Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2023 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rishikesh Dave; Publisher – Ayush Pandey

A Constitutional Scrutiny of the 'First Originator Clause' of Information Technology Rules 2021

Abhishek Gupta[a]

[a]Banaras Hindu University, Varanasi, India

Received 19 January 2023; *Accepted* 07 February 2023; *Published* 10 February 2023

To counter terrorism, fake news, criminal conspiracies, riots, mob lynchings, and other serious offences proliferating through cyberspace, the Government of India enacted Information Technology Rules, 2021 which surprisingly received severe backlash for being violative of fundamental rights. Rule 4(2) or the "First Originator Clause", the bone of contention, received serious allegations of being violative of Art. 19(1)(a) and Art.21. In this article, an attempt is being made to examine the constitutionality of Rule 4(2) through the tests prescribed and evolved through Judicial decisions. The findings regarding the "Right to Freedom of Speech and Expression" are in favour of the "First Originator Clause" but regarding the "Right to Privacy," the findings are problematic. Due to the lack of prescription of any specific technology to identify the "First Originator" which does not intrude into the privacy of all users in a wide sweeping bulk manner and is proportionate in achieving the compelling state interest, the provision makes room for absolute giving up or deletion of end-to-end encryption between every communication which makes it violative of Art. 21. A feasible way of legitimizing the "First Originator Clause" on the touchstone of the Constitution is to reform it by prescribing an alternative less intrusive method of identification of the first originator of information which does not affect the end-to-end encryption of communications and also fulfills the discussed test of intrusion into privacy. The introduction of reform is sine quo non to let the "First Originator Clause" serve its extremely essential compelling state interest.

Keywords: *counter terrorism, fake news, first originator clause.*

INTRODUCTION

On February 25, 2021, the Ministry of Electronics and Information Technology of the Government of India notified, in the exercise of the powers conferred by sub-section (1), clauses (z) and (zg) of sub-section (2) of section 87 of the Information Technology Act, 2000 (21 of 2000)[1], and in supersession of the Information Technology (Intermediaries Guidelines) Rules, 2011, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[2]. Although the IT Rules were enacted for the general welfare of the netizens by affixing intermediary guidelines and ethics codes upon intermediaries, the outcome was just opposite to the expectation of the government. Huge debates started in the public domain over the encroaching tendencies of its provisions on the fundamental rights of netizens. One particular provision, Rule (4), subrule (2)[3], created a huge controversy.

This Rule 4(2) of IT Rules, 2021 provides the "First Originator Clause." Several Digital Rights Organizations, Non-profit organizations, Human rights organizations, etc. started a lot of hues and cries over this clause and other provisions of IT Rules. Even Whatsapp, a significant social media platform, challenged the constitutionality of the impugned rules in the Delhi High Court for being violative of the fundamental rights of million of its users[4]. The issues are still a hot topic of prime-time debate. The resolution of this outcry lies in a very crucial question: "Does the 'First Originator Clause' actually violates the Constitution of India? Answering this question is certainly not a cakewalk, for it requires a full fledge and serious scrutiny of the "First Originator Clause" through the lens of Part III of the Constitution. This is not an easy task even for a senior lawyer, for an argument in favour can anytime be rebutted by a better argument against. Still, in this article, an attempt is going to be made to scrutinize the subject of this article.

[1] Information Technology Act 2000
[2] Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules 2021
[3] Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules 2021, r 4(2)
[4] 'WhatsApp challenges new IT rules in Delhi HC, terms it 'unconstitutional'' (*The Print*, 26 May 2021) <https://theprint.in/india/whatsapp-challenges-new-it-rules-in-delhi-hc-terms-it-unconstitutional/666023/> accessed 15 January 2022

THE IMPUGNED LEGAL PROVISION

Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, commonly known as the "First Originator Clause" reads as:

"A significant social media intermediary[5] providing services primarily like messaging[6] shall enable the identification of the ***first originator of the information*** *on its computer resource as may be required* ***by a judicial order passed by a court of competent jurisdiction*** *or* ***order passed under section 69 by the Competent Authority*** *as per the Information Technology (Procedure and Safeguards for interception, monitoring, and decryption of information) Rules, 2009, which shall be supported with a copy of such information in electronic form:*

Provided that an order shall only be passed for prevention, detection, investigation, prosecution, or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, or incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years:

Provided further that no order shall be passed in cases where other less intrusive means are effective in identifying the originator of the information:

Provided also that in complying with an order for identification of the first originator, no significant social media intermediary shall be required to disclose the contents of any electronic message, any other information related to the first originator, or any information related to its other users:

Provided also that where the first originator of any information on the computer resource of an intermediary is located outside the territory of India, the first originator of that information within the territory of India shall be deemed to be the first originator of the information for this clause."

[5] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 2(1)(v)
[6] *Ibid*

The aforementioned rule provides for additional due diligence to be observed by significant social media intermediaries which they are bound to observe under s.79[7] to enjoy safe harbour exemption from liability.

MEANING OF "FIRST ORIGINATOR"

The IT Rules, 2021 nowhere defines the meaning of "First Originator." Even the Parent Act of this delegated legislation, The Information Technology Act, of 2000; does not define the same. Section 2(1)(za)[8] defines 'Originator' as: "*Originator*" *means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;*

The electronic message here means any information, message, communication, image, video, audio note, etc. in electronic or digital form. Construing the meaning of "First Originator" from the above definition, the first originator refers to that person who was the first to or caused to, send, generate, store or transmit any specific electronic message on or through the computer resource[9] of an intermediary. He was the first to bring any electronic message onto the computer resource of the Intermediary. In non-technical language, he is the first to introduce any electronic information in that social media ecosystem. For example, the person bringing a video on the telegram for the first time is the first originator. An illustration to explain the meaning of "First Originator" as contemplated by Rule 4(2) of IT Rules, 2021:

A, created a voice note and send it to B on Whatsapp who in return sent it to C on the same messaging platform who in return sent it to several other people. A chain reaction of circulation of the voice note happened as a result of which the voice note which was created and sent by A to B is now sent and forwarded again and again on Whatsapp by its several users. Here every user of Whatsapp who has sent or forwarded the voice note is an Originator within the meaning

[7] Information Technology Act 2000, s 79
[8] Information Technology Act 2000, s 2(1)(za)
[9] Information Technology Act 2000, s 2(1)(c)

of s.2(1)(za) but it is "A" who is the "First Originator" because he was the first to send, generate, store or transmit such voice note on the computer resource of Whatsapp.

Suppose A, a user of both telegram and Whatsapp, got a morphed image from telegram and he sent the same to B on Whatsapp who in turn to C, and again the chain reaction of forwarding and circulation started. Within the meaning of Rule 4(2), for Whatsapp, A is the "First Originator" although he had not created the morphed image and he was only the forwarder. It was A who was first to put the morphed image on the computer resource of Whatsapp, he is the "First Originator" even though he is not the real first originator and was only a forwarder.

The latter illustration points out the drawback of this meaning of "First Originator", adopted by the impugned rule, that an innocent one being the first sender, uploader, transmitter, storer, and generator of a specific electronic message is considered as the creator of such message. This problem is being incorporated in several discussions but it shouldn't be because of this imposition of a duty upon netizens to not forward anything negligently and to verify the veracity of the electronic message before introducing it into an altogether new digital ecosystem or in technical language, in computer resource of Intermediary is the need of the hour to prevent any contingencies like riots due to fake news. First Forwarder cum First Originator owes a great duty to verify the veracity and this excuse (that I am not the first originator in the real sense but I have only sent it negligently or to verify the authenticity) frustrates the purpose of the provision.

CONSTITUTIONAL SCRUTINY OF "FIRST ORIGINATOR CLAUSE

The investigation of the "First Originator Clause" through the lens of "The Constitution of India" brings before us the following issues:

- **Whether the First Originator Clause violates Art. 21 of the Indian Constitution.**
- **Whether the First Originator Clause violates Art. 19 of the Indian Constitution.**

WHETHER THE FIRST ORIGINATOR CLAUSE VIOLATES ART. 21 OF THE INDIAN CONSTITUTION

The answer to this question itself depends upon the answer to two paramount questions. If those answers are against the impugned provision then certainly it is violative of Art. 21[10].

i. Whether the First Originator Clause violates Privacy.

Privacy, in layman's terms, refers to the state of being alone and not watched or disturbed by other people, the state of being free from the attention of the public, the state in which one is free to express his desires without any public interference or restraint, a state or condition of liberty coupled with seclusion. In ***Kharak Singh v State of Uttar Pradesh***[11], Subba Rao J. defined Privacy as the right to "*be free from restrictions or encroachments on his person, whether those restrictions or encroachments are directly imposed or indirectly brought about by calculated measures.*"

In ***K.S. Puttaswamy (Retd.) v Union of India***[12], Bobde J. defines Privacy as a **necessary and unavoidable logical entailment of rights guaranteed in the text of the constitution**. In Justice Bobde's opinion, we find the important insight that to be effectively exercised, the liberties in Article 19(1) (speech, expression, association, assembly, movement) and 21 (personal liberty) require, on occasion, to be exercised in **seclusion**. Privacy, therefore, is **an enabler of guaranteed freedoms** and **an inarticulate major premise in Part III of the Constitution.**

In the same case, Kaul J. defined **'privacy… is nothing but a form of dignity, which itself is a 'subset of liberty'**[13] and **'key to the freedom of thought"**[14]. From the definitions of privacy given in K.S. Puttaswamy, it is well established that the right to privacy is an overarching right or the spirit of part III of the Constitution for it is the facilitator of other rights and privacy is at the heart of individual self-determination, of dignity, autonomy and liberty, and concretely, inseparable from the meaningful exercise of guaranteed freedoms such as speech, association,

[10] Constitution of India 1950, art 21
[11] *Kharak Singh v State of Uttar Pradesh* AIR (1963) SC 1295
[12] *KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1
[13] *Ibid* [40]
[14] *Ibid* [52]

movement, personal liberty, and freedom of conscience. Privacy, therefore, is both an overarching, foundational value of the Constitution and is incorporated into the text of Part III's specific, enforceable right under Art.21. **Glenn Greenwald** points out the importance of privacy in our daily life in his work **"No Place to Hide**", the book that chronicles Edward Snowden's unmasking of the American mass surveillance regime. He writes:

"Only when we believe that nobody else is watching us do we feel free – safe – to truly experiment, to test boundaries, to explore new ways of thinking and being, to explore what it means to be ourselves… for that reason, it is in the realm of privacy where creativity, dissent, and challenges to orthodoxy germinate. A society in which everyone knows they can be watched by the state – where the private realm is effectively eliminated – is one in which those attributes are lost, at both the societal and the individual level."[15]

Hence the importance of the "Right to Privacy" in one's life is so much that one can't think of a dignified existence in human life without it.

Now coming to the question of privacy breach by rule 4(2), it violates the right to privacy of every user of internet-based communication platforms working on end-to-end encryption because, as argued by Whatsapp, it is not possible to disclose the identity of "First Originator" unless the intermediary, when served with a copy of such information in electronic form along with an order issued under Rule 4(2)[16], knows the content of the messages of its every user to know which communication contains such information and send by whom and have a well-organized database of record of contents of messages along with the identity of its sender. An illustration can lucidly explain this:

"A Court of competent jurisdiction passed a judicial order mandating Whatsapp to disclose the identity of the first originator of a voice message provoking the masses to kill a religious community. The voice message was sent by "B." Now Whatsapp can only find out that it was "B" who send the message, if it maintains a database of contents of messages, contacts, communications, etc, of its every user in decrypted form. This situation is identical to a situation where "A" is provided with 20 letters written by 20 different persons (their names written in the letters themselves) containing the description of different tourist places

[15] Glenn Greenwald, *No Place to Hide* (Metropolitan Books 2014)
[16] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 4(2)

and "B" asked "A" to point out the man who wrote the letter containing information about Taj Mahal. Now, "A" can do so only if he knows the content of all letters and hence it violates the privacy of every writer."

It is only by removing the end-to-end encryption technology that a database of the contents of a message can be made along with the identity of its originator or sender so that it can be disclosed at the instance of an order and this will lead to the disclosure of the confidential chats of users to the intermediaries or any third party private contractors doing this job for the intermediary. It makes the private data of every individual vulnerable to breach and commercialization. There are several instances already where private data has been sold for advertisements[17] and in this meta era, it is not rare that a subsidiary company shares its users' private chats and data with its parent company[18]. If this end-to-end encryption of communications is dispensed with they would be aware of every piece of information of private nature relating to individuals on sexual orientation, finance, banking, food habits, dressing sense, ideology, likeness, and every kind of confidential information which is being communicated through a such medium. Unless some alternate way, other than the way of breaking end-to-end encryption of every communication, as alleged by Whatsapp to comply with the "First Originator Clause", is being followed the situation is no doubt that of "Bulk Surveillance."

And precisely the problem with bulk surveillance is that it will make the intermediary or their private contractor aware of everything about your personal life, your religious beliefs, your political views, what you watch on the internet, which restaurant you go to eat, your friends, workmates and lovers and more precisely it helps to construct a complete record of a person's social, sexual, religious and political mores.

Hence, it is certainly patent that rule 4(2) infringes, violates, curtails, and interferes with the privacy of users by giving an implied acceptance, by remaining silent on the method to be

[17] Jurgita Lapienyte, 'WhatsApp data leaked - 500 million user records for sale online' (*Cybernews*) <https://cybernews.com/news/whatsappdataleak/#:~:text=The%20dataset%20allegedly%20contains%20WhatsApp,million%20US%20user%20records%20included> accessed 19 January 2023

[18] Lily Hay Newman, 'WhatsApp Has Shared Your Data With Facebook for Years, Actually' (*Wired*, 8 January 2021) <https://www.wired.com/story/whatsapp-facebook-data-share-notification/> accessed 19 January 2023

adopted, to the impugned method (of dispensing with encryption of messages and communications) for compliance purpose. If the communications are stored along with identities in a database in a decrypted form such that they are disclosed to the intermediaries, it can't be said that the privacy of millions of users is not violated. Until and unless the government comes up with a specific alternative way of finding the "First Originator" without interfering and intruding on the private communications of other users, rule 4(2) remains violative of privacy right.

ii. Whether the intrusion into the Right to Privacy by the First Originator Clause is justified under Art.21.

In ***Maneka Gandhi v Union of India***[19], the Supreme Court devised the concept of Substantive due procedure of law which is an amalgamation of procedure established by law and due process of law. The Court held that procedure established by law must not be read in isolation but with due process of law. It means that for an intrusion in right to life and personal liberty by law, the law must be reasonable and unarbitrary in its substance and its procedure. The "First Originator Clause" must follow this ratio to intrude into privacy without violating Art. 21.

Since the recognition of the "Right to Privacy" as a Fundamental Right is not too old so there is no authoritative judicial test explicitly iterated and followed in a series of cases to test the intrusion into Privacy on the benchmarks of Art.21. Moreover, there are not so many judicial pronouncements on privacy. Hence, the only remedial option left is the total of the few judicial rulings on privacy breaches.

In the matter of ***People's Union for Civil Liberties (PUCL) v Union of India***[20], the court while dealing with the constitutionality of Section 5(2) of the Telegraph Act laid down certain rules for the intrusion of privacy. The Court's rules in PUCL are extremely instructive. The Court required under:

- *Rule 2 that the communications to be intercepted be specified in the order;*

[19] *Maneka Gandhi v Union of India* (1978) 1 SCC 248
[20] *People's Union for Civil Liberties (PUCL) v Union of India* (1997) 1 SCC 301

- *Rule 4 that the persons whose communication is to be intercepted and the addresses from where the communications are to be intercepted specified as well in the order;*
- *Rule 3 that the government to take into account whether "the information which is considered necessary to acquire could reasonably be acquired by other means."*[21]
- *Rule 7 that the use of intercepted material shall be limited to the necessary minimum.*[22]

Thus, the court laid down its intention that any legislative enactment intending to intrude into privacy must be specified in the context of such intrusion. It means that the intrusion of privacy must not be in a wide-sweeping form engulfing it bulk of people. These rules were further indirectly upheld by the same court in the matter of ***State of Maharashtra v Bharat Shanti Lal Shah***[23] where the court upheld the constitutionality of the privacy intruding provision under Sections 13 – 16 of the Maharashtra Control of Organised Crime Act even though they infringe upon the overarching right of privacy. If we scrutinize the impugned provisions closely in that matter, we can understand that the kinds of safeguards provided under the legislation in question that the Court found satisfactory are in line with the rules laid down. Section 14, for example, requires details of the organized crime that "is being committed" or is "about to be committed" before surveillance may be authorized; the requirements include, in addition, a description of the "nature and location of the facilities" from which the communication is to be intercepted, the "nature of the communication" and, if known, "the identity of the person."

In addition, Section 14(2)(c) requires a "statement as to whether or not other modes of inquiry or intelligence gathering have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous or is likely to expose the identity of those connected with the operation of interception." Section 14(2)(d) requires special reasons for surveillance to continue after the information has been received. An extension application, under Section 14(2)(f), requires an update on results thus far. Section 14(8) limits duration to sixty days, permitting extensions on specific grounds but only – again – for a period of sixty days, and requires "minimal interception." Like PUCL, the focus of these rules is to prevent abuse through

[21] *Ibid* 317, 398
[22] *Ibid* 301, 318
[23] *State of Maharashtra v Bharat Shanti Lal Shah* (2008) 13 SCC 5

specificity: specificity of individuals and locations, specificity of the duration of surveillance, and specificity of reasons. Once again – and it almost no longer bears repeating – surveillance is tolerated only because of its narrow, targeted nature[24].

The rulings in ***PUCL v Union of India*** and ***State of Maharashtra v Bharat Shanti Lal Shah*** bring us to a new test to check the constitutionality of intrusion in right to privacy which is the **Compelling State Interest/Narrow Tailoring test.** The Narrow tailoring test connotes that the restriction upon right must be tailored in a manner that infringes the right in the narrowest manner that is possible to achieve its goals. The statement of the rule may be found in the American Supreme Court case of ***Grutter v Bollinger***: *"Even in the limited circumstance when drawing racial distinctions is permissible to further a* ***compelling state interest****, the government is still constrained under the equal protection clause in how it may pursue that end: the means chosen to accomplish the government's asserted purpose must be specifically and* ***narrowly framed to accomplish that purpose****."*[25]

In ***Gobind v State of M.P***, the court itself accepted the test in the following words: *"Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right to privacy is itself a fundamental right, that fundamental right must be subject to the restriction based on compelling public interest."*[26]

The "Compelling State Interest/narrow tailoring principle" test can be summarised as encompassing:

A. Proportionality Test; there must exist a proportionate nexus between the intrusion and the compelling state interest.

Chandrachud J. in K.S. Puttaswamy case laid a three-fold test for the intrusion into privacy to be intra vires to the Constitution which was chiefly concerned with "proportionality." In

[24] Gautam Bhatia,' State Surveillance And The Right To Privacy In India: A Constitutional Biography' [2014] 26 NLSI Rev 148
[25] *Grutter v Bollinger* [2003] 539 US 306, 333
[26] *Gobind v State of MP* (1975) 2 SCC 148, 157

Andrews v Law Society of British Columbia, the Canadian Supreme Court articulated the meaning of proportionality as follows:

"The proportionality requirement, in turn, normally has three aspects:

- *The limiting measures must be carefully designed, or rationally connected with the objective.*
- *They must impair the right as little as possible.*
- *Their effects must not so severely trench on individual or group rights that the legislative objective, albeit important, is nevertheless outweighed by the abridgement of rights."* [27]

It means that a legislative enactment fulfills the proportionate nexus test when the limiting measure or intrusion substantially fulfills the objective of such intrusion (req. 1) and follows the narrow tailoring principle (req. 2 and 3).

B. Narrow Tailoring Principle; the restrictive law to be narrowly tailored. In other words, the government must show that its infringing law not only achieves the compelling State interest but does so in a way that restricts privacy in the narrowest possible manner.

C. Adoption of Alternative and Less Intrusive Ways; exhaustion of all conceivable ways of achieving the same goal that does not infringe upon privacy to the extent the impugned law does.

D. Specificity; must not be generally applicable but must be specified in respect of the nature and content of the message or communication to be intercepted or suspended, the period for which the suspension of communication shall be operational, the grounds or eligibility of the person or classes of the person whose communication is to be suspended and the specific purpose or ground for the suspension of communication.

The impugned "First Originator Clause" under Rule 4(2) in its present form (which says nothing about the method of identification thus allowing no encryption method) satisfies the compelling state interest requirement because, firstly, the proviso 1 mandates an order for the disclosure

[27] *Andrews v Law Society of British Columbia* [1989] 1 SCR 143

only on compelling state interests that are prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years. All the grounds upon which an order can be passed under Rule 4(2) are so serious and extremely important in the public interest that they can certainly be regarded as "compelling public interest." An order is not to be issued in trivial cases but only in the compelling public interest.

The impugned provision fulfills the 1st element of the proportionality test because the disclosure of "First Originator" fulfills the compelling state interest as it facilitates the prevention, detection, investigation, prosecution, or conviction of actual offenders who have done the offences like sedition, riots, mob lynching, circulation of child pornography, etc. falling in the category mentioned under proviso 1 through the means of the electronic message by disclosure of their identity. Now, offenders can't hide under the anonymity of end-to-end encryption and use these online messaging intermediaries as a haven for committing such offences. Moreover, it creates a deterrence in the mind of potential offenders that they are now not safe under the curtain of end-to-end encryption and their identity can be disclosed. This provision is providing immense help and assistance to law enforcement agencies, in this new digital era where the nature of offences has evolved from traditional to digital, in coping with digital offenders. Hence, there exists a rational connection between the intrusion in privacy under Rule 4(2) and compelling state interest.

The 2nd and 3rd element of the proportionality test is very bluntly overlooked by the current Rule 4(2). Proviso 2 of Rule 4(2) provides that no order shall be passed in cases where other less intrusive means are effective in identifying the originator of the information. Although this provision smells like being narrowly tailored, this doesn't solve the issue of the non-fulfillment of the narrow tailoring principle in case of breaking end-to-end encryption of all communications. Although the order may not be passed under rule 4(2) when other less intrusive means are there, as long as the breaking of end-to-end encryption of every

communication as a method of enforcing the disclosure of the first originator is being followed, it can't be said that the impugned provision is narrowly tailored. But since the legislation is silent over the method to be adopted for finding out the identity of the first originator, the legislation is prima facie problematic for it generates the scope of mass surveillance by intermediaries of its users by encryption breaking way (as explained earlier).

The other two requirements of the compelling state interest test/narrow tailoring test viz. specificity and exhaustion of alternative means are also not followed by the present structure of Rule 4(2). The intrusion into the privacy of users is generally without any specificity in the no encryption method. Specificity requires that the intermediary must know the identity of the "First Originator" only and not of all users.

Moreover, In ***K.S. Puttaswamy v Union of India***[28], the Court significantly, while holding that the right to privacy is not absolute in nature, gave an overview of the standard of judicial review that must be applied in cases of intrusion by the State in the privacy of an individual. It held that the right to privacy may be restricted where such invasion meets the three-fold requirement of:

- legality, which postulates the existence of law;
- need, defined in terms of a legitimate state aim;
- proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.

Justice S.K Kaul added a fourth prong (D) to this test which mandated "procedural guarantees against abuse of such interference". The "First Originator Clause" though incidentally intrudes on privacy, fulfills:

A. Legality; S. 69 of the Information Technology Act, 2000 provides for the legality of the "First Originator Clause". It provides the power to the executive to issue directions for interception or monitoring or decryption of any information through any computer resource and s. 87 [29]

[28] *KS Puttaswamy* (n 12)
[29] Information Technology Act 2000, s 87

provides the power to the Central Government to make rules to carry out the provisions of this Act.

B. Need; as explained earlier, rule 4(2) provides for the identification of the "First Originator" by the intermediary to be disclosed to the authorities only to fulfill the legitimate state aims provided under proviso 2.

C. Procedural Guarantee; The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009 was specially enacted for this purpose to provide procedural safeguards while discharging the powers under IT ACT. But until and unless the impugned provision is silent over the method to be adopted by the intermediary to identify the "First Originator" and makes the scope for the deployment of breaking end-to-end encryption method of every user to fulfill the mandate provided:

D. does not fulfill the Proportionality; just to facilitate the identification of "First Originator" by intermediary upon receiving an order in that regard, giving up with the end-to-end encryption technology at all thus putting the personal information of users at peril is not proportional in any respect. The Government's stand that they want the identity of digital offenders, within the meaning of Rule 4(2), at all costs to fulfill legitimate state aims is nevertheless outweighed by the abridgement of rights in such a wide engulfing manner. In ***Selvi v State of Karnataka***[30] where the court rejected compulsory polygraph or narcoanalysis against the will of the accused on the ground that upon weighing the importance of convicting a guilty to the protection of the right to privacy of hundreds of innocent, the narrow tailoring principle directs for opting of the latter one. Going through the ruling in Selvi's case, under Rule 4(2), 1 in millions of messages or communications may be relevant towards achieving compelling state interest but still for millions of others, this would amount to a violation of the right to privacy. It would be in the public interest if the identity of a first originator cum chaos creator be disclosed so that the authorities can take reasonable punitive measures against him, but allowing this by breaking end-to-end encryption of millions of communications is not proportionate.

[30] *Selvi v State of Karnataka* (2010) 7 SCC 263

Hence the "First Originator Clause" is problematic under Art. 21 and, technically speaking, violative of the "Right to Privacy" in its present form. The provision is not substantially unconstitutional in nature but since it leaves scope for privacy violation on a bulk scale, it can't be justified as in consonance with Art. 21 either, hence doesn't follow the substantial due procedure provided in Maneka Gandhi. The "First Originator Clause" is violative of Art. 21 in its present form due to procedural unconstitutionality.

WHETHER THE FIRST ORIGINATOR CLAUSE VIOLATES ART. 19 OF THE INDIAN CONSTITUTION.

As soon as the MeitY released the new IT Rules, 2021; a heated debate started in the public arena and one of the major apples of discord is that the "First Originator Clause" is violative of the "Right to Freedom of Speech and Expression" guaranteed to every citizen under Art.19 (1)(a). However, coming to this conclusion would be fatal unless the validity of the impugned clause is tested on the touchstone of Art. 19 itself. To test the validity, two essential questions are needed to be discussed:

i) ***Whether the First Originator Clause infringes, restricts, or curtails free speech and expression.***

It is prima facie obvious that Rule 4(2) restricts Free Speech and Expression. The mandatory disclosure of "First Originator" is violative of "Freedom of Speech and Expression". It puts up a psychological restraint, due to the fear of order being passed under the aforesaid rule, upon the masses and inhibits them to express their views on social media. This leads to the decline of public space which allows free and fair discussion on the public matter because if we know that our identity would be disclosed at any point in time at the order of "competent authority"[31], who is nothing but an agent of the ruling government, based upon the whims and fancies of the ruling government upon an order under Rule 4(2) which may be issued under the garb of loose and ambiguous ground of "potential to disturb Public Order", we would certainly hesitate to

[31] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r 2(d)

engage in such communication or nature of communication which may be declared as a threat to public safety by the government which in reality be an honest discussion or critique upon social, educational, economic, political or any matter.

We will hesitate to associate with unpopular groups espousing unpopular causes if we know that we are being watched. There is so much that we will not say to each other if we know that, one day, it could be made public including our identity. We will self-censor, draw ever more constricting lines in the sand, and suffocate ourselves with our caution. We will censor others, warning them not to speak too much, be too radical, or think too differently. And if this would be the situation then there would be no meaning of so-called democracy. It would be like expressing only what the government wants or permits. In that case, there would be the right to speech and expression but that right would lack the vital element of "Freedom", "Freedom of speech and expression", and freedom to express what one wants within the prescribed boundaries. Even though the identity of only perpetrators of offences mentioned under proviso 2 would be disclosed, the psychological restraint upon the free speech and expression would be upon every user that they may be declared perpetrators by the competent authority and would be subjected to punitive measures. Only when we know that our communications are end-to-end encrypted such that even the intermediary doesn't know it and can't disclose either our identity or our message, do we heartily exercise our "Right to Freedom of Speech and Expression?"

Mind it, the changing of the method of identification of "First Originator", from (breaking the encryption of all) method to some alternate and less intrusive method like that of V Kamakoti (to be discussed later), would not solve the issue of free speech either. Even when only the encryption of the first originator is broken in contrast to that of all, still "Right to freedom of Speech and Expression" of all users is being violated because at every moment they would be in constant mental fear that their identity would be disclosed on the mandate of an order for being so-called offender under rule 4(2) for breaking public order.

ii) Whether the First Originator Clause falls within the definition of reasonable restriction upon free speech and expression as provided under Art. 19(2).

Even though the "First Originator Clause" psychologically inhibits the users of computer resources of Intermediaries or in simple language social media and thus an impediment to "Freedom of Speech and Expression", this restriction upon Art 19(1)(a)[32] is reasonable within Art. 19(2)[33]. Art. 19(2) imposes reasonable restrictions on the exercise of the said right in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or about contempt of court, defamation or incitement to an offence.

In 1997, "The Supreme Court, in ***People's Union for Civil Liberties v Union of India***[34], laid down that the Right to freedom of Speech and Expression guaranteed under Article 19(1)(a) is subject to reasonable restrictions which might be imposed by the State. Reasonable restrictions can be imposed by the state in the interests of national sovereignty and integrity, state security, friendly relations with foreign states, public order, or for preventing incitement to the commission of an offence.

In the cases of ***Ramji Lal Modi v State of UP*** [35] and ***Virendra v State of Punjab*** [36] that the phrase "for the interests of" has a very broad scope and the government has essentially unlimited authority to enact laws purportedly to maintain public order and has always had a check on the freedom of speech and expression through its restrictions.

Even the aforementioned rulings upheld that fundamental rights are not absolute and subject to certain reasonable restrictions provided under art. 19(2), arguing that the mental restriction put up by the impugned clause is unconstitutional, is not right. The grounds provided under Proviso 2 of Rule 4(2) for the disclosure of the identity of the "First Originator" are substantially identical to the reasonable restrictions provided under Art. 19(2) because the grounds deal with the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or about rape, sexually

[32] Constitution of India 1950, art 19(1)(a)
[33] Constitution of India 1950, art 19(2)
[34] *People's Union for Civil* (n 20)
[35] *Ramji Lal Modi v State of UP* AIR 1957 SC 620
[36] *Virendra v State of Punjab* AIR 1957 SC 896

explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years.

Even though the First Originator Clause infringes or curtails the freedom of speech and expression, it does so on the grounds which are well within the reasonable restrictions provided under the Art. 19(2). Hence, it is not unconstitutional.

CONCLUSION AND SUGGESTIONS

Since the enactment of IT Rules, 2021; the life of the First Originator clause has never been without controversy. Time and again, it received severe allegations of being violative of basic human rights also known as fundamental rights of citizens in a democracy. It has been portrayed as an antidemocratic, tyrannical interference upon the right to freedom of speech and expression and right to privacy, which are at the very base of a democratic political system, by several Organizations, MNCs, intermediaries, etc. since its inception. An attempt made, in this article, to constitutionally scrutinize the First Originator Clause shows that it is not violative of Art. 19(1)(a) due to falling in the category of reasonable restrictions under Art. 19(2). But this doesn't mean that the outcry is not genuine. Regarding Art. 21 their allegations though not absolutely, up to some extent are right because the First Originator Clause fails to fulfill firstly the Puttaswamy test and secondly the compelling state interest /narrow tailoring test for intrusion into privacy.

Complete deletion of the First Originator Clause is also not advantageous. It is a must in this digital era to curtail the misuse of end-to-end encryption communication platforms by antisocial elements like terrorists etc. There are several reported instances where under the curtain of end-to-end encrypted communications the whole conspiracies of riots, terrorist activities, mob lynchings, and several other serious offences are planned. Thus, the provision must exist under the cyber law and for which revision, amendment, or reform is essential. As pointed out earlier that the chief problem with Rule 4(2) is its implied assent, by way of silence, to no encryption method. Hence, the only suggestion for reform is the specific prescription of the method to be adopted under Rule 4(2) which fulfills the privacy test discussed earlier.

As suggested by Indian Institute of Technology-Madras Professor **V Kamakoti**, who is also a member of the National Security Advisory Board, the identity of the Originators of the message can be disclosed even without breaking the end-to-end encryption. He said WhatsApp can trace messages without breaking encryption. For this, he suggested a technical solution. He had proposed two solutions to enable traceability- one, everyone gets the WhatsApp forward along with the originator of information with end-to-end (E2E) encryption intact, and two, the originator of the information is encrypted on top of the end-to-end encryption and only WhatsApp holds the key to decrypt the former.[37] (this article isn't going to delve into its details). But the point is that there are other alternatives and less intrusive means available for achieving the compelling state interest. When these kinds of methods are being prescribed and adopted then only the privacy of the first originator would be intruded upon and not of all thus making the intrusion specific and narrowly tailored and ultimately this will satisfy the four-prong test of Puttaswamy and Compelling State Interest/Narrow Tailoring Principle test. It is only by the required clarification legislation that the proviso 2 and 3 of present Rule 4(2) would truly manifest narrow tailoring principle and adoption of alternative and less intrusive ways requirements.

Here the only requirement is that the Stakeholders must come forward to clarify, by the way of legislation, that the breaking of end-to-end encryption of every user is not to be followed for complying with Rule 4(2) of IT Rules but some other less intrusive and alternate way, maybe that of V Kamakoti is to be followed. It is only then the "First Originator Clause" is well within the constitutional limits.

[37] Swathi Moorthy, 'An IIT-M professor says WhatsApp can trace messages without breaking encryption. Can it work?' (*Money Control*, 1 June 2021) <https://www.moneycontrol.com/news/business/an-iit-m-prof-says-whatsapp-can-trace-messages-without-breaking-encryption-can-it-work-6969971.html> accessed 19 January 2023