC OnLine Mad 5592
19. *Suraj Pal v Communication & IT*, 2009 SCC OnLine CIC 12247
20. *Nandini Satpathy v P.L. Dani*, [1978] 2 SCC 424
21. *Selvi v State of Karnataka*, [2010] 7 SCC 263, [128]
22. *Anuradha Bhasin v Union of India* [2020] 3 SCC 637
23. *Sakal Papers [P] Ltd. v Union of India* AIR 1962 SC 305, [315]
24. *Kesavananda Bharati & Ors. v State of Kerala & Anr* [1973] 4 SCC 225
25. *Shreya Singhal v Union of India* [2015] 5 SCC 1
26. *Chief Settlement Commissioner, Punjab v Om Prakash* [1968] 3 SCR 655
27. *People's Union for Civil Liberties v Union of India* [1997] 1 SCC 301
28. *Sharat Babu Digumarti v Govt. [NCT of Delhi]* [2017] 2 SCC 18
29. *Kihoto Hollohan v Zachillhu* 1992 Supp [2] SCC 651
30. *Jacob Puliyel v Union of India* 2022 SCCOnline SC 533
31. *Modern Dental College and Research Centre v State of Madhya Pradesh* [2016] 7 SCC 353
32. *Gesamtverband Autoteile-Handel eV v Scania CV AB* OJ 2018 L 151, [1]
33. *Akshay N. Patel v RBI* [2022] 3 SCC 694
34. *Francis Coralie Mullin v Union Territory of Delhi* [1981] 2 SCR 516
35. *R.S. Raghunath v State of Karnataka* [1992] 1 SCC 335; AIR 1992 SC 81
36. *Central Coalfields Ltd. v State of M.P.* [1995] 2 SCC 11
37. *Facebook Inc v Union of India,* 2019 SCCOnline SC 1264
38. *Toofan Singh v State of T.N.,* [2021] 4 SCC 1
39. *Kharak Singh v State of UP & Ors* [1964] SCR (1) 332
40. *Dwarka Prasad Laxmi Narain v State of Uttar Pradesh & Two Ors* [1954] SCR 803
41. *Rustom Cavasjee Cooper v Union of India* [1970] 1 SCC 248
42. *Mohd. Yasin v Town Area Committee* [1952] 1 SCC 205
43. *Kaushal Kishore v State of Uttar Pradesh & Ors* [2023] 4 SCC 1
44. *Hukam Chand Shyam Lal v Union of India And Ors* [1976] SCR (2)1060

45. *Pramod Singla v Union of India* [2023] SCC OnLine SC 374
46. *Indira Nehru Gandhi v Raj Narain* [1975] 2 SCC 159
47. *Union of India v Association for Democratic Reforms* [2002] (3) SCR 294
48. *Internet & Mobile Assn. of India v RBI* [2020] 10 SCC 274
49. *Benett Coleman & Co. v Union of India* [1973] 2 SCR 757
50. *Bachan Singh v State of Punjab* [1982] 3 SCC 24
51. *Sakal Papers v Union of India* [1962] SCR (3) 842
52. *Rev Stanislaus v Madhya Pradesh* [1977] SCR (2) 611
53. *Franklin Templeton Trustee Services (P) Ltd. v Amruta Garg* [2021] 9 SCC 606.

STATUTES

1. The Constitution of India
2. The Digital Personal Data Protection Act, 2023
3. Information Technology Act, 2000
4. The Evidence Act, 1872
5. The Criminal Procedure Code, 1973
6. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009
7. Telegraph Act, 1855
8. Telecommunications Act, 2023

ARTICLES

1. Alekhya Sattigeri, 'Gauging the Constitutionality of S. 69 of the IT Act Vis-à-Vis Test of Proportionality Laid Down in KS Puttaswamy', (*Live Law,* 10 Apr 201) <https://www.livelaw.in/columns/information-technology-act-2000-ks-puttaswamy-fundamental-rights-172407?infinitescroll=1> accessed on 27 Dec 2023
2. Bedavyasa Mohanty, 'The Constitutionality of Indian Surveillance Law: Public Emergency as a Condition Precedent for Intercepting Communications' (*The Centre for Internet & Society*) <https://cis-india.org/internet-governance/blog/the-constitutionality-of-indian-surveillance-law> accessed on 27 December 2023

3. Monica Shaurya Gohil and Chetna Bujad, 'Data Privacy Implications of Contact Tracing Apps in India' (2021) 11.1 NULJ 1
4. Vinod Joseph & Protiti Basu, 'Right of Erasure - Under the Personal Data Protection Bill, 2019' (*MONDAQ*) <https://www.mondaq.com/india/data/protection/877732/right-of-erasure---under-the-personal-data-protection-bill-2019> accessed on 27 December 2023
5. Supratim Chakraborty, 'Data Protection in India: Overview' (Khaitan & Co. LLP) <https://www.khaitanco.com/sites/default/files/2021-04/Data%20Protection%20in%20India%20Overview.pdf> accessed on 3 January 2024
6. Aditya Sarmah, 'Privacy and the Right Against Self-Incrimination: Theorising a Criminal Process in the Context of Personal Gadgets', 3.2 CALQ (2017) 28.
7. NASSCOM-DSCI, 'Encryption and The Digital Economy: Balancing Security, Privacy, and National Security' [2020]
8. Gaurav Kumar, 'An Analysis of the Pegasus Spyware issue in light of Surveillance Laws and the Right to Privacy in India' (2022) 2.3 JCLJ 827.
9. Ashutosh Chandra, 'Pegasus - Spyware with Wings as Seen from a Legal Lens' (2022) 2.1 DSNLUJ SCI Tech L 124.

INTERNATIONAL LEGISLATIONS

1. The General Data Protection Regulation, 2016
2. European Data Protection Board's Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications
3. International Principles on the Application of Human Rights to Communication Surveillance, 2013

OTHER SOURCES

1. United Nations Human Rights Office of High Commissioner, Basic Principles on the Independence of the Judiciary [Mar. 16, 2023, 9:00 PM], https://www.ohchr.org/en/instruments-mechanisms /instruments/basic-principles-independence-judiciary.

2. MEITY <https://www.meity.govin> accessed on 21 December 2023
3. INFORMATION COMMISSIONER's OFFICE <https://ico.org.uk/for-organisations/> accessed on 21 Dec 2023
4. DATA PROTECTION COMMISSION, <https://www.dataprotection.ie/en/individuals/> accessed on 21 Dec 2023
5. Department of Telecommunication, Ministry of Communications & Government of India, Licensing Agreement for Unified License [2014]
6. A P Shah, Report of the Group of Experts on Privacy [2012]
7. B N Srikrishna Committee, free and fair economy [2018]
8. Report by the Committee of Experts on Non-Personal Data Governance Framework [2020]
9. SFLC.IN, 'Surveillance – Is There A Need For Judicial Oversight?', (SFLC.IN, 25 September 2013) https://sflc.in/surveillance-there-need-judicial-oversight/ accessed 4 January 2024

STATEMENT OF JURISDICTION

The petitioner submits this writ petition before the Hon'ble Supreme Court of Indica maintainable under Article 32 and Article 139-A of the Constitution of Indica.

Article 32 confers powers to the Hon'ble Supreme Court for enforcement of Fundamental Rights.

"32. Remedies for enforcement of rights conferred by this Part
(1) The right to move the Supreme Court by appropriate proceedings for the enforcement of the rights conferred by this Part is guaranteed
(2) The Supreme Court shall have power to issue directions or orders or writs, including writs in the nature of habeas corpus, mandamus, prohibition, quo warranto and certiorari, whichever may be appropriate, for the enforcement of any of the rights conferred by this Part
(3) Without prejudice to the powers conferred on the Supreme Court by clause (1) and
(2), Parliament may by law empower any other court to exercise within the local limits of its jurisdiction all or any of the powers exercisable by the Supreme Court under clause (2)
(4) The right guaranteed by this article shall not be suspended except as otherwise provided for by this Constitution"

Article 139-A grants power to the Supreme Court to Transfer certain cases

"139A. Transfer of certain cases-
(1) Where cases involving the same or substantially the same
questions of law are pending before the Supreme Court and one or more High Courts or before two or more High Courts and the Supreme Court is satisfied on its own motion or on an application made by the Attorney-General of India or by a party to any such case that such questions are substantial questions of general importance, the Supreme Court may withdraw the case or cases pending before the High Court or the High Courts and dispose of all the cases itself:
Provided that the Supreme Court may after determining the said questions of law return any case so withdrawn together with a copy of its judgment on such questions to the High Court

from which the case has been withdrawn, and the High Court shall on receipt thereof, proceed to dispose of the case in conformity with such judgment.

(2) The Supreme Court may, if it deems it expedient so to do for the ends of justice, transfer any case,

appeal or other proceedings pending before any High Court to any other High Court."

The Petitioner shall humbly accept the Court's decision as final and binding and execute it in good faith and with due diligence.

STATEMENT OF FACTS

INDICA

The Republic of Indica is a democratic country and has become a fast-growing major economy. The Parliament of Indica enacted various legislations to regulate the advancements that have occurred. One such prominent legislation was the Information Technology Act in the year 2000 which was extensively amended in 2008.

THE ACCIDENT

On 13th of August 2022, at about 7:00 am, a family, on vacation, saw a body lying in a pool of blood on the road next to the car (with registration number SK 47 BH 1234). The police arrived and after searching, understood that the body was of Mr. Anand.

UNDISPUTED FACTS

The police took note of the vehicles passed through State Highway No. 106 and decided to investigate more into Mr. Ian. Police confiscated Mr. Ian's car, and identified that the said vehicle had onboard ICT facilities which could show details of the vehicle.

AUTOMATED SYSTEM

The automated system used in CG-Metron used blockchain technology for storing data and the access to the same was using the private key with the owner. The electronic modules used in the vehicle recorded information about driving, vehicle conditions and features.

THE DISPUTE

This proceeding was challenged by Mr. Ian the High Court of Antartaka. The Head office of CG Car Company in India filed a writ petition in the Hon'ble Supreme Court of Indica. The Supreme Court of Indica ordered the transfer of the connected case and decided to hear both the matters.

STATEMENT OF ISSUES

ISSUE 1

WHETHER SECTION 69 OF THE INFORMATION TECHNOLOGY ACT, 2000 IS CONSTITUTIONALLY VALID?

ISSUE 2

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

SUMMARY OF ARGUMENTS

ISSUE 1

The counsel on behalf of petitioners submits that Section 69 of the IT Act violates the right against self-incrimination and the right to privacy. The arguments highlight concerns about the collection and acquisition of personal data through illegal methods, lack of proportionality, and non-compliance with the DPDP Act. Section 69 is criticized for being arbitrary, lacking safeguards, and conflicting with data protection laws. The counsel asserts that Section 69 infringes on constitutional rights, specifically Article 20(3) and Article 21 of the Constitution of Indica.

ISSUE 2

The Petitioners humbly submit before this Hon'ble Court that the governmental control over cryptographic techniques is not too restrictive in nature. Firstly, the mandatory requirement to submit cryptographic techniques is manifestly arbitrary. Secondly, the restrictions imposed by the government are unreasonable and it violates the rights conferred under Article 19 of the Constitution of India. Thirdly, the lack of judicial oversight and the inadequacy of safeguards against the arbitrary misuse of power renders the governmental control too restrictive. Additionally, the governmental control is in violation of the Right to Information Act, 2005, Digital Personal Data Protection Act, 2023 & the Non-Personal Data governance framework. Thus, it is submitted that the governmental control over cryptographic techniques is far too restrictive.

ARGUMENTS ADVANCED

ISSUE 1

WHETHER SECTION 69 OF THE INFORMATION TECHNOLOGY ACT, 2000 IS CONSTITUTIONALLY VALID?

1. It is submitted that the use of blockchain technology in CG-Metron's automated system collecting personal driving and vehicle data violates privacy rights under the Constitution and the DPDP Act. Illegal hacking, acquiring entire datasets, and non-compliance with evidence laws further infringe on privacy rights. Section 69 compels self-incrimination, contravening Article 20(3) and violating the right to privacy.

I. SECTION 69 VIOLATES THE RIGHT AGAINST SELF-INCRIMINATION

(i) THE DATA BEING COLLECTED QUALIFIES AS "PERSONAL INFORMATION"

2. The automated system used in CG-Metron used blockchain technology for storing data. The electronic modules used in the vehicle recorded information about driving and vehicle conditions, including braking, acceleration, and other related data. These modules also record information about the vehicle's features such as charging events and status, the enabling/disabling of various systems, diagnostic trouble codes, speed, direction, **location**, etc.[1]
3. In the landmark Privacy Judgement, **K.S. Puttaswamy** v. Union of India, it classified "location" details under personal information.[2] The court laid down that the non-consensual revelation of personal information such as the state of one's health, finances, place of residence, **location**, daily routines and so on efface one's sense of personal and financial security.[3]

   Therefore, it is a violation of the fundamental right of privacy enshrined in article 21 of the Constitution of Indica. As the data being collected is data about an individual who is identifiable by or in relation to such data,[4] Section 69[5] violates the objectives of The

[1] Moot Proposition [16].
[2] *Supreme Court of India v Subhash Chandra Agarwal*, [2020] 5 SCC 481; *District Registrar and Collector v Canara Bank*, [2005] 1 SCC 496.
[3] *K.S. Puttaswamy [Privacy-9J.] v Union of India*, [2017] 10 SCC 1, *District Registrar and Collector v Canara Bank*, [2005] 1 SCC 496.
[4] The Digital Personal Data Protection Act 2023, s 2(t).
[5] The Information Technology Act 2000, s 69.

Digital Personal Data Protection Act, 2023 [hereinafter referred to as "DPDP Act"] such as **consent.**[6]

4. **The Digital Personal Data Protection Act (DPDP Act) emerged from the landmark Puttaswamy judgement**, which recognized privacy as a fundamental right in India. Inspired by the Puttaswamy Court's reliance on international principles and foreign precedents, the DPDP Act embodies these principles, including purpose limitation, data minimization, transparency, and individual rights. It builds upon the Puttaswamy foundation, translating its ideals into a comprehensive framework for protecting personal data in the digital age.

(ii) SECTION 69 VIOLATES AN INDIVIDUAL'S RIGHT TO FAIR INVESTIGATION

5. As the Consent of the Data Principal was not considered it is in violation of his Right to fair Investigation.[7] As held by this Court in Vinay Tyagi,[8] lays down that fair and proper investigation has a **twin purpose**, firstly, the investigation must be unbiased, honest, just and in **accordance with law**, secondly, the entire emphasis on a fair investigation[9] has to be to **bring out the truth** of the case before the court of competent jurisdiction.[10]
6. The current case does not qualify the twin test as the investigation conducted was not in accordance with law and the evidence collected might not serve the purpose of reveal the entire truth about the case.

(iii) ILLEGAL METHODS OF ACQUIRING DATA VIOLATES THE RIGHT TO PRIVACY

7. This proceeding was challenged by Mr. Ian under Section 482 of the Code of Criminal Procedure before the High Court of Antartaka, as the police tried to **illegally hack**[11] into his system and for the infringement on his privacy.[12]

---

[6] The Digital Personal Data Protection Act 2023, s 6.
[7] *Mukesh Singh v State [NCT of Delhi],* [2020] 10 SCC 120.
[8] *Vinay Tyagi v Irshad Ali*, [2013] 5 SCC 762.
[9] *Shatrughan Chauhan v Union of India*, [2014] 3 SCC 1; *State of W.B. v Committee for Protection of Democratic Rights*, [2010] 3 SCC 571.
[10] *H.N. Rishbud v State of Delhi*, AIR 1955 SC 196; *Niranjan Singh v State of U.P.*, 1956 SCR 734; *Paramjit Singh v State of Punjab*, [2007] 13 SCC 530; *Rekha v State of Maharashtra*, [2010] 15 SCC 725; *Union of India v T. Nathamuni*, [2014] 16 SCC 285.
[11] *M.P. Sharma v Satish Chandra*, [1954] 1 SCR 1077.
[12] Moot Proposition [19].

8. The police illegally hacking into the computer system violates section 43[13] of the Information Technology Act, 2000 [hereinafter referred to as "IT Act"] which provides for Penalty and Compensation for damage to computer, computer system, when a person without permission of the owner or any other person who is in charge of a computer, computer system or computer network tries to access the data. This method of acquiring evidence violates due process of law laid down in *Maneka Gandhi.*[14]
9. Acquiring data by illegally hacking into the system would have altered the data stored in it. This would have been in direct violation of section 65B(2)(c) of the Indian Evidence Act, 1872 [hereinafter referred to as "Evidence Act"] and should not be admissible.[15]

(iv) THE ENTIRE DATA SET BEING COLLECTED

10. The police tried to acquire the encrypted data in which the entire system was capable of being operated by the smartphone linked.[16] Accessing the data by entering the private key would unlock all the information stored in the blockchain technology.
11. This is in clear violation **section 39[17] of the Evidence Act** which states that when the evidence is stored in an electronic record, only the relevant part of the data should be accessed. Collection of the entire vehicular data would not serve the purpose of the investigation. This also violates the principle of **purpose limitation** under section 6(1) of the DPDP Act.
12. In the case of *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*,[18] the court laid down that the Call Detail Record being collected should be in tune with Section 39 of the Evidence Act.
13. Rules 23[19] of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 [hereinafter referred to as "Interception Rules"], states that every record, including electronic records pertaining to such directions for interception or monitoring or decryption of information and of intercepted or monitored or decrypted information shall be destroyed by the security

[13] The Information Technology Act 2000, s 43.
[14] *Maneka Gandhi v UOI* [1978] AIR 597.
[15] *R.M. Malkani v State of Maharashtra*, [1973] 1 SCC 471.
[16] Moot Proposition [16].
[17] The Evidence Act 1872, s 39.
[18] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, [2020] 7 SCC 1, para 64; *V Narayanan v District Collector*, 2018 SCC OnLine Mad 5592.
[19] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, rule 23.

agency in every six months except in a case where such information is required, or likely to be required for functional requirements.

14. The exception mentioned in the rule does not elaborate on the conditions for storing the data for longer than six months which is manifestly arbitrary.

(v) IN VIOLATION OF ARTICLE 20(3) OF THE CONSTITUTION

15. Article 20(3)[20] of the Constitution of Indica grants protection against self-incrimination. The provision states that "*No person accused of any offence shall be compelled to be a witness against himself*".

16. In the case of Suraj Pal v. Communication & IT,[21] the court held that:

"*14. After perusal of all the materials/documents available on record, and also after taking into consideration the arguments of both the parties, it is evident that the sharing of* ***Appellant's call details*** *by the MTNL with the Law Enforcement Agency without seeking consent/approval of either the Competent Authority or even the Appellant was* ***clearly unlawful*** *as discussed hereinabove being* ***violation of Section 131 of the Indian Evidence Act, 1872*** *and* ***the Section 69 of the IT Act*** *as alleged*."

(Emphasis Supplied)

17. Therefore, Section 69 violates the right against self-incrimination as there is compulsion[22] created by issuing a notice and illegally hacking into the blockchain technology. This is a clear violation of section 131 of the Evidence Act as the personal information acquired is against the individual's right to privacy and is used to strengthen the case.[23]

II. SECTION 69 OF THE IT ACT VIOLATES RIGHT TO PRIVACY

(i) DOES NOT QUALIFY THE TESTS FOR REASONABLE RESTRICTION

It is submitted that Section 69 of the IT Act is not a reasonable restriction on the Right to Privacy. The threefold test of legality, necessity and proportionality laid down in the case of K.S Puttaswamy v. Union of India are being contended in three folds - [A] Section 69 of the IT Act fails the test of legality [B] Section 69 of the IT

[20] The Constitution of India, art 20(3).
[21] *Suraj Pal v Communication & IT*, 2009 SCC OnLine CIC 12247.
[22] *Nandini Satpathy v P.L. Dani*, [1978] 2 SCC 424.
[23] *Selvi v State of Karnataka*, [2010] 7 SCC 263, [128].

Act fails the test of necessity [C] Section 69 of the IT Act fails the test of Proportionality.

(A) SECTION 69 OF THE IT ACT FAILS THE TEST OF LEGALITY

18. It is submitted that Section 69 of the IT Act fails the test of legality.[24] The Right to Privacy is subject to certain reasonable restraints.[25] The grounds provided for restrictions in Art. 19(2)-(6) are exhaustive and must be interpreted strictly.[26]
19. The Interception Rules has expanded the scope of government interception by introducing grounds[27] such as 'defence of India', 'investigation of any offence', giving the **Executive overarching authority** to issue Interception orders as they may deem fit.[28]
20. Therefore, the arbitrary[29] nature of power assured to the Central Government and executive authority by Section 69 of the IT Act marks the provision as unjust, unfair and unreasonable, hence, violating the condition of legality.[30]

(B) SECTION 69 OF THE IT ACT FAILS THE TEST OF NECESSITY

21. The term 'investigation of any offence', which are the grounds under Section 69 of the IT Act for issuance of interception orders have not been clearly defined by the legislature or the court and the question of the existence of these grounds is left to the sole determination of an Executive, vesting arbitrary powers[31] to order interception of communication, violating Art. 14.[32] Therefore, this absolute and unquestioned discretion[33] which Section 69 of the IT Act confers upon the Executive is manifestly arbitrary.[34]

---

[24] *Anuradha Bhasin v Union of India* [2020] 3 SCC 637.
[25] *K.S. Puttaswamy v Union of India* [2017] 10 SCC 1, [310].
[26] *Sakal Papers [P] Ltd. v Union of India* AIR 1962 SC 305, [315].
[27] *Kesavananda Bharati & Ors. v State of Kerala & Anr* [1973] 4 SCC 225.
[28] Alekhya Sattigeri, 'Gauging the Constitutionality of S. 69 of the IT Act Vis-à-Vis Test of Proportionality Laid Down in KS Puttaswamy', (*Live Law,* 10 Apr 201) <https://www.livelaw.in/columns/information- technology-act-2000-ks-puttaswamy-fundamental-rights-172407?infinitescroll=1>.
[29] *Shreya Singhal v Union of India* [2015] 5 SCC 1.
[30] *Chief Settlement Commissioner, Punjab v Om Prakash* [1968] 3 SCR 655.
[31] *People's Union for Civil Liberties v Union of India* [1997] 1 SCC 301.
[32] Bedavyasa Mohanty, 'The Constitutionality of Indian Surveillance Law: Public Emergency as a Condition Precedent for Intercepting Communications' (*The Centre for Internet & Society*) <https://cis-india.org/internet-governance/blog/the-constitutionality-of-indian-surveillance-law> accessed on 27 December 2023.
[33] *Sharat Babu Digumarti v Govt. [NCT of Delhi]* [2017] 2 SCC 18.
[34] *Kihoto Hollohan v Zachillhu* 1992 Supp [2] SCC 651.

In the current case, it is not necessary for the police to acquire the stored data through illegally hacking into the private key.

(C) SECTION 69 OF THE IT ACT FAILS THE TEST OF PROPORTIONALITY

22. It is submitted that Section 69 fails the test of Proportionality[35] as it is inconsistent with the requirement of the Proportionality test laid down in *K.S. Puttaswamy Judgement,*[36] which states that a measure restricting a right must serve a legitimate goal; there must be a suitable means of furthering this goal; there should not be any less restrictive[37] and equally effective alternative available and it must not have a disproportionate impact on the right-holder.
23. This rule is a gross violation of the proportionality test of the reasonable restrictions[38] and also violates the principle of **erasure of data[39]** under section 12 of the DPDP Act, which states that "*A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent*"
24. Therefore, the test of proportionality and have impacted the civil and fundamental rights of the people.[40] It can be gathered that Section 69 of the IT Act is antithetical to the right to privacy as it fails the aforementioned tests, and, therefore, should be deemed unconstitutional, thereby invalidating the action of the government.
25. Moreover, with there being no adequate safeguards provided in Section 69 of the IT Act, the government can issue any order, irrespective of its proportionality with the purpose intended. The Impugned Section provides no guideline for data retention, allowing for misuse of data acquired and subjecting the right to privacy to the government's discretion.[41]

---

[35] *Jacob Puliyel v Union of India* 2022 SCCOnline SC 533.
[36] *Modern Dental College and Research Centre v State of Madhya Pradesh* [2016] 7 SCC 353.
[37] *Gesamtverband Autoteile-Handel eV v Scania CV* C-319/22.
[38] *K.S. Puttaswamy v Union of India* [2017] 10 SCC 1, [310].
[39] The Digital Personal Data Protection Act 2023, s 12.
[40] United Nations Human Rights Office of High Commissioner, Basic Principles on the Independence of the Judiciary [Mar. 16, 2023, 9:00 PM], https://www.ohchr.org/en/instruments-mechanisms /instruments/basic-principles-independence-judiciary accessed on 27 December 2023.
[41] Monica Shaurya Gohil and Chetna Bujad, 'Data Privacy Implications of Contact Tracing Apps in India' (2021) 11.1 NULJ 1.

(ii) SECTION 69 OF THE IT ACT VIOLATES THE BASIC PRINCIPLES OF PRIVACY

26. It is submitted that the **Requirement of Notice and Consent** which also violate the individual's right to fair trial. Section 4[42] of the DPDP Act provides that personal data be processed only for the lawful purpose for which consent or deemed consent has been given and Section 5[43] of the said Act mandates notice to the Data Principal, specifying the purpose along with the data to be collected. However, Section 69 of the IT Act is in clear contravention of this as it does not recognize the concept of consent for the processing of data. It only mandates the satisfaction of certain grounds mentioned therein to issue Interception orders and neither does mandates for providing notice or purpose of data collection.
27. The **Purpose limitation** principle asks that the State must collect data only for the purpose it has previously stated.[44] The use limitation principle provides that after specifying the purpose of data collection the data collector must not use it for other purposes.[45] Further, the principle of data minimization says that a data fiduciary shall not gather excess data.[46] Storage limitation ensures that once the goal for data acquisition is met, data be removed. Section 69 does not follow any of these.
28. The powers which the executive holds under Section 69 of the IT Act would breach data fiduciary's duty of data security. The decryption process require breaking of end-to-end encryption which would reveal excess information, thereby exposing the users to cybercrimes and violating their fundamental rights under Art. 14, 19, 21[47] of the Constitution of Indica.

(iii) SECTION 69 OF THE IT ACT VIOLATES SECTION 11, SECTION 12 OF THE DATA PROTECTION ACT AS WELL AS THE MANDATE OF THE DATA PROTECTION ACT

29. It is submitted that Section 69 of IT Act violates Sections 11 & 12 of the DPDP Act as well as its mandate. DPDP Act has been enacted to protect the Privacy of the individuals

[42] The Digital Personal Data Protection Act 2023, s 4.
[43] The Digital Personal Data Protection Act 2023, s 5.
[44] MEITY <https://www.meity.govin> accessed on 21 December 2023.
[45] INFORMATION COMMISSIONER's OFFICE <https://ico.org.uk/for-organisations/> accessed on 21 Dec 2023.
[46] DATA PROTECTION COMMISSION, <https://www.dataprotection.ie/en/individuals/> accessed on 21 Dec 2023.
[47] *Akshay N. Patel v RBI* [2022] 3 SCC 694.

and is contravened herein. The right to Privacy has been read to be a Right under Art. 21 of the Constitution of Indica[48] and **without a just and fair procedure established**, it is not possible to safeguard the fundamental rights of citizens under the said Articles.[49]

30. It is submitted that Section 11[50] & 12[51] of the Data Protection Act gives Data Principal the **right to information** regarding the processing of their personal data and the **erasure of data** are no longer being honoured as the data principal has no control over the personal data of the individuals after it is handed over to the instruments of the State.[52] Therefore, vitiating Section 11 and Section 12 of the DPDP Act.
31. Further, it is submitted that Section 81[53] of the IT Act and Section 38[54] of the Data Protection Act suggests that in event of a conflict with any other law, the provision of this act would prevail. Generally, special law prevails over the general legislation[55] but in this case, IT Act is a special law enacted especially to deal with IT-related issues and DPDP Act is enacted especially in furtherance of the Right to Privacy according to the Puttaswamy Judgement. The supremacy of both legislations is, therefore, contradictory.[56]
32. Hence, it is contended that the contradictory nature of legislation with no clear indication of the fact that which legislation would prevail ensues arbitrariness[57] and vagueness in the legislation. Therefore, the Data Protection Act and Section 11 and Section 12 of the Act are infringed upon by Section 69 of the IT Act.
33. We must also highlight that de-encryption, if available easily, could defeat the fundamental right of privacy and de-encryption of messages may be done under special circumstances but it must be ensured that the privacy of an individual is not invaded.[58]

---

[48] *Francis Coralie Mullin v Union Territory of Delhi* [1981] 2 SCR 516.
[49] *People's Union of Civil Liberties v Union of India* [1997] 1 SCC 301.
[50] The Digital Personal Data Protection Act 2023, s 11.
[51] The Digital Personal Data Protection Act 2023, s 12.
[52] Aditya Sarmah, 'Privacy and the Right Against Self-Incrimination: Theorising a Criminal Process in the Context of Personal Gadgets', 3.2 CALQ (2017) 28.
[53] The Information Technology Act 2000, s 81.
[54] The Digital Personal Data Protection Act 2023, s 5.
[55] *R.S. Raghunath v State of Karnataka* [1992] 1 SCC 335; AIR 1992 SC 81.
[56] Supratim Chakraborty, 'Data Protection in India: Overview' (Khaitan & Co. LLP) <https://www.khaitanco.com/sites/default/files/2021-04/Data%20 Protection%20in%20India%20Overview.pdf> accessed on 3 January 2024.
[57] *Central Coalfields Ltd. v State of M.P.* [1995] 2 SCC 11.
[58] *Facebook Inc v Union of India,* 2019 SCCOnline SC 1264.

34. The counsel on behalf submits the abovementioned arguments to that Section 69 of the IT Act is in Violation of Article 20(3) and Article 21 of the Constitution of Indica.[59]

ISSUE 2

WHETHER GOVERNEMNT RESTRICTIONS ON CRYPTOGRAPHIC TECHNIQUES ARE TOO RESTRICTIVE OR NOT

35. The petitioners submit before this Hon'ble Court that the restrictions on cryptographic techniques are too restrictive and therefore, needs to be struck down for the following reasons:

I. MANDATORY REQUIREMENT TO SHARE THE CRYPTOGRAPHIC TECHNIQUES IS MANIFESTLY ARBITRARY

36. The Rules with respect to the use of cryptographic tools requires cryptographic algorithms that were proposed to be used by anyone for any purpose to be submitted to 'The Authority on Control and Regulation of Cryptography'[60].
37. The above requirement is far too restrictive as it mandates such a requirement on anyone using cryptographic tools for any purpose, which is clearly **far too excessive and disproportionate**. It was held by the Supreme Court that delegated legislations that are forbiddingly excessive or disproportionate are **manifestly arbitrary**[61].
38. Additionally, the above-stated mandatory requirements can be stated to be far too restrictive, as it proposes a limitation that is even more restrictive than the licensing agreement between DoT (Department of Telecommunications) & ISPs (Internet Service Providers), an agreement which has been considered a highly restrictive measure with regards to encryption in India[62]. The above agreement states that only encryption standards that are lower than 40-bits can be used without any sort of prior approval or submission[63].

[59] *Toofan Singh v State of T.N.*, [2021] 4 SCC 1.
[60] Moot proposition [20].
[61] *Franklin Templeton Trustee Services (P) Ltd. v Amruta Garg* [2021] 9 SCC 606.
[62] NASSCOM-DSCI, 'Encryption And The Digital Economy: Balancing Security, Privacy, and National Security' [2020].
[63] Department of Telecommunication, Ministry of Communications & Government of India, Licensing Agreement for Unified License [2014].

39. Thus, it is submitted that mandatory requirement to share cryptographic techniques and receive prior approval for them is manifestly arbitrary, and far too restrictive.

II. VIOLATES ARTICLE 19 OF THE CONSTITUTION OF INDIA –

(i) INFRINGES RIGHT TO FREEDOM OF MOVEMENT[64] –

40. Given that most computer sources, such as mobile phones & automated systems in vehicles, include location tracking features and if sec. 69 of the IT Act, 2000 confers upon the government the decrypt any computer source that stores the location data of the owner of the data, it is likely to **have a chilling effect** on the right to freedom of movement. Justice Subba Rao's dissenting judgement in the *Kharak Singh*[65] case, which was later upheld in the *Privacy*[66] judgement, clearly enumerates how surveillance acts as an impediment to the right to freedom of movement guaranteed by Art. 19(1)(d).

(ii) INFRINGES RIGHT TO PRACTICE ANY BUSINESS[67] –

41. The powers conferred upon the government to decrypt all computer resources means that companies can no longer offer complete security on the computer-based products and services offered by them. As was in the case of CG Car Company and other car manufacturers, the powers under Sec. 69 of the IT Act meant that the car companies could no longer offer the security features, a feature that mostly attracted their clients[68]. As a result, it is likely to affect the business of the car manufactures in India substantially, and therefore, Sec. 69 infringes the right to business guaranteed by Art. 19(1)(g) of the Constitution of India.

42. The Apex Court[69] has held that if the multiple entities feel that their profits or business are likely to be affected, then it would not be in the interest of the general public and therefore, an unreasonable restriction. It has also been held that if a restriction imposed is so stringent, that it has the **probability of affecting the ability to practice that said business**, would be deemed an unreasonable restriction[70]. In the present case, since the petition has been filed by multiple car manufacturers as they all feel that Sec. 69 is

[64] Constitution of India, art 19(1)(d).
[65] *Kharak Singh v State of UP & Ors* [1964] SCR (1) 332.
[66] *Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors* [2017] 10 SCC 1.
[67] Constitution of India, art 19(1)(g).
[68] Moot Proposition [20].
[69] *Dwarka Prasad Laxmi Narain v State of Uttar Pradesh & Two Ors* [1954] SCR 803.
[70] *Rustom Cavasjee Cooper v Union of India* [1970] 1 SCC 248; *Mohd. Yasin v Town Area Committee* [1952] 1 SCC 205.

likely to affect their business in India substantially, it can be deemed as an unreasonable restriction, and therefore violative of Art. 19(1)(g).

III. AMOUNTS TO AN UNREASONABLE RESTRICTION –

(i) SEC. 69 PROVIDES FOR EXCESSIVE GROUNDS UNDER WHICH, THE POWERS GRANTED BY SEC. 69 CAN BE EXERCISED –

43. Sec. 69 lists the grounds under which it can exercise the powers conferred by this provision. While most of the grounds listed under this provision are contemplated under Art. 19(2) to 19(6), the provision also provides for certain grounds, i.e. Defence of India & the Investigation of any Offence, that have **not been contemplated anywhere under art. 19(2) to 19(6) as reasonable restrictions**. Thus, it is very clear that the restrictions imposed by Sec. 69 are unreasonable[71], and therefore needs to be struck down.

(A) FAILS THE 'PROPORTIONALITY TEST' –

44. The proportionality test was applied to decide whether or not a restriction under Article 19 is reasonable or not[72]. Relying upon the proportionality test as applied in the *Privacy*[73] judgement, it holds that the measure must not have a disproportionate impact on the right holder. In the present case, it can, in no way, be said that the impact on the right holders, i.e. CG Car Company, other car manufacturers & other intermediaries, as the IT Act places an additional obligation on such intermediaries to extend all forms of technical assistance and facilities to decrypt information on computer sources, even though they are not the owners of the information that is directed to be decrypted and have no connection with the purpose sought to be achieved.
45. Additionally, the proportionality test also requires that the restriction so imposed be the least restrictive measure employed to achieve the said objective[74]. A paper[75] released by the Data Security Council of India (DSCI) about the encryption debate talks about **various alternative and less restrictive measures that could be employed by law enforcement agencies instead of relying upon the surveillance powers[76] under the IT Act**.

---

[71] *Kaushal Kishore v State of Uttar Pradesh & Ors* [2023] 4 SCC 1.
[72] *Anuradha Bhasin v Union of India* [2020] 3 SCC 637.
[73] *Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors* [2017] 10 SCC 1.
[74] *Modern Dental College & Research Centre v State of Madhya Pradesh* [2016] 7 SCC 353.
[75] NASSCOM-DSCI, 'Encryption And The Digital Economy: Balancing Security, Privacy, and National Security' [2020].
[76] Information Technology Act 2000, s 69.

IV. LACK OF JUDICIAL OVERSIGHT

46. The entire power of issuance of a direction for decryption of information from a computer source under Sec. 69 of the IT Act, 2000 lies in the hands of the executive alone. The order can only be issued by the Central or State Government, or a 'Competent Authority[77]', as laid down in the 2009 Rules, which only comprises of members belonging to the Executive. Similarly, the 'Review Committee[78]', that is tasked with reviewing the directions that have been issued for the decryption of information from a computer source consists of members merely belonging to the Executive.

47. The **lack of judicial oversight** in this entire process can lead to an arbitrary exercise of power by the Executive, due to the lack of a system of checks and balances. The importance of judicial oversight has been highlighted in the landmark *Aadhar*[79] and the *Privacy*[80] judgements, which held that judicial oversight in such a surveillance process would be the minimum requirement to pass the test of constitutionality, as the judiciary is the only competent body that has the authority to adjudicate on whether or not the measures adopted is proportionate, and to decide whether or not the least restrictive measure has been applied.

48. The requirement of judicial oversight is also seen in the 'International Principles on the Application of Human Rights to Communication Surveillance'[81], the importance of which was recognised by Justice Nariman in the *Privacy* judgement. Additionally, the problems with the lack of judicial oversight in the surveillance systems have also been enumerated in the Justice A.P. Shah Report[82], which was endorsed in the *Privacy* judgment, and in the Justice B.N. Srikrishna Report[83].

---

[77] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, Rule 2(d).
[78] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 Rule 2(q).
[79] *Justice K.S. Puttaswamy and Anr v Union of India and Ors* [2019] 1 SCC 1.
[80] *Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors* [2017] 10 SCC 1.
[81] International Principles on the Application of Human Rights to Communication Surveillance, 2013, principle 6.
[82] A P Shah, Report of the Group of Experts on Privacy [2012].
[83] B N Srikrishna Committee, *free and fair economy* [2018].

V. SEC. 69 OF THE IT ACT, 2000 DOES NOT PROVIDE ADEQUATE SAFEGUARDS AGAINST THE ARBITRARY MISUSE OF POWER

(i) SEC. 69 DOES NOT NECESSITATE AN OCCURRENCE OF A 'PUBLIC EMERGENCY' –

49. Section 69 of the Information Technology Act, 2000, confers upon the government the authority to issue an order for the decryption of any electronic record, a power that bears a striking resemblance[84], if not greater invasiveness, to the one conferred upon the government by Section 5(2) of the Telegraph Act.
50. In a number of Supreme Court judgements[85], the Courts articulated that the fundamental prerequisite for the government to exercise its powers under Section 5(2) of the Telegraph Act, 2005, is the existence of a public emergency, as explicitly stipulated in the provision.
51. However, a notable distinction arises when examining Section 69 of the IT Act, 2000, which imposes no such requirement. This provision lacks the imperative for the occurrence of a public emergency as a condition precedent for the government to exercise its powers, thereby creating a potential for arbitrary misuse of the authority vested under Section 69.
52. Despite conferring comparable powers to the government as those granted by the Telegraph Act, **it appears illogical and irrational that the IT Act does not institute a higher threshold[86], such as the occurrence of a public emergency, for the government to exercise its powers under the IT Act**[87].
53. A similar position was held by the Apex Court in the case of *Pramod Singla vs. Union of India*[88], which held that arbitrary power of the state must only be exercised in the rarest of rare cases, i.e. the occurrence of a public emergency.

[84] Gaurav Kumar, 'An Analysis of the Pegasus Spyware issue in light of Surveillance Laws and the Right to Privacy in India' (2022) 2.3 JCLJ 827.
[85] *Hukam Chand Shyam Lal v Union of India And Ors* [1976] SCR (2)1060; *People's Union for Civic Liberties v Union of India & Ors* [1997] 1 SCC 301.
[86] Ashutosh Chandra, 'Pegasus - Spyware with Wings as Seen from a Legal Lens' (2022) 2.1 DSNLUJ SCI Tech L 124.
[87] Information Technology Act 2000, s 69.
[88] *Pramod Singla v Union of India* [2023] SCC OnLine SC 374.

VI. VIOLATION OF THE RIGHT TO INFORMATION ACT, 2005

54. Rule 23 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 states that all records pertaining to intercepted, monitored, and decrypted information, including the directions passed to intercept, monitor and decrypt information will be destroyed after a period of six months.

55. However, the following Rule is in contravention to Sec. 4 of the RTI Act, 2005 which requires all public bodies to duly maintain its records[89]. By destroying the records pertaining to the directions issued by the competent authority, including the directions itself, this leads to a denial of information with regards to the due process followed by the 'Competent Authority' & the 'Review Committee' and creates a sense of opacity with regards to their working. By doing so, it is evidently **violating the Right to Information**[90] of the citizens, which has not only been recognized as a statutory right[91], but also a fundamental right[92] that forms a part of the right under Article 19(1)(a).

VII. IN CONTRAVENTION TO THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

56. The Digital Personal Data Protection Act, 2023 requires a data fiduciary to protect the personal data of the data principal, and also implement necessary safeguards to protect it[93]. This would mean that the Data Fiduciary, i.e. CG Car Company, has a duty to protect the personal data of the Data Principal, i.e. Mr. Ian, and this would mean that CG Car Company would be bound to protect the private key unless Mr. Ian consented to the sharing of the private key. Yet, Sec. 69 of the IT Act and the rules made thereunder, imposes a negative obligation on CG Car Company which is **contrary to the duties of a data fiduciary** as put forth in the Digital Personal Data Protection Act, 2023.

---

[89] Right To Information Act, 2005, s 4.
[90] *Indira Nehru Gandhi v Raj Narain* [1975] 2 SCC 159.
[91] Right To Information Act, 2005, s 3.
[92] *Union of India v Association for Democratic Reforms* [2002] (3) SCR 294.
[93] The Digital Personal Data Protection Act, 2023, s 8(5).

VIII. IN CONTRAVENTION TO NON-PERSONAL DATA GOVERNANCE FRAMEWORK[94]

57. The Non-Personal Data Governance framework proposes that the community, i.e. in this case, CG Car Company & Mr. Ian, can exercise rights over non personal data. The rights include the right to derive economic benefit and other value, and the right to eliminate or minimize the harms from the data to the community. Thus, the obligation imposed by Sec. 69 of the IT Act is in **contravention to the rights proposed by the Non-Personal Data Governance framework**.

IX. INSTITUTIONAL INEFFICIENCY OF COMPETETENT AUTHORITY AND REVIEW COMMITTEE UNDER SEC. 69 OF IT ACT, 2000

58. The Competent Authority under Sec. 69 of the IT Act, 2000 and Sec. 5(2) of the Telegraph Act, 2005 issues nearly 10,000 directions for interception, monitoring and decryption under the IT Act and the Telegraph Act every month[95]. This is a substantially large number of orders, which indicates an abuse of power under the following acts, without adequately ensuring that they are exercising the least restrictive measure, which they are required to do so as per the rules[96] made under Sec. 69 of the IT Act. Additionally, the Review Committee has the responsibility of meeting at least once every two months and ensuring that the directions issued by the Competent Authority is in accordance with the impugned provision and the rules made thereunder[97]. The Review Committee also has an unrealistic target of reviewing nearly 20,000 orders every meeting.[98]
59. The above numbers **cast serious doubts on the efficiency and validity of the powers exercised under the IT Act**. This, coupled with the fact that there is a lack of judicial overview, means that the powers conferred under Sec. 69 of the IT Act operate in an overly restrictive manner.

---

[94] Report by the Committee of Experts on Non-Personal Data Governance Framework [2020].
[95] SFLC.IN, 'Surveillance – Is There A Need For Judicial Oversight?', (SFLC.IN, 25 September 2013) https://sflc.in/surveillance-there-need-judicial-oversight/ accessed 4 January 2024.
[96] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 8.
[97] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 22.
[98] B N Sri Krishna Committee, *free and fair economy* [2018].

PRAYER

Wherefore, in light of the issues raised, arguments advanced, and authorities cited, it is most humbly by the counsel of respondents and respectfully prayed before this Hon'ble Court to:

1) Section 69 of the Information Technology Act, 2000 is **not constitutionally valid.**
2) Governmental control over the use of cryptographic techniques is **excessively restrictive** in nature.

AND/OR

Pass any other order it may deem fit, in the interest of Justice, Equity and Good Conscience.

All of which is most humbly and respectfully submitted.