TL-09

4TH SURANA & SURANA AND CAUSAT SCHOOL OF LEGAL STUDIES,

DR. AT MARKOSE MEMORIAL TECHNOLOGY LAW

MOOT COURT COMPETITION, 2024

19TH JANUARY – 21ST JANUARY 2024

BEFORE THE HON'BLE SUPREME COURT OF INDICA

In the clubbed matter of:

CG CAR COMPANY AND OTHERS — **PETITIONERS**

V.

UNION OF INDICA — **RESPONDENT**

PETITION UNDER ARTICLE 32 OF THE CONSTITUTION OF INDICA

UPON SUBMISSION TO THE HON'BLE CHIEF JUSTICE AND HIS LORDSHIP'S COMPANION JUSTICES OF THE HON'BLE SUPREME COURT OF INDICA

Written Submission on behalf of the Respondent

Counsel for the Respondent

TABLE OF CONTENT

INDEX OF AUTHORITIES

STATUES

CASES

BOOKS

OTHER SOURCES

STATEMENT OF JURISDICTION

The Respondents are responding to the petition filed by the petitioner below mentioned. Hon'ble Supreme Court has the power to issue writs-

Article 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

STATEMENT OF FACTS

In the Southern part of Asian Sub Continent, the Republic of Indica has State of Antartaka as the most developed state of the country. It is famous for its growth of the Information Technology sector and the city of Singaluru is often referred to as Silicon Valley of Indica. The body of Mr. Parth was found lying in a pool of blood beside his car, on the side of State Highway No. 106 by a family around 7:00 am on 13th August 2022. The investigative officers sent the body to Government Hospital after the necessary formalities and inquest were fulfilled.

After preliminary investigation the suspicion was on Mr. Ian as the time estimated of the death of Mr. Anand was same as the time when the SUV, CG-Metron of Mr. Ian passed through the State Highway. The suspicion on Mr. Ian is bolstered as his vehicle took longer time for covering the distance, compared to the other vehicles. It was found that Mr. Ian and Mr. Anand used to frequent the same eatery. During investigation, Mr. Ian answered all the question posed without any dispelling doubt but couldn't give a satisfactory reason for his travel during the specified time. His car was confiscated by police to check the movement and other details of the vehicle as it had ICT facilities.

The investigative officers found that the data was secured by password and needed private key to decrypt it. By exercising the power given by "The Authority on Control and Regulation of Cryptography" asked for the private key to which he declined stating that it is an self-incriminating evidence under Art.20(3). Police officers after following the procedure contacted Headquarters of CG Metron for the copy of key to which they denied stating that the security of the data is their trade secret. Police tried to hack into the system off the records to investigate and failed. They proceeded against CG Metron and Mr. Ian under S. 69 of IT Act, 2000. Mr. Ian challenged it in 482 CrPC before HC for infringement of privacy and CG Metron filed a writ in SC contending S. 69 and rules of "The Authority" to be unconstitutional. SC Clubbed the matters.

STATEMENT OF ISSUES

-ISSUE 1-

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

-ISSUE 2-

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

SUMMARY OF ARGUMENTS

1. WHETHER S.69 OF THE INFORMATION TECHNOLOGY ACT, 2000 IS CONSTITUTIONALLY VALID?

The Section 69 of the Information and Technology Act, 2000 is constitutionally valid as S.69 acts within the framework of the constitution not in contravention of any fundamental right as the section provides for reasonable intrusion of privacy providing definite rules. S.69 provides for reasonably defined circumstances within which the imposition can be placed and further a definite time period provided by the rules established for the retaining of such data. S.69 also provides for reasonable proportionate stand for decryption of the encrypted data for definite goal. Hence, it proves that section 69 is constitutionally valid.

2. WHETHER GOVENRMENTAL CONTROL OVER THE USE OF CRYPTOGRAPHIC TECHNIQUES IS TOO RESTRICTIVE IN NATURE?

The Governmental Rule in question here, is the rule of 13 August 2022. The rule mandated that the cryptographic algorithms that are used by anyone for any purpose were to be submitted to "The Authority on Control and Regulation of Cryptographic" and the prior approval of the Authority was necessary for using the same. The Authority is to be provided with a copy of keys that could be used for decrypting and they were bound to share the keys with the government on demand. *In casu,* Mr. Ian's phone is confiscated by police and he is being asked by them to tell his private key to which he has denied. Police here is trying to investigate him as he is under suspicion regarding murder of Mr. Anand as during investigations he is unable to give a satisfactory reason about his car's driving speed near the alleged crime scene. As such the government's control over the cryptographic technique is not restrictive in nature.

ARGUMENT ADVANCED

1. WHETHER S.69 OF THE INFORMATION TECHNOLOGY ACT, 2000 IS CONSTITUTIONALLY VALID?

The counsel would like to most humbly present before this hon'ble court that S.69 stands constitutionally valid and as the apex court has attained the role as that of a "sentinel on the qui vive."[1]. The above stated issue shall be dealt under three limbs- **[1.1]** *S.69 is not in contravention to the Fundamental Rights* **&** **[1.2]** *The test of constitutionality is not being tarnished by the impugned legislation.*

1.1. S.69[2] is not in contravention to the Art 14[3], 19[4] & 21[5]

A statute can be struck down when it is arbitrary or unreasonable[6], in relation to the constitutional provision such as, Art 14, 19 or 21.[7] S.69 is not infringing any of the rights mentioned above and is supported by unambiguous and rational approach to achieve a welfare state in the technologically advanced society. In ***Balwant Singh v. Commr of Police***[8] it is asserted that constitution casts a duty upon the State to protect the fundamental right guaranteed to the citizen and make the same available to the individual, subject to reasonable restriction. In casu S.69 provides for a reasonable standard for monitoring, encryption and decryption of data as per the necessities established under S.69(1). ***Renu v. District and Sessions Judge***[9] it was stated that power has to be exercised by authorities within the framework of constitution. And in ***State of West Bengal v. Committee for protection of Democratic Rights, West Bengal***[10] it was upheld that

[1] *State of Madras v VG Row* (1952) SCR 597.
[2] The Information Technology Act 2000, s 69.
[3] The Constitution of India 1949, art 14.
[4] The Constitution of India 1949, art 19.
[5] The Constitution of India 1949, art 21.
[6] *The Collector of Customs, Madras v Nathalla Sampathu Chetty & Anr* (1962) 3 SCR 786.
[7] *District Registrar and Collector v Canara Bank* (2005) 1 SCC 496.
[8] *Balwant Singh v Commr. of Police* (2015) 4 SCC 801.
[9] *Renu v District and Sessions Judge* (2014) 14 SCC 50.
[10] *State of West Bengal v Committee for protection of Democratic Rights, West Bengal* (2010) 3 SCC 571.

the state shall not enact any law which either takes away or abridges a fundamental right. Art 13[11] is a protective provision which enshrines Fundamental Rights[12]. In casu, S.69 acts within the framework of the constitution not in contravention of any fundamental right as the section provides for reasonable intrusion of privacy providing definite rules.

1.1.1. S.69 does not stand in contravention to the Art. 14

The cardinal rule is that the state action must not be arbitrary[13] to stand valid however, may have reasonable restrictions is controlled discretion to achieve the balanced of the political society. ***Bachan Singh v. State of Punjab***[14] stated that rule of law which permeates the entire fabric of the Constitution excludes arbitrariness. If there is any arbitrariness there will be absence of rule of law.[15] However, as stated in ***Federation of Railway officers Association v. UOI***[16]**,** if there is a controlled discretion as such exclude arbitrariness. In casu, S.69 provides for a definite approach to regulate the monitoring of encrypted data as per the need of S.69(1)[17].

It was stated in ***Naraindas v. State of Madhya Pradesh***[18] that if there is no principle to guide the power of the statute, the latter will stand arbitrary in nature. S.69, holds no arbitrariness with proper rules established for its application in defined scenario, as per S.69(1), having a rational approach behind monitoring of encrypted data.

1.1.2. S.69 stands reasonable and not in contravention to Art. 19(1)(a)[19]

The Fundamental freedom enumerated under Art. 19(1)(a) are not absolute in nature, rather they are subject to reasonable us per Art.19(2). ***Gujarat Water Supply v. Unique Electro (Gujarat)(P)***[20] stated that there is no precise definition to "reasonable". Further as stated in ***Krishnan Kakkanth***

[11] The Constitution of India 1949, art 13.
[12] *Ramlila Maidan IncidTent v Home Secretary, UOI* (2012) 5 SCC 1.
[13] M P Jain, *Indian Constitutional Law* (8th edn, LexisNexis 2023) 941.
[14] *Bachan Singh v State of Punjab* (1982) AIR 1982 SC 1336.
[15] M P Jain, *Indian Constitutional Law* (8th edn, LexisNexis 2023) 941.
[16] *Federation of Railway officers Association v UOI* (2003) 4 SCC 289.
[17] The Information Technology Act 2000, s 69 cl 1.
[18] *Naraindas v State of Madhya Pradesh* (1974) 4 SCC 788.
[19] The Constitution of India 1949, art 13 cl (1) sub cl (a).
[20] *Gujarat Water Supply v Unique Electro (Gujarat)(P)* (1989) 1 SCC 532.

v. State of Kerala[21] while adjudging "reasonableness of restriction"[22], certain factors such as, the duration, extent of the restriction, the circumstances under which that imposition has been authorised, need to be looked into. *In casu*, S.69 provides for reasonably defined circumstances within which the imposition can be placed and further a definite time period provided by the rules[23] established for the retaining of such data.

In ***Pathumma v. State of Kerala***[24]**,** it was stated that while interpreting a constitutional provision the court should keep in mind the social condition, the needs of the nation and the problems of day-to-day life of the people and how the legislature seeks to solve the same problem. *And the limitation should be required w.r.t interest of the general public.*[25] S.69 provides for its application in times of maintaining public order and other mentioned times of need and being in a technologically advanced society the same needs to be regulated.

1.1.3. The impugned section doesn't approve unreasonable surveillance contravening Art 19(1)(d)[26]

"Since pre independence time police surveillance has been placed upon person suspected of criminal tendencies."[27] S.69 provides for breach of data privacy only upon such individual where it is expedient for the purpose of S.69(1). In ***Kharak Singh v. State of Punjab***[28] surveillance was not covered under Art 19(1)(d). However, in ***Govind v. State of Madhya Pradesh***[29] it was held that surveillance shall be restricted upon such individual suspected to lead a life of crime; and the police can maintain careful surveillance over potential offenders of law, as stated in ***Malak Singh***

[21] *Krishnan Kakkanth v State of Kerala* (1997) 9 SCC 495.
[22] *A.K. Gopalan v The State of Madras* (1950) SC 27.
[23] The Information Technology (Procedure and safeguard for interception and decryption of information) Rules 2009, s 11.
[24] *Pathumma v State of Kerala* (1978) 2 SCC 1.
[25] *MRF Limited v Inspector Kerala Government* (1998) 8 SCC 227.
[26] The Constitution of India 1949, art 13 cl (1) sub cl (d).
[27] M P Jain, *Indian Constitutional Law* (8th edn, LexisNexis 2023) 1105.
[28] *Kharak Singh v State of U.P*. (1964) 1 SCR 285.
[29] *Govind v State of Madhya Pradesh* (1975) 2 SCC 148.

v. State of Punjab[30]. S.69 nowhere supports unreasonable surveillance but rather a definite approach within a defined time limit and for a particular purpose to regulate the technological space.

1.1.4. <u>The impugned Section is not infringing Art 19(1)(g)</u>[31]

A regulation is challengeable for directly interfering with the exercise of freedom of trade.[32] However, as per, ***Sreenivasa General Traders v. State of Andhra Pradesh***[33] in order to determine the reasonableness of restriction, the nature of business, the prevailing conditions of the trade, must be taken into consideration. *In casu,* intrusion of privacy is only reasonably exercised by S.69 in *times of need*, which essentially requires the monitoring of encrypted data for prevailing justice and maintaining law and order, as such not interfering in the functioning of business.

1.1.5. <u>The impugned Section is not in contravention to Art 21</u>

In ***Maneka Gandhi v. UOI***[34]**,** that Art 14, 19, 21 are not mutually exclusive but mutually inclusive. In ***Dist. Registrar and Collector v. Cannara Bank***[35] interference with personal liberty of a person is detected there is a procedure to be followed and it should be tested w.r.t Art 19 and 14. S.69 provides for the procedure established by law to infringe the privacy of the individual provided under the rules. *There should be genuineness of complaint and reasonable belief as to a person's complicity for placing a person under arrest and not just suspicion.*[36] *In casu,* arrest is based upon the assertion that Mr. Ian was not to state as to why he was on the route where the incident took place which creates reasonable belief for arrest. The apex court upheld in ***Justice KS Puttaswamy v. UOI***[37] that invasion in privacy must satisfy the triple test of legality, legitimate aim and

[30] *Malak Singh v State of Punjab* (1981) 1 SCC 420.
[31] The Constitution of India 1949, art 13 cl (1) sub cl (g).
[32] M P Jain, *Indian Constitutional Law* (8th edn, LexisNexis 2023) 1114.
[33] *Sreenivasa General Traders v State of Andhra Pradesh* (1984) 4 SCC 353.
[34] *Maneka Gandhi v UOI* (1978) 1 SCC 248.
[35] *Dist. Registrar and Collector v Canara Bank* (2005) 1 SCC 496.
[36] M P Jain, *Indian Constitutional Law* (8th edn, LexisNexis 2023) 1178.
[37] *Justice KS Puttaswamy v UOI* (2017) 10 SCC 1.

proportionality, establishing a rational nexus. S.69 has the legality as it provides for the reasonable breach of privacy without affecting the data privacy of the individuals

The impugned legislation has a legitimate aim not infringing anyone's livelihood. It is a settled law[38] that right provided under Art 19 are available exclusively for the natural citizen and not for corporation[39]. *In casu,* the case has been brought by corporations and as such no right is provide under Art 19 to corporation as such. And the customer shall understand the need of this S.69 in todays-time where offences are not just concerned with the physical world but also the virtual interface and the same is required for their welfare only. And as such the same shall not indirectly affect the business dealing in encrypted data rather make them

The impugned S.69 provides for the needed proportionality for building the rational nexus. As stated in ***Maneka Gandhi v. UOI,[40]*** Art.21 signifies that the procedure established by law to deprive a person of his personal liberty must be "reasonable, fair and just". S.69 provides for a definite ground, which are much established in their senses with the required procedural safeguard, while dealing with the privacy of encrypted data and hence, providing no arbitrary intrusion. Also, the decryption of data is required[41] only because of the inference that this data could help in the investigation of murder of Mr. Anand[42] thus upholding law and order; and administration of justice

1.2 S.69 is not in violation of Art 20(3)[43] of the Constitution

The impugned S.69 doesn't stand as a medium to justify self-incriminatory evidence but rather as a medium to regulate the encrypted data. In ***Ajay Bhardwaj v. UOI[44],*** stated that the petitioner should cooperate with the investigating officer w.r.t the disclosure of password. Earlier in

[38] *State Trading Corp. v C.T.O.* (1964) (4) SCR 99.
[39] *Dharam Dutt v UOI* (2004) 1 SCC 712.
[40] *Maneka Gandhi v UOI* (1978) 1 SCC 248.
[41] Moot Proposition [15].
[42] Moot Proposition [9].
[43] The Constitution of India 1949, art 20 cl 3.
[44] *Ajay Bhardwaj v UOI*

Virendra Khanna v. State of Karnataka and Ors[45], mere direction to provide password was held to not amount to testimonial evidence, as it is for the investigating officer to prove and establish the same in the court of law. *In casu*, Mr. Ian or the company being asked to submit the decryption key[46] is all for the cooperation with the investigation of a murder[47] and further the same data needs to be proved whether tending towards culpability or not. It shall be proved in reference to ***Sec 79A***[48]***,*** which provides for formation of examiner of electronic evidence, who provides expert opinion on the electronic form of evidence before any court.

In ***Greater Manchester Police v Andrews***[49]***,*** the EWHC stated that the privilege against self-incrimination is available to a very limited extent and it was proportionate of him to give up the key. ***S.51(4), RIPA, 2000***[50] provides if under proportionate circumstances the notice to disclose the key is not given, the purpose would be defeated. S.69 provides for a proportionate standard for the monitoring of encrypted data where the application of S.69 shall take place as per S.69(1).

In ***R v. Padellec***[51]***,*** individual was jailed for the refusal of production of password to the encrypted file. S.69 also provides for reasonable proportionate stand for decryption of the encrypted data for definite goal, as in casu the same is being exercised to investigate the suspicious presence of Mr. Ian at place of occurring.

In the US Court of Circuit ***United States of America v Gavegnano***[52] stated the **foregone conclusion doctrine**[53] which proved that appellant was the sole user of the computer and as such sharing of password and retrieving data shall not be incriminating testimony. *In casu*, the data is

[45] *Virendra Khanna v State of Karnataka & Ors* (2021) SCC OnLine Kar 5032
[46] Moot Proposition [17].
[47] Moot Proposition [15].
[48] The Information Technology Act 2000, s 79A.
[49] *Greater Manchester Police v Andrews* (2011) EWHC 1966 (Admin).
[50] RIPA 2000, s 51 cl 4.
[51] *R v Padellec* (2012) EWCA Crim 1956.
[52] *United States of America v Gavegnano* (CRIMINAL NO. 3:05cr00017 (W.D. Va. Mar. 15, 2007).
[53] *Fisher v United States* 1976 425 U.S. 391 (1976).

not self-incriminatory as it is being asked from the car[54] that is used by Mr Ian himself which shall be further proved.

In the Canadian Court ***R v. Beauchamp[55],*** a balanced approach was given which enable the defence to disclose the key so that both parties will have access to the plain text material. *In cas*S.69 provides for balanced equation for both the parties to have much needed access, where one party is only gaining access to same at definite times of necessity, as provided under S.69(1) as needed on the present case for interrogation[56].

1.3. The fundamental rights are not being infringed by the impugned legislation

In ***Bachan Singh v. State of Punjab[57]*** it was held that the court generally leans towards the premise that the legislature understands the need of the people and enact laws with a reasonable purpose and they would not deliberately defy constitutional safeguard. S.69 has its presence to provide an instrument for regulating the encrypted data, as the same shall be used for the detriment of the nation and maintenance of law and order.

1.3.1. The "effect and consequence" of the legislation aligned with the Constitution

Express Newspaper v. UOI[58] stated that unless the disadvantages were the direct and inevitable consequence of the legislation, it cannot be stuck down. In ***Maneka Gandhi v. UOI[59],*** the test of "direct and indirect effect" was used to determine whether there was violation of freedom of occupation. *In casu,* no disadvantage shall come in furtherance of the application of S.69 as its consequence as it provides for definite degree of encroachment[60] of encrypted data stored for the reasonable intrusion of privacy, protected under the framework of Art 19 and 21 the reasonable restrictions upon those.

---

[54] Moot Proposition [17].
[55] *R v Beauchamp* 2000 SCC 54.
[56] Moot Proposition [14].
[57] *Bachan Singh v State of Punjab* (1982) 3 SCC 24.
[58] *Express Newspaper v UOI* (1985) SCR (2) 287.
[59] *Maneka Gandhi v UOI* (1978) 1 SCC 248.
[60] *Man Singh v State of Punjab* (1985) 4 SCC 146.

1.3.2. <u>The "pith and substance" test proves its reasonable nature</u>

The SC laid down in ***State of Bombay v. Balsara***[61]**,** the test of pith and substance, where the main object, scope and effect of its provision establishes "true nature and character"[62]. S.69 in true nature and character provides for maintaining law and order and efficient regulation of encrypted data and monitoring of same under rules and safeguards provided without any unreasonable access to encrypted data.

1.3.3. <u>Indirect Judicial Review provides for the constitutionality of S.69</u>

BR Enterprises v. State of Uttar Pradesh[63] it was held that court must take the dynamic meaning into consideration which shall uphold the validity of the provision. And as per ***The Mysore State Electricity Board v. Bangalore Woolen, Cotton and Silk Mills Ltd***[64]**.**if there are two interpretations to a legislation available the court must prefer that interpretation which renders it constitutional. S.69 interpretation provides for monitoring encrypted data in essential times of needed regulation provided under S.69(1) and also provided investigation in such offences where these data can have evidentiary value.

Hence, the counsel humbly submits before this hon'ble court that in the light of the above arguments S.69 stands constitutionally valid as it nowhere results in the infringement of Fundamental Rights or any other constitutional framework.

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

The counsel would like to most humbly submit before the Hon'ble SC that the rules, notified on 13th August 2022, mandated by the "Authority" in the regulations, regarding the restrictions on cryptographic algorithm do not stand disproportionately restrictive. The regulation invading the

[61] *State of Bombay v Balsara* (1951) SCR 682 (708).
[62] *EV Chinnaiah v State of AP* (2005) 1 SCC 394.
[63] *BR Enterprises v State of Uttar Pradesh* (1999) 9 SCC 700.
[64] *The Mysore State Electricity Board v Bangalore Woolen, Cotton and Silk Mills Ltd* (1963) SC 1128.

data privacy of the individual shall be tested for proportionality using the triple test[65] by establishing the **[2.1]** The rule is in consonance with constitutional principles, **[2.2]** The rule is not self-incriminatory **[2.3.]** Possibility of the rule being abused is no ground question its validity and **[2.4]** Security of State is of paramount importance.

2.1. The Rule is in consonance with fundamental rights

In the case of ***K.S. Puttasawamy v. UOI***[66], Sanjay Kishan Kaul J. opined that it is wrong to consider that the concept of the supervening spirit of justice manifesting in different forms to cure the evils of a new age is unknown to Indian history. Lord Shri Krishna declared in Bhagwat Geeta[67] thus:

परित्राणायसाधूनां विनाशायचदुष्कृताम्। धर्मसंस्थापनार्थाय सम्भवामि युगे युगे ||

The meaning of this profound statement, when viewed after a thousand generations is this: That each age and each generation brings with it the challenges and tribulations of the times. But the Supreme spirit of Justice manifests itself in different social situations, as different values to ensure that there always exists the protection and preservation of certain eternally cherished rights and ideals.

The deflection of 'Brooding spirit of the law', 'the collective conscience', has found mention in the ideals enshrined in inter- alia, Article 14 and 21, which together serve as the heart stones of the Constitution. The spirit that finds enshrinement in these articles manifests and reincarnates itself. In ways and forms that protect the needs of the society in various ages, as the values of liberty, equality, fraternity, dignity, and various other Constitutional values and principles. It always grows stronger and covers within its sweep the great needs of the times. This spirit can neither remain dormant nor static and can never be allowed to fossilise.

---

[65] *Justice KS Puttaswamy v UOI* (2017) 10 SCC 1.
[66] *Justice KS Puttaswamy v UOI* (2017) 10 SCC 1.
[67] The Bhagavad Gita, Chapter 4, Text 8

Therefore, with the changing times and changing needs the need to curb crimes and to ensure peace and justice also changes with time as there is an imminent number of cases involving evidence in the shape of content found on digital devices such as phones, cars etc. which the accused persons are asked to decrypt/ unlock at the behest of investigation agencies consequently the need for the rule like "The Authority".

2.2. The rule is not self-incriminatory

The observed factor is that non-testimonial pieces of evidence[68] have no independent incriminatory nature, but simply aid the investigating agencies in investigating and connecting the dots.[69] *In casu,* investigative officer has asked for private key from Mr. Ian for investigation purposes to find out if he was a participant in the murder of Mr. Anand.

2.2.1 The data to be retrieved by investigation officers is non-testimonial in nature

Decryption key provided to state for investigation of the encryption is required to use merely to know the contents of the physical act and could not be fairly characterised as a that would be nontestimonial in nature. Hence in the present case we can conclude that the Mr. Ian's reluctance in decryption and production of the said data would be tantamount to the testimony of himself having the knowledge of presence at the location. The same is the decision in ***U.S. v. Doe***[70] where the accused took the Fifth Amendment privilege against self-incrimination and refused to decrypt the same and thus was held in civil contempt. The same is an observed fact in the case of ***Ajay Bharadwaj***[71] as well.

2.2.2. No reasonable expectation of breach of privacy involved

Supreme Court of Canada held that the use of thermal imaging by the police in the course of an investigation of a suspect's property did not constitute a violation of the accused's right to a

[68] *State v. Diamond*. 905 N.W.2d 870 (Minn 2018)
[69] *State of Bombay v Kathi Kalu Oghad & Ors.*(1961) AIR 1961 SC 1808.
[70] *US v Doe* 465 U.S. 605 (1984)
[71] *Ajay Bharadwaj v UOI*

reasonable expectation of privacy under Section 8 of the Canadian Charter.[72] On the reasonable expectation of privacy, it was held that the totality of circumstances need to be considered with particular emphasis on both the existence of a subjective expectation of privacy, and the objective reasonableness of the expectation. Here, in the present case, the reason for investigation is the cold-blooded murder of Mr. Anand, the suspicion is on Mr. Ian for the same. The sole reason of investigation and need of decryption is to determine his participation in the crime and that cannot amount to encroachment in his right to privacy.

2.2.3. Search and seizure of devices by authorities is justified

In the words of **Langa J.** in ***Hyundai Motor Distributive*** case, "*Search and seizure provisions, in the context of a preparatory investigation, serve an important purpose in the fight against crime. That the state has a pressing interest which involves the security and freedom of the community as a whole is beyond question. It is an objective which is sufficiently important to justify the limitation of the right to privacy of an individual in certain circumstances*." To authorise search and seizure for preparatory investigation. [73] The Court held that what the perimeter search violated the Charter[74] and that the seizure of consumption records was not in violation of Section 8[75]. This decision was based on the ground that the pattern of electricity consumption revealed as a result of computer investigations could not be said to reveal intimate details since "electricity consumption reveals very little about the personal lifestyle or private decisions."[76] The same instance is in the present case, where the investigative officers are only demanding private key to decrypt the data stored by car in electronic modules of driving, vehicle condition, braking, accelerating related data which is related to locomotive objective and hence cannot reveal intimidate details of the driver.

[72] *Her Majesty, The Queen v Walter Tessling*, (2004) SCC 67.
[73] *Investigating Directorate: Serious Offences v Hyundai Motor Distributors Ltd* (2001) (1) SA 545 (CC)
[74] Canadian Charter of Rights and Freedom 1981.
[75] Canadian Charter of Rights and Freedom 1981, s 8.
[76] *United States v Miller*, 425 us 435 (1976).

Hence, the data retrieved will only benefit in investigative aspect of the case without encroaching right to privacy.

2.3. Possibility of the rule being abused is no ground question its validity

The Apex Court has observed in ***The Collector of Customs, Madras v. Nathella Sampathu Chetty & Anr.***[77] that the possibility of the abuse of the powers under the provisions contained in any statute is no ground for declaring the provision to be unreasonable or void. As the comments of the judgement in Court of Appeal of Northern Ireland ***Viscount Simonds*** observed "if *such powers are capable of being exercised reasonably it is impossible to say that they may not also be exercised unreasonably*" and this cannot be sole reason to determine its invalidity.[78] The same must be followed in the present case as well with the augment of rule "The Authority", the Government here as well, is committed to *Right to Privacy* and other rights ensured in Part III and the impugned rule is not to curb any of the rights, however, it would be used only when excessed are perpetrated by persons on the right of others.[79] As, in the present case, Mr. Ian is only being investigated when he became a suspect in the murder case of Mr. Anand and the private key of his device only to determine his participation in crime.

a. Security of State is of paramount importance

Laws requiring registration and government approval of encryption tools reverse the well-established presumption that States bear the burden of justifying restrictions on these rights.[80]The security environment not only in our country, but throughout the world makes the safety of persons and the State a matter to be balanced against this right to privacy.[81]The growth and development of technology has created new instruments for the possible invasion of privacy by

[77] *The Collector of Customs, Madras v. Nathella Sampathu Chetty & Anr* (1962) 3 S.C.R. 786.
[78] *Belfast Corporation v O.D. Commission* (1960) AC 490.
[79] *Shreya Singhal v UOI* (2015) 5 SCC 1.
[80] Computer Crimes Act, Jan. 23, 2010 <https://www.unodc.org/res/cld/document/computer-crimes-act_html/Computer_Crimes_Act.pdf.> accessed 01 January 2023.
[81] Tom Goodwin 'The Battle is for Customer Interface.'<https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle--is-all-for-the-customer-interface/> accessed 28 December 2023.

the State, including through surveillance, profiling and data collection and processing. Surveillance is not new, but technology has permitted surveillance in ways that are unimaginable.

2.3.1. The Rule is vital to curb threat to national security

In USA, States are utilizing technology in the most imaginative ways particularly in view of increasing global terrorist attacks and heightened public safety concerns.[82] Following a 2015 attack in ***San Bernardino, California,*** that left 14 people dead, the U.S. FBI[83] sought to compel Apple to create software that would disable security features on the suspect's iPhone. The FBI ultimately withdrew its request when it secured access to the cell phone data with the assistance of an unidentified third party. However, the dispute highlighted how security vulnerabilities introduced on a single device and for a specific investigation could nevertheless be exploited to compromise all devices of the same model or type for protection of state.[84]

In 2017, ***Australia*** announced its intention to introduce cybersecurity legislation that would "impose an obligation upon device manufacturers and service providers to provide appropriate assistance to intelligence and law enforcement on a warranted basis."[85] ***China's*** 2016 Cybersecurity Law requires network operators to "provide technical support and assistance" to state and public security organs for the purposes of national security and law enforcement.[86]Since, the similar law/ rules/regulations has been deliberated by various countries for national security and investigative purposes in prior years than the rule was enacted. The main purpose of these rules is not to infringe rights enshrined in Part III but to aid in investigative purposes and serving a

[82] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[83] Federal Bureau of Investigation, America.
[84] See Letter to U.S. Judge Regarding Seizure of Mobile Phone and Search Warrant (March 2, 2016), <https://freedex.org/wpcontent/blogs.dir/2015/files/2017/08/Letter_from_David_Kaye_UN_Special_Rapporteur_on_the_promotion_and_protection_of_the_right_to_freedom_of_opinion_and_expression.pdf.> accessed 06 December 2023.
[85] See Prime Minister, National Security Statement (21 December 2023) <https://www.pm.gov.au/media/national-security-statement> accessed 20 December 2023.
[86] Cybersecurity Law 2023, Art. 28 (China) <https://www.chinalawtranslate.com/cybersecuritylaw/?lang=en.> accessed 01 January 2024.

larger role i.e. to maintain peace and security of the state. Hence, the rule mentioned in "The Authority" cannot be termed as "too restrictive".

2.3.2. Trade Right of CG Metron is in jeopardy in State

Here is the list of countries that has enacted laws to access data of the companies for security, investigation of cognizable offense, purposes- In the **United States**, the Department of Justice reportedly sought to compel software companies to hand over their source code and private encryption keys to government authorities under gag order.[87] In **South Korea**, for example, law enforcement is permitted to access customer identity data held by telecommunications providers without a warrant.[88] In **Russia,** providers of communications services have been forced to disclose the identity of users under government investigation.[89]

As the 2015 Report emphasized, key escrows increase the risks of hacking, attacks and other forms of misuse that undermine users' security and privacy.[90] In 2016, Russia adopted the "**Yarovaya Law**" (Federal Law No. 375-FZ), which also requires authorities to certify the use of encryption technology[91] and establishes administrative penalties for the use of non-certified encryption equipment.[92] Such requirements raise the prospect of direct interference with the ability to use encryption tools without enabling government intrusions through backdoors or other vulnerabilities. At the request of the government, a district court in the Russian Federation issued a ruling blocking access to Telegram, a popular messaging app, after the company refused to

[87] Bruce Schneier, Companies Handing Source Code Over to Governments (*Schneier,* 18 December 2023) <https://www.schneier.com/blog/archives/2016/03/companies_handi.html.> accessed 25 December 2023.
[88] Intervention Submission to Korean Court Regarding Law Enforcement and Anonymity <https://freedex.org/wp-content/blogs.dir/2023/files/2023/05/2023Heonma388-English.pdf> accessed 19 December 2023.
[89] Freedom on the Net 2017, Freedom House <https://freedomhouse.org/report/freedom-net/2017/russia.> accessed 02 January 2024.
[90] Electronic Transactions and Cyber Security Act, 2016 ss. 52, 53 <https://www.malawilii.org/mw/legislation/act/2016/33> accessed 20 December 202.
[91] Overview of the Package of Changes into a Number of Laws of the Russian Federation Designed to Provide for Additional Measures to Counteract Terrorism, The International Centre for Not-for-Profit Law <http://www.icnl.org/research/library/files/Russia/Yarovaya.pdf.> accessed 18 December 2023.
[92] *Id.*

provide encryption keys to the government as may be required under the "Yarovaya Law."[93] This ruling follows a Constitutional Court decision that effectively eliminates the need for a judicial warrant to review and analyse information stored on electronic devices "seized during the course of investigative activities."[94]

As, in the present case, the company has outrightly denied from contributing with the investigation and has not provided the key of their cryptographic algorithms and defied the rules for which it can be penalised. In the present case, when investigation of a cognizable offence such as murder, and public security is in question then it is the duty of company to cooperate with state.

Therefore, in the light of the issues raised and arguments advanced, the rules enacted by Central Government in "The Authority" are only concentrated towards smooth ensuing of law and order in society, hence cannot be categorised as "too restrictive" in nature.

[93] Joint Commc'n to Russia Regarding Amendments to Criminal Code <http://www.ohchr.org/Documents/Issues/Opinion/Legislation/RUS_7_2016.pdf.> accessed 23 December 2023.
[94] Peter Roudik, Russia: No Warrant Needed for Chat and Email Eavesdropping <http://www.loc.gov/law/foreign-news/article/russia-no-warrant-needed-for-chat-and-emaileavesdropping.> accessed 19 December 2023.

PRAYER

Wherefore, may it please the Hon'ble Supreme Court of Indica, in the light of facts and circumstances, the issue presented, arguments advanced, and authorities cited, the Respondent prays that this Hon'ble Court may be pleased to adjudge, rule upon and declare the following-:

1. That Section 69 of the Information Technology Act, 2000 is constitutionally valid.
2. That governmental control over the use of cryptographic techniques is not too restrictive in nature.

And pass any such order that this Hon'ble Court deems fit in the interest of justice, equity and good conscience.

Rest is left to this Hon'ble Court's wisdom and fine sense of judgment.

All of which is respectfully affirmed and submitted

(Counsels on behalf of Respondent)