THE FUTURE OF INTERMEDIARY LIABILITY IN INDIA

JANUARY 2020

sflc.in

Future of Intermediary Liability in India

Published by: SFLC.IN

Address:
SFLC.IN
2nd Floor, K-9,
Birbal Road, K-Block,
Jangpura Extension, Delhi
India – 110014

Email: mail@sflc.in
Website: https://www.sflc.in
Twitter: @SFLCin

Table of Contents

LIST OF CASES

- Amitabha Gupta v. Union of India, W. P. No. 13076/2019, Madhya Pradesh HC (at Jabalpur)
- Antony Clement Rubin v. Union of India & Others, W. P. 20774/2018, Madras High Court
- Facebook Inc. v. Antony Clement Rubin, Diary No. 32478/2019, Supreme Court of India
- Facebook Inc. v. Union of India, T.P. (C) No. 001943–001946/2019, Supreme Court of India
- ITW Signode India Ltd. v. Collector of Central Excise, (2004) 3 SCC 48
- Janani Krishnamurthy v. Union of India & Others, WP 20214/2018, Madras High Court
- K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1
- K. S. Puttaswamy v. Union of India, (2019) 1 SCC 1
- Kent RO Systems Ltd. v. Amit Kotak, 240 (2017) DLT3
- Khushwant Singh v. Maneka Gandhi, AIR 2002 Del 58
- MySpace Inc. v. Super Cassettes Industries Ltd., 236 (2017) DLT 478
- National Stock Exchange Member v. Union of India, 125 (2005) DLT 165
- New York Times v. United States, 403 U.S. 713, 726 (1971)
- Petronet LNG Ltd. v. Indian Petro Group, 158 (2009) DLT 759
- R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632
- Sagar Rajabhau Surywanshi v. Union of India, PIL/147/2018, Bombay High Court
- Shreya Singhal v. Union of India, AIR 2015 SC 1532
- United States v. Jones, 565 U.S. 400 (2012)
- WhatsApp Inc. v. Janani Krishnamurthy, Diary No. 32487/2019, Supreme Court of India

LIST OF ABBREVIATIONS

- **AI –** Artificial Intelligence
- **AIR –** All India Reporter
- **CJEU –** Court of Justice of the European Union
- **Del –** Delhi
- **DLT –** Delhi Law Times
- **E2EE –** End-to-End Encryption
- **ECD –** EU Copyright Directive
- **EFF –** Electronic Frontier Foundation
- **EU –** European Union
- **FBI –** Federal Bureau of Investigation
- **FOSS –** Free and Open Source Software
- **HTTP –** Hypertext Transfer Protocol
- **IIT –** Indian Institute of Technology
- **IT –** Information Technology
- **ISP –** Internet Service Provider
- **LEA –** Law Enforcement Agencies
- **MeitY –** Ministry of Electronics and Information Technology
- **NLP –** Natural Language Processing
- **NSA –** National Security Agency
- **SC –** Supreme Court
- **SCC –** Supreme Court Cases
- **TSP –** Telecom Service Provider
- **UK –** United Kingdom
- **US/USA –** United States/United States of America
- **WP –** Writ Petition

ACKNOWLEDGEMENTS

*W*e express sincere gratitude to our knowledge partner Mishi Choudhary and Associates LLP without whose support this report would not have been made possible. We also thank the intermediaries whose inputs provided valuable direction for our research. In addition, we are grateful to all who took time out of their busy schedules to participate in our events on intermediary liability.

INTRODUCTION

The *Shreya Singhal*(1) judgment of the Supreme Court of India in 2015, was a watershed moment, not just for online speech in India, but for intermediary liability law in the country. In *Shreya Singhal*,the apex court clarified that online content could be taken down from intermediary platforms like Facebook or Twitter only by a court's order or at the behest of the government. This protected intermediary platforms from liability on the basis of user generated content and ensured that frivolous take down requests were culled out, protecting user speech online.

The centralization of platforms on the Internet has put pressure on governments around the world to revisit protections afforded to them for user speech. Post the Cambridge Analytica revelations, nations have woken up to the threat of dis/misinformation online. The influence of social media on society, from electoral democracy to mass movements on subjects like sexual harassment and climate change has exponentially increased in the past few years. Nation states around the world are pressurizing online platforms to purge extremist/ illegal content from their services. Countries like Germany, Singapore, Australia, and the EU (Terrorist Content Regulation and the Copyright Directive) have been introducing legislations to enhance responsibility of online platforms for user generated content.

In India, the government has proposed amendments to the Information Technology (Intermediaries Guidelines) Rules(2) by including provisions like mandatory upload filters and traceability of messages(3). Apart from the Indian government other countries like the US, UK and Australia too have made demands for gaining access to content on E2EE platforms. Recently, these nations sent a letter to Facebook for stalling its proposal on introducing cross-platform E2EE on all its services – Facebook, Instagram and WhatsApp. The letter sent by these countries to Facebook, cited concerns around child exploitation and other criminal activity which takes place on E2EE platforms as a reason to build back-doors for lawful access. Similarly, despite all major platforms using upload filters to pre-censor potentially illegal content from their services, countries have been codifying demand for mandatory use of filters. Beyond India's proposal to introduce 'automated' filters on all intermediary platforms, the EU in its new Copyright Directive requires intermediary platforms to make 'best efforts' to prevent future uploads (read upload filters).

The menace of so called 'fake news' has been driving countries to introduce laws to curb it. Singapore, China, and Russia have already passed legislation to combat fake news and one of the key reasons cited by the Indian government to issue amendments to its Intermediaries Guidelines is to combat 'fake news'.

Challenges like the proliferation of fake news, child exploitation imagery, terrorist content, hate speech and vitriol online are grave concerns, but nation states, including India must not draft policy which has the unintended consequence of diluting rights like privacy and free speech in the online space. Lawful access to private data must adhere to constitutional standards of necessity and proportionality. Regulations targeted at fake news run the risk of negatively impacting free speech. Upload filters are imperfect and are prone to throwing up false positives. A number of these challenges can be addressed by existing laws, and fresh regulation which undermines basic tenets of the Internet like encryption and open and free information exchange must not be imposed.

The promise of the Internet being an open, inclusive, global and decentralized network is under threat. Technology companies and nations often work in tandem, and this diminishes user rights and negatively affects their interests. To ensure that digital rights of users remain intact, policy makers and influencers must not ignore their voices and ensure that people have the same rights online, as they enjoy in the physical world.

---

(1) Shreya Singhal v. Union of India, AIR 2015 SC 1532

(2) The Information Technology (Intermediaries Guidelines) Rules, 2011

(3) A provision to trace out the originator of messages in the Intermediaries Guidelines Rules, will disproportionately affect end-to-end encrypted (E2EE) platforms like WhatsApp and Signal as the security and privacy built into E2EE platforms does not allow for such tracing out.

PAST WORK AND RESEARCH METHODOLOGY

The scope of this report is restricted to analysing and studying the digital rights impact of key changes recommended by the Ministry of Electronics and Information Technology in the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules],2018(4). SFLC.in's past work on the subject of Intermediary Liability has covered – the evolution of intermediary liability law in India including landmark judgments from various courts in India and international developments on intermediary liability law, along with key judgments from foreign jurisdictions.

SFLC.in's existing work on intermediary liability can be accessed, here –*https://sflc.in/publications*.

This report studies the law and policy implications of four subject areas namely, upload filters, traceability of originator, local registration and office thresholds for foreign companies, and 24-hour take down timelines. The analysis includes technical assessments, legal impact, global perspectives and policy recommendations for these subject areas.

This study relies on both primary and secondary resources. For primary research, interviews with domestic and international technology companies were conducted, on the impact of the Draft Intermediaries Guidelines (Amendment) Rules, 2018. The insights from these interviews have been documented in this report. For secondary research, scholarship by researchers from around the world, that is available for open access, and case law has been relied upon.

(4) The Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 - *https://www.meity.gov.in/ writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf*

CHAPTER 1

1. UPLOAD FILTERS, WHAT'S THE IDEA?

Automated filtering technology or upload filters are not new. Google has been using such filtering technology on its video streaming platform, YouTube, since 2007(5). Google's technology called Content ID, matches uploaded videos to a database of copyright protected content and based on these matches lets rights owners decide what to do with such content(6) (they can monetize such content or have it removed from the platform). Other platforms like Facebook, use technological means to detect(7) hate speech(8) and even WhatsApp, which is an E2EE platform, uses AI technology to weed out(9) fake and automated accounts. Google, Facebook, Twitter and Microsoft have been working together to purge extremist and child abuse content from their platforms by creating a shared database(10) and using filtering technology to remove such content. Recently, both Google(11) and Facebook(12) have released their open AI tools to combat child sexual abuse material on the Internet.

The debate around automated filters gained global traction with the introduction of the draft EU Copyright Directive ("the ECD") (a revamp of the existing copyright law applicable in EU member states)(13). Article 17 of the ECD, requires platforms hosting copyright protected content, to ensure the unavailability of unauthorised content and to make best efforts to prevent future uploads of such content on their platforms. These requirements do not state specifically how hosting platforms like YouTube or Facebook are to ensure take down of unauthorised content and what it means by 'making best efforts'. As services like Facebook and YouTube already utilize automated tools for purging illegal content, this regulation codifies the use of upload filters, indirectly making them a requirement under law. Earlier versions of the clause directly pointed to the use of content recognition technologies, but such language was later tweaked to include words and phrases such as - 'unavailability of specific works' and 'best efforts'(14).

In India, the debate on automated filters was ignited by the introduction of the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018(15) ("The Draft Intermediaries Guidelines"). These guidelines seek to amend existing due diligence rules for Internet intermediary platforms (like Facebook, Twitter, TikTok and YouTube), which make them

eligible for safeharbour protection from liability arising from third party content(16). Rule 3(9) of the Draft Intermediaries Guidelines(17) proposes to make the deployment of automated tools, which will be required to proactively identify and remove unlawful content from intermediary platforms, mandatory. This recommendation made by the Ministry of Electronics and Information Technology ("MeitY")(18) made the upload filters debate mainstream in India. Purportedly, the proposed changes to the intermediaries guidelines have been introduced to address challenges faced by law enforcement agencies in relation to terrorist content, obscene content, issues of public order, and fake news (among other things)(19). Many civil society groups, academia and experts have criticised the move as a form of online censorship and a threat to free expression online.(20)

Existing filters used by social media companies to block content are notorious for taking down benign content. Recently, an Indian lawyer, Sanjay Hegde's Twitter account was suspended by the company as he had posted a historical picture of August Landmesser, in which Mr. Landmesser does not perform the Nazi salute in a rally being addressed by Adolf Hitler. After reinstating his account, Twitter again suspended his account for having posted an objectionable poem from a few years back.(21) Mr. Hegde has recently moved the Delhi High Court against Twitter for arbitrarily suspending his account(22). Early last year, journalist Barkha Dutt's Twitter account was suspended after she had posted personal details of people who were sending her rape threats and obscene pictures. While blocking her account, Twitter failed to take down the obscene content which was posted by users who had threatened her.(23) In another incident from late 2018, Ather Zia, a professor of anthropology and gender studies at the University of Northern Colorado, Greeley, found her cover picture on Facebook, which was the flag of Azad Jammu and Kashmir, censored from users in India. She was never informed of such a take down by Facebook, as it was selective, and she could see her cover picture herself.(24) In another incident from Kerala last year, YouTube users were blocked (based on upload filters) from sharing audio/ video clips of traditional orchestra during festivities at temples, due to a copyright claim by Sony Music on the music in such clips. The copyright claim was based on a film which covered the traditional orchestra music while recording the sounds of the festival.(25)

---

(5) Google launched its Content ID system in 2007 - *https://googleblog.blogspot.com/2007/10/latest-content-id-tool-foryoutube.html*

(6) Google's Content ID system and how it works - *https://support.google.com/youtube/answer/9245819?hl=en&ref_topic=9282364*

(7) Facebook's Rosetta technology - *https://engineering.fb.com/ai-research/rosetta-understanding-text-in-images-andvideos-with-machine-learning/*

(8) Facebook's AI Can Analyze Memes, but Can It Understand Them? - *https://www.wired.com/story/facebook-rosettaai-memes/*

(9) WhatsApp cracks down on fake and abusive accounts ahead of general elections (India) - *https://yourstory.com/2019/02/whatsapp-ban-accounts-misuse-elections-2019*

(10) Facebook, Twitter, Google and Microsoft team up to tackle extremist content - *https://www.theguardian.com/technology/2016/dec/05/facebook-twitter-google-microsoft-terrorist-extremist-content*

(11) Google releases free AI tool to help companies identify child sexual abuse material - *https://www.theverge.com/2018/9/3/17814188/google-ai-child-sex-abuse-material-moderation-tool-internet-watchfoundation*

(12) Facebook open-sources algorithms for detecting child exploitation and terrorism imagery - *https://www.theverge.com/2019/8/1/20750752/facebook-child-exploitation-terrorism-open-source-algorithm-pdq-tmk*

(13) The EU Parliament adopted the revised law on April 17, 2019 - *https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=uriserv:OJ.L_.2019.130.01.0092.01.ENG*

(14) Refer to Article 17 of the ECD

(15) The Draft Intermediaries Guidelines (Amendment) Rules, 2018, seek to amend the Information Technology Intermediaries Guidelines Rules, 2011, which lists down conditions to be adhered to by intermediaries, for being eligible for safe-harbour protection under Sec. 79 of India's Information Technology Act, 2000. Sec. 79 of the Information Technology Act, 2000, provides for conditional safe-harbour to intermediaries for hosting third party

These are a few examples of how existing upload filters arbitrarily take down legal content from social media platforms, based on self regulation exercised by such companies. If upload filtering is converted into a precondition for claiming safe-harbour protection by online intermediaries, the existing challenge faced by social media platforms of over-censorship will get further exacerbated.

1.1 The Legal Conundrum

Sec. 79 of the Information Technology Act, 2000 ("the IT Act") provides for conditional safeharbour protection to all categories of intermediaries(26) for third party content on their platforms. Intermediaries are required to either be mere conduits, providing access to communication systems or not participate in the transmission of the content to be eligible for this safe-harbour protection. In addition to their function, intermediaries are required to adhere to due diligence rules (the Intermediaries Guidelines Rules, 2011 under the IT Act) and remove content from their platforms when asked to by courts or appropriate government agencies, to be eligible for safe-harbour protection.

The Intermediaries Guidelines Rules, 2011 ("the Current Intermediaries Guidelines") require intermediaries to have privacy policies, remove content when asked to (by courts or the government), and provide assistance to law enforcement agencies among other things. The safeharbour protection given to intermediary platforms under Sec. 79 of the IT Act is linked with their adherence to the Current Intermediaries Guidelines. Now, by way of an amendment to these rules, MeitY has proposed to bring out changes to these guidelines, such as - the mandatory deployment of automated filters for proactive monitoring of content on these platforms.

The issue of whether intermediaries could be left to decide the legality of content on their platforms was addressed by the Supreme Court of India in its landmark judgment of *Shreya Singhal v. Union of India*(27). A submission was made before the court in *Shreya Singhal* that intermediary platforms cannot be required to determine the legality of content on their platforms. The court while delivering its judgment held that the requirement for intermediaries to apply their own mind for judging legality of content was absent from the framework of the IT Act. The court clarified that intermediaries could only be asked to remove content from their platforms vide a court order or by an appropriate government agency as they could not be expected to judge the legality of content on their platforms. Thus, after *Shreya Singhal*, the law on content take downs in India is settled to the effect that intermediary platforms cannot be required to monitor their platforms and determine the legality of

---

content on their platforms. For further reading, please refer to our comprehensive report on Intermediary Liability - *https://sflc.in/intermediary-liability-20-shifting-paradigm*

(16) Refer to Sec. 79 of the Information Technology Act, 2000

(17) You may download the Draft Intermediaries Guidelines from - *https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf*

(18) The nodal government agency for enforcement of the IT Act in India.

(19) Kindly refer to the press notification released alongside the Draft Intermediaries Guidelines - *https://pib.gov.in/newsite/PrintRelease.aspx?relid=186770*

(20) Public comments on the Draft Intermediaries Guidelines can be accessed, here - *https://meity.gov.in/writereaddata/files/public_comments_draft_intermediary_guidelines_rules_2018.pdf and here - https://meity.gov.in/writereaddata/files/Addendum1_Public_comments_on_draft_intermediary_guidelines.pdf*

(21) Senior SC Advocate Sanjay Hedge's Twitter Account Suspended Twice in Two Days - *https://www.thequint.com/news/india/sanjay-hegde-twitter-account-suspended-blames-organised-trolling*

(22) Sanjay Hegde Moves Delhi HC Against Account Suspension - *https://www.livelaw.in/top-stories/sanjay-hegdemoves-delhi-hc-against-twitter-account-suspension--150838*

(23) Journalist Barkha Dutt Condemns Twitter for Blocking Account After Abuse Online - *https://www.news18.com/news/india/journalist-barkha-dutt-condemns-twitter-for-blocking-account-after-abuse-online-41563.html*

(24) Block List – How Facebook helps silence Kashmiris - *https://caravanmagazine.in/commentary/how-facebook-helpssilence-kashmiris*

(25) The Thrissur Pooram Sound Story: Copyright on Sounds of the Festival? - *http://scholarship.ciipc.org/2019/06/04/the-thrissur-pooram-sound-story-copyright-on-sounds-of-the-festival/#_ftn9*

content on their platforms. The court in *Shreya Singhal*, clarified that any restriction on online speech in India must adhere to the constitutional limitations as imposed by Article 19(2) of the Constitution of India.

In matters related to intellectual property rights, the Delhi High Court in two important cases – *My Space Inc. v. Super Cassettes Industries Ltd.*(28) and *Kent RO Systems Ltd. v. Amit Kotak*(29)held that tasking intermediaries with the responsibility of identifying illegal content (infringement of IP rights in the particular cases) could have a chilling effect on free speech on the Internet.

As per the current law and jurisprudence on platform and content regulation in India, the mandatory requirement of installing automated filters for proactively monitoring and removing illegal content from intermediary platforms falls foul of law. Such a requirement will negatively impact the online privacy of users, as these tools will comb through each and every piece of content uploaded on intermediary platforms and dilute free speech on the Internet by legitimizing pre-censorship tools.

From a privacy standpoint, a 9-judge bench of the Supreme Court of India in *K. S. Puttaswamy v. Union of India*(30), declared informational and communicational privacy as fundamental rights under the Indian Constitution, as part of the overall right to privacy in India. At various points in the judgment, it has been made clear that individuals have the sole and complete right to their informational and data privacy and meaningful consent should be the basis of accessing data. Justice Chandrachud in his judgment also recognized that dangers to privacy might not only originate from the State but non-State actors (such as private corporations) as well. The mandatory requirement for automated filters will require constant monitoring of each and every byte of information uploaded by users. Since this requirement will apply to all intermediaries, it will be a real threat to user privacy and invalidate meaningful consent. Legally mandated monitoring requirements by private entities, which are often non-transparent and without recourse to grievance redressal will severely hamper privacy on the Internet.

1.2 Pre-Censorship

Another challenge that upload filters throw up, is the risk of pre-censorship or as in legal terms – 'prior restraint. Prior restraint' is the censorship of speech before such speech becomes public. It is considered as one of the most serious modes of suppressing free speech. Such a mode of censorship restricts speech from entering the marketplace of ideas. In case of prior restraint, the onus of proving why speech should be permitted gets shifted to the speaker instead of the government. In a regime of prior restraint, the government has disproportionate powers to determine what does and does not enter the public sphere, giving them the ability to control public discourse.(31)

One of the landmark cases on prior restraint in India is *R. Rajagopal v. State of Tamil Nadu*(32) where the Supreme Court held that any system of prior restraint bears a heavy presumption against constitutional validity.

In *Rajagopal*, a Tamil magazine wished to publish the autobiography of an individual by the name of Auto Shankar, who was convicted of the murders of six people, without his apparent consent. Claims were made that the autobiography contained defamatory content on police and other government officials, alleging that there was a connection between them and the criminal. It was argued before the court that due to Auto Shankar's privacy claims, and defamation and privacy claims made by government officials,

(26) Under Sec. 2(1)(w) of the IT Act, intermediaries include a wide range of entities – social media platforms, search engines, e-commerce platforms, ISPs, TSPs, cyber cafes etc.
(27) (Supra) Note 1
(28) MySpace Inc. v. Super Cassettes Industries Ltd., 236 (2017) DLT 478
(29) Kent RO Systems Ltd. v. Amit Kotak, 240 (2017) DLT 3
(30) K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1
(31) Gautam Bhatia, Offend, Shock, or Disturb: Free Speech under the Indian Constitution, Oxford University Press
(32) R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632

the publication of the autobiography must not be allowed.

The court in *Rajagopal*, after citing various decisions from the US and UK, held that the State or its officials do not have authority in law to impose a prior restraint on publication (in this case of material that is defamatory to State officials). Citing the pentagon papers case from the US *[New York Times v. United States]*(33) the court held that any system of prior restraint of free speech must bear a heavy presumption against its constitutional validity and in such cases the government carries a heavy burden of showing justification for the imposition of such a restraint.

Subsequently, in *Khushwant Singh v. Maneka Gandhi*(34), a division bench of the Delhi High Court upheld the principle expounded in Rajagopal wherein, for any kind of prior restraint on speech, the government authorities need to show justification for the imposition of such a restraint. The court was deciding on pre-publication injunctions on the publication of Khushwant Singh's autobiography, which commented on the relationship between Maneka Gandhi and her family. The division bench refused to grant an order of restraint and held that the remedy could be by way of damages post the publication of the book.

In another judgment from the Delhi High Court *[Petronet LNG Ltd. v. Indian Petro Group*(35)*]*, the court in an attempt to balance the claim of the plaintiff for protective injunction for confidential corporate information and the defendant's claim of right to publish (speech) such information, held that public interest in ensuring dissemination of news and free flow of ideas, is of paramount importance. It declined to order a prior restraint on a news item, which was claimed to be confidential and damaging to a business entity, on the basis of the public importance of sharing such information. The court stated - *"The news or information disclosure of which may be uncomfortable to an individual or corporate entity but which otherwise fosters a debate and awareness about functioning of such individuals or bodies, particularly, if they are engaged in matters that affect people's lives, serve a vital public purpose."*

The court clarified that unless the information is of a nature that the business of a corporate entity or its very existence is threatened (specially where the government owns a stake in such a corporate entity) courts will not be inclined to restrain the publication of such information. The court put this principle succinctly *"The Constitution's democratic framework, depends on a free commerce in ideas, which is its life blood."*

The automated filters requirement as per Rule 3 (9) of the Draft Intermediaries Guidelines makes it mandatory for all intermediaries to deploy automated tools for proactively identifying and removing access to unlawful content. Looking at the principle expounded in *Shreya Singhal* that intermediaries cannot, after applying their own mind, determine what is legal content or not and the jurisprudence on prior restraint, this requirement violates the standards of free speech established by courts in India. Considering that the Supreme Court in *Shreya Singhal* also held that any limitations on speech must adhere to constitutional limitations as listed under Article 19 (2), the proactive identification and removal of 'unlawful' content is beyond the scope of existing free speech law in India.

1.3 Do Automated Filters Work? A Technical Assessment

There are a few popular technological tools which are available for use by intermediaries for performing filtering on their services. But the problems are aplenty – filtering tools are expensive, they undermine safe-harbour protection, they discriminate against marginalized groups, and they are not effective for non-English languages (among other things).

All filtering methods broadly require - identification of unwanted content using technological tools (at the first instance of uploading), matching this unwanted content with a pre-existing

(33) New York Times v. United States, 403 US 713, 726 (1971)
(34) Khushwant Singh v. Maneka Gandhi, AIR 2002 Del 58

database (of content or content identification metrics like metadata) to check for positives and then blocking access to the specific content. Errors at any level in this process may throw up false positives or false negatives undermining the accuracy of the filtering tools, affecting free speech and privacy on the Internet.

1.3.1 An Assessment of Popular Methods of Filtering Existing Filtering Techniques for Media Content(36)

Metadata Filtering

One of the most common techniques of identifying digital files is searching on the basis of metadata. Metadata is data which is annotated to the main content and contains details like title, data, file size, length, encoding rate etc. Such techniques require automated scripts to crawl over content and identify specific files based on the tagged metadata, such as – title, author/ artist name, text description and tagged keywords. Such metadata crawling can be achieved without necessarily analysing the actual content.

The efficiency of metadata searches is heavily dependent on the accuracy of the information/ description contained in the annotated data itself. Imprecise information due to mislabeling makes metadata searches redundant. Different media content could have the same metadata (movie and a book with the same title), making identification a problem. Often, converting the file format of media content drastically alters the metadata, thus rendering a metadata search on that content fruitless. The fact that metadata searches can result in both false positives and false negatives, clubbed with the reality that altering the metadata of a file is relatively easy, a filtering system which solely relies on metadata searches will not be reliable for accurately identifying infringing content.

Hash Based Identification/ Filtering

Hash based identification systems are more accurate and generally a reliable method for uniquely identifying media content. A hash is a numeric representation of a file that is significantly smaller than the original content and is unique to that particular content. The hash value of a file is computed by using a cryptographic hash function that takes the file as input. Each media content will have a unique hash value and even slight modifications will result in new hashes. The relatively smaller size of hash functions as compared to the associated media files makes hash based searches and identification much less cumbersome as compared to analysing complete media files. Databases of unique hashes are much easier to maintain and do not require analysing the underlying content.

Despite the benefits, hash based searches have their own demerits. Any alteration in the original media file, while result in a new hash value. e.g.. A change in format of the file, will render a new hash value for the same content and any hash database used for identification will then be required to be updated with both hashes for efficient identification. Thus, infringing content might escape identification in a hash-based identification system if databases are not robust enough to capture hash values of altered files.

Audio and Video Fingerprinting

In comparison to hash or metadata based filtering, fingerprinting techniques are more advanced methods of content identification. Typically, such techniques make identification based on certain characteristics of media files themselves. For example, for audio files, fingerprinting techniques can first identify the different frequencies in a file and create a fingerprint for different frequency values over a sequence of specific time intervals. Such identification is unique to the underlying media content of the file and immune to transformations of the original files.

Fingerprinting techniques require algorithms to process the underlying media content of a given file based on specific metrics, such as frequency valuesin an audio file. This limits the capacity of fingerprinting techniques to be used for a diverse set of content. A technique built to identify audio files will not be useful for identifying other types of content such as – photographs or software pro-

(35) Petronet LNG Ltd. v. Indian Petro Group, 158 (2009) DLT 759

(36) Reliance placed on 'The Limits of Filtering: A Look at the Functionality of Content Detection Tools' by Evan Engstrom and Nick Feamster - *https://www.engine.is/the-limits-of-filtering*

(37) Reliance placed on - 'Mixed Messages? The Limits of Automated Social Media Content Analysis' by the Center for Democracy & Technology, available at *https://cdt.org/wp-content/uploads/2017/11/Mixed-Messages-Paper.pdf*

grams. Fingerprinting techniques can be targeted by altering the encoded content in the media file. Any such alteration will render false positives or false negatives. Audio and video files can be transcoded from one file format to the other or from one bit rate to the other, this transcoding process often distorts aspects of the audio/ video encoding that might be used for fingerprinting and identification, thus decreasing the efficiency of the identification process. Most fingerprinting tools are also proprietary in nature, making it difficult to ascertain and evaluate their accuracy andtechnical functionality.

Natural Language Processing for Analyzing Text(37)
Natural Language Processing (NLP) is a computer science technique for parsing text in digital form. The general goal of NLP tools is to ascertain the meaning of a particular text. For ex. tools used by social media companies to analyse text on their platforms. A broad road map of how these NLP tools work is given below:

a) Training corpus
NLP tools are trained using human labeled text. Text is marked for belonging to a particular category or not (for ex. hate speech v. non hate speech). These examples are then used by neural networks to sort out new and unlabeled text based on the target content.

b) Pre-processing of training corpora
The training corpora is pre-processed to numerically represent features such as the words, phrases, and grammatical structures appearing in the text. For ex. spam detection tools might learn words which occur more frequently in spam mails to classify them from non-spam content.

c) Training machine-learning classifier
After the training corpus has been created and annotated with features, this is then used to train a machine-learning classifier.

d) Testing the tool
The final stage is testing and adjusting the tool for errors. Implementers typically test the tool for errors and check for false positives and false negatives. Appropriate tweaks can be made at this stage for avoiding unwanted outcomes.

Limitations of Using NLP Tools for Online Filtering

1. NLP tools work best when applied to specific domains of speech
NLP tools work best when they are applied to specific domains of speech. For ex. a tool which has been trained to determine political hate speech will not be effective for identifying other categories of speech such as child abuse text. A one size-fits-all approach at using text classifiers to filter content will not be effective in purging problematic content of all types.

2. NLP tools further marginalize groups that face discrimination
As with other machine learning tools, NLP tools amplify existing social bias reflected in language. Any bias which is incorporated in the data set used to train NLP tools will be reflected in outputs if not corrected for. If training data sets contain language which discriminates against groups based on gender, race or religion, NLP tools will end up misinterpreting speech and further marginalize minorities. Existing NLP tools are better and more effective for English language text. Reliance placed on these tools will disproportionately affect non-English speakers. Since, India is a country of many languages, NLP tools may end up censoring and misinterpreting non-English languages.

3. NLP tools require clear and precise definitions of targeted speech
Often, the kind of speech which is required to be purged from platforms such as – hate speech and other types of discriminatory speech on the lines of gender, race or religion do not have clear and precise definitions. The illegality or extremist nature of such speech heavily depends on context. NLP tools work best when the input data which is used to train them is clear and consistent. There is an inherent anomaly here as it is hard to restrict definitions of extreme speech as it covers a vast category of instances and NLP tools do not work effectively in un-defined territories.

(38) Ibid.

4. NLP tools are easy to evade

Though their complexity grows with innovation and technology, the success of NLP tools is currently heavily dependent on input data. Meaning of language is deeply interlinked with contextual elements like – tone, speaker, audience, and forum. Because of their limitations, NLP tools are easy to evade for bad actors who know how they work.

The biggest problem with any filtering technique remains that each one of them has limitations and loopholes bad actors and motivated persons can exploit. For media content files, manipulations of the original file can easily help bypass filters. Further, media content filters will only be accurate if platforms have access to the underlying content alongside other tagged details such as hash functions or fingerprinting data.

Similarly with NLP tools for text speech, policy makers stressing on automated filtering of illegal content will end up censoring innocent speech on the Internet due to the limitations of speech determination and inefficiency of these tools on non-English languages.

The above referenced study conducted by the Center for Democracy and Technology(38) found that Natural Language processing tools require clear, consistent definitions of the type of speech to be identified and screening of social media content based on poorly defined categories is not likely to be successful. The study recommends that use of automated content analysis tools to detect or remove illegal content should never be mandated in law.

Some other issues with mandating upload filters in law are - affordability of sophisticated filtering tools by smaller companies, outsourcing speech policing to private companies leading to censorship, codified privacy violation due to constant monitoring, dilution of safe-harbour protection to intermediaries – which will negatively affect the platform economy on the Internet, and non-purging of illegal data floating on P2P sharing networks and the dark net.

1.4 One - Size Fits All Approach

The proposed rules do not distinguish between categories of intermediaries or size of intermediaries in mandating the use of automated filters. A platform like Facebook is quite different from an encrypted messaging platform like WhatsApp and these are different from a Telecom Service Provider, although all fall under the definition of 'intermediary' under the IT Act. The one size fits all approach will result in forcing a number of businesses ranging from shopping sites to blogging platforms to cab aggregators to review websites to install automated filters.

Moreover, there are many applications like Mastodon and Diaspora which are Free and Open Source Software (FOSS) and instances (servers) of such applications are managed by various communities of software developers and even by individuals. Recently, there was a large exodus of users from Twitter to decentralised platforms like Mastodon(39). As these tools do not use automate filters, these regulations will result in such communities being saddled with liability for usergenerated content.

Recently, a report in Reuters(40), pointed to a possibility where the Indian government could split the Draft Intermediaries Guidelines into a 'two-tier system' wherein, the more stringent rules will be specifically made applicable to social media companies and not all intermediaries as envisaged previously. The government through its MeitY, hasn't released the latest version of Draft Intermediaries Guidelines and it remains to be seen whether such changes see the light of day.

1.5 International Debate on Upload-Filters

In June 2018, the Special Rapporteur to the UN on the promotion and protection of the right to freedom of opinion and expression, David Kaye, wrote

---

(39) Toots not tweets: India's Twitter users are angry – and this chart from Mastadon shows it - *https://scroll.in/article/943455/toots-not-tweets-indias-twitter-users-are-angry-and-this-chart-from-mastadon-shows-it (Scroll, India)*

(40) India to tweak proposed content regulations to ease burden on some – sources - *https://in.reuters.com/article/indiasocialmedia/*india-to-tweak-proposed-content-regulations-to-ease-burden-on-some-sources-idINKBN1Z71Q2 (Reuters)

to the European Commission(41) expressing his concerns with the EU Copyright Directive. Pointing to Article 13, (Article 17 in the final version of the law) Mr. Kaye stated that requiring content-sharing platforms to use upload filters will incentivise them to restrict perfectly legitimate and lawful speech at the point of upload and will restrict freedom of expression on the Internet without prior judicial review of the legality, necessity and proportionality of such restriction.

In his letter he argued that filtering technologies are not equipped to perform context sensitive interpretations - *"... Exacerbating these concerns is the reality that content filtering technologies are not equipped to perform context-sensitive interpretations of the valid scope of limitations and exceptions to copyright, such as fair comment or reporting, teaching, criticism, satire and parody."*

Referring to the impact of mandating the use of filtering technology on small and medium businesses, a letter addressed to the President of the European Parliament in June 2018 by Internet pioneers like Vint Cerf, Tim Berners-Lee (inventor of the world wide web), and Jimmy Wales (cofounder of the Wikimedia Foundation) (among other luminaries)(42), pointed to the impact of the EU Copyright Directive on the open architecture of the Internet. The signatories also expressed their concerns about the impact of upload filters on ordinary Internet users. The letter stated that users often rely on copyright exceptions while uploading music or video and that upload filters will impact such legitimate speech. Contributors on platforms like Wikipedia and GitHub, which are open collaborative tools, will get negatively impacted by automated filters.

Mozilla in its statement on the EU Copyright Directive and its mandate to use upload filters, expressed concern over how these legal requirements will impact SMEs and will undermine access to knowledge and sharing on the Internet - *"The new rules that MEPs are set to adopt will compel online services to implement blanket upload filters, with an overly complex and limited SME carve out that will be unworkable in practice. At the same time, lawmakers have forced through a new ancillary copyright for press publishers, a regressive and disproven measure that will undermine access to knowledge and the sharing of information online."*(43)

Recently, the Court of Justice of the European Union ("the CJEU") delivered a judgment(44) approving global take down of content from social media platforms like Facebook and declared that according to EU law, regional courts may require platforms to purge content which has been previously been declared illegal if it is substantially similar. Though, the court made it clear that this was not to mean a general monitoring requirement on social media platforms, monitoring for specific content was held to be legal. This requirement to specifically monitor and purge out illegal content raises privacy concerns and places a strict obligation on social media platforms to pre-filter and scan each piece of uploaded content. In addition to privacy risks due to such requirements, upload filters will lead to censoring of legitimate speech online.

This collective expression of concern over the legal mandate of deploying upload filters points to the recurring theme of issues with filtering technology and its negative effect on free expression and privacy. Despite public opposition to automated filters, the EU Parliament passed the EU Copyright Directive with the requirement of making 'best efforts to ensure unavailability of content protected by copyright without due authorisation' and 'make best efforts to prevent their future uploads'.

---

(41) UN Special Rapporteur on Free Speech, David Kaye's letter to the European Comission - *https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-OTH-41-2018.pdf*
(42) Letter sent to the President of the European Parliament expressing concerns with the EU Copyright Directive - *https://www.eff.org/files/2018/06/12/article13letter.pdf*
access to knowledge and the sharing of information online."
(43) Mozilla's statement on the EU Copyright Directive can be found here - *https://blog.mozilla.org/netpolicy/2019/03/25/eu-copyright-reform-a-missed-opportunity/*
(44) Refer to Eva Glawischnig-Piesczek v. Facebook Ireland Limited (CJEU 2019), available here - *http://curia.europa.eu/juris/document/document.jsftext=&docid=218621&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5315653*

Not just in India, but nation states around the world are imposing or are threatening to enact laws which will make online intermediaries responsible for illegal content on their platforms. Governments want Internet platforms to either pre-censor or expeditiously take content down without the application of judicial mind or procedural safeguards to ensure due process of law. In the wake of the Christchurch killings, Australia has enacted a law(45) (Sharing of Abhorrent Violent Material Bill, 2019) which will indirectly force platforms to use filtering technology to take down 'abhorrent violent material' - like other terrorist content regulations, this term is not properly defined. Similarly, on October 2, 2019 Singapore brought its 'fake news' law into effect(46). Under this law, social media platforms will be required to delete or correct government approved falsehoods or face fines upto SGD $ 1 Million – such laws will have the effect of severely undermining free speech online. Earlier this year, the UK published a detailed white paper on 'Online Harms'(47). This paper recommends making Internet companies like social networks, search engines, and messaging services responsible for illegal content. Such suggestions will make these companies ramp up their efforts to use filtering technology which will in turn dilute online free speech.

Another infamous law is EU's Terrorist Content Regulation(48) – which is aimed at regulating terrorist content online. With risks such as – a vague definition of terrorist content, private determination of illegality, and devoid of substantial proof whether blocking such content will actually ebb its dissemination, experts have called out the draft regulation and criticised(49) it for negatively affecting free speech online.

1.6 Insights from Stakeholder Interviews on Upload Filters

- The provision for using automated filters for proactively removing content must not be made mandatory for all intermediaries. All intermediaries don't have the capacity to deploy expensive filtering mechanisms, if enacted this will disproportionately affect service providers operating at a smaller scale.
- A provision to deploy automated filters for removing content should be on a 'best-efforts' basis, which does not mandate the requirement on all types of intermediaries.
- The requirement to deploy automated filters for all types of intermediaries will negatively impact collaboration on the Internet. There are online tools which function on the principle of open collaboration, such tools will lose their uniqueness due to mandatory filtering.
- If illegal content would be required to be taken off globally based on automated filters, this would drastically affect free speech and access to information rights on the Internet. Differential standards of speech around the world will create conflict in laws.
- Automation on the Internet shall be directed at creation of knowledge and not destruction of information.
- The Internet is a cohesive unit, different services rely on each other for their reach. The restrictions on speech and information as a result of mandating automated filters will not only affect a few services, but the Internet ecosystem as a whole.
- There can be specific requirements for content like – child exploitative imagery and terrorist content. For terrorist content too, it is essential to understand context. Matters of public importance should not get filtered out due to a vague filtering requirement.

1.7 Policy Recommendation for Upload Filters

Technological tools for purging illegal content from online platforms should not be mandated under law. These tools are known to be ineffective, enhance existing biases and further margianalize existing minority groups.

---

(45) The Sharing of Abhorrent Violent Material Bill, 2019, can be accessed here - *https://www.legislation.gov.au/Details/C2019A00038*

(46) The Singapore law, Protection from Online Falsehoods and Manipulation Act, 2019, can be accessed here - *https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625*

(47) The UK Online Harms White Paper can be accessed here - *https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper(48)* The EU Terrotist Content Regulation can be accessed here - *https://eur-lex.europa.eu/resource.html?uri=cellar:dc0b5b0f-b65f-11e8-99ee-01aa75ed71a1.0001.02/DOC_1&format=PDF*

(49) Mozilla's statement on the EU Terrorist Content Regulation - *https://blog.mozilla.org/netpolicy/2019/02/13/terrorist_content_regulation/free speech online.*

CHAPTER 2

2. TRACEABILITY

The Draft Intermediaries Guidelines were purportedly brought in to tackle the issues of misinformation(50) being spread through messaging services like WhatsApp that resulted in mob lynchings across India. The Draft Intermediaries Guidelines mandate that *"the intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised."*

Traceability is a feature, proposed to be implemented within messaging applications/ platforms of intermediaries, and is aimed to identify the originator of any message posted or spread within the platform. The word 'originator' has been defined in Section 2(za) of the IT Act as follows:

"...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"

Through the above mentioned sub-rule of the Draft Intermediaries Guidelines, the State seeks the implementation of a specific feature in the services offered by intermediaries where the intermediary is able to trace out the originator of information (includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche) within the intermediary's platform or service.

Once the Draft Intermediaries Guidelines were published in December, 2018, respondents, in the rounds of public consultation to draft guidelines pointed out the impact such a provision would have on the fundamental right to online privacy.(51)

The debate on whether to enable traceability or not, is essentially not confined to the Indian context but is tied with the larger global debate on whether law enforcement should get access to encrypted text (or plaintext information).

(50) (Supra) Note 19
(51) (Supra) Note 20

2.1 Court Cases on Traceability

In 2018, petitions were filed and moved in the High Court of Madras (W. P. 20214/2018 & W. P. 20774/2018) petitioning the court to direct social networking services to link user accounts with their Aadhaar cards in order for law enforcement agencies to track and indict cyber offenders. The petitions were filed by animal activists who faced cyberbullying from a social media page and faced difficulties in resolving the identities of the perpetrators. Janani Krishnamurthy(52) and Antony Clement Rubin(53) filed a petition before the Madras High Court to direct the government to link Aadhaar or any government ID of users with their accounts on the platforms and also to form a committee to handle such issues. Similar petitions were also filed in the Bombay, and Madhya Pradesh (at Jabalpur) High Courts during this time.

The Madras High Court eventually decided against linking Aadhaar with social media accounts on the basis of the 2018 Supreme Court decision that Aadhaar can only be linked with social welfare schemes of the government. However, the case forked into a matter to resolve whether enabling traceability within applications such as WhatsApp is possible, given the E2EE feature enabled by default within the application. Thus, the Madras High Court enlarged the scope of the writ petition to address the question of identifying originators of messages within the messaging platform. Also, the court sought the assistance of Prof. V. Kamakoti, a professor at IIT-Madras and also a member of the Prime Minister's scientific advisory committee in ascertaining whether it is technically possible to enable traceability as a feature within WhatsApp. Pursuant to the court's query, Prof. Kamakoti submitted a proposal outlining the possibility of enabling traceability in WhatsApp. Enabling traceability as proposed by Prof. Kamakoti in the WhatsApp traceability case in the Madras High Court, has drawn flak(54) and also approval(55) from different experts. However, WhatsApp has denied the feasibility of Prof. Kamakoti's solution(56) and also stated that it won't solve the issue of correctly identifying the originator of a message.

Subsequently, technology companies such as WhatsApp, Google, YouTube, and Facebook were impleaded in the matter. The primary argument of WhatsApp was that it was impossible to track the originator of any sender due to the fact that WhatsApp employed E2EE technology in its messaging platform. This prevented WhatsApp from possessing any decryption keys for the messages being sent within the platform. WhatsApp submitted before court that they only had access to basic user information.

In the meantime, Facebook/ WhatsApp, a respondent in the Madras High Court and in matters across different High Courts in India, approached the Supreme Court to transfer all matters, relating to the traceability issue, to the Supreme Court and resolve them together. The Supreme Court noted that the main issue arising in the petitions was how and in what manner the intermediaries should provide information including the names of the originators of any message/ content/ information shared on the platforms run by the intermediaries. During the course of the hearings, the

---

(52) "Why Aadhaar-social media linkage petitioner Janani Krishnamurthy wants traceability", *https://www.medianama.com/2019/08/223-why-aadhaar-social-media-linkage-petitioner-janani-krishnamurthy-want-traceability/*

(53) "Why Antony Clement Rubin petitioned Madras HC to link Aadhaar to social media accounts", *https://www.medianama.com/2019/07/223-why-antony-clement-rubin-petitioned-madras-hc-to-link-aadhaar-to-socialmedia-accounts /*

(54) "Dr Kamakoti's solution for WhatsApp traceability without breaking encryption is erroneous and not feasible", *https://www.medianama.com/2019/08/223-kamakoti-solution-for-traceabilitywhatsapp-encryption-madras-anand-venkatanarayanan/*

(55) "Battle for privacy and encryption: WhatsApp and government head for a showdown on access to messages", *https://prime.economictimes.indiatimes.com/news/71367088/corporate-governance/battle-for-privacy-and-encryption-whatsapp*-and-government-head-for-a-showdown-on-access-to-messages

(56) "Exclusive: WhatsApp's response to Dr Kamakoti's submission", *https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/*

The following table reflects the relevant cases that are pending pertaining the issue

Litigation Re: Traceability

S. No.	Case Name	Court	Case No.	Status
1	*Janani Krishnamurthy v. Union of India & Others*	*Madras High Court*	*W. P. 20214/2018*	*By order dated 24.10.2019, the Supreme Court has directed these matters to be transferred to the Supreme Court.*
2	*Janani Krishnamurthy v. Union of India & Others*	*Madras High Court*	*W. P. 20774/2018*	
3	*Sagar Rajabhau Surywanshi v. Union of India*	*Bombay High Court*	*PIL/147/2018*	*Withdrawn as the petitioner submitted in the court that the petitioner wishes to intervene in the matter pending in the Supreme Court.*
4	*Amitabha Gupta v. Union of India*	*High Court of Madhya Pradesh (at Jabalpur)*	*W. P. No. 13076/2019*	*The matters, along with the transferred matters are to be listed on January 30th, 2020*
5	*Facebook Inc. v. Union of India*	*Supreme Court of India*	*T. P. (C) No. 001943 - 001946/2019*	
6	*Facebook Inc. v. Antony Clement Rubin*	*Supreme Court of India*	*Diary No. 32478/2019*	
7	*WhatsApp Inc. v. Janani Krishnamurthy*	*Supreme Court of India*	*Diary No. 32487/2019*	

Government of India submitted that the Draft Intermediaries Guidelines were under consideration and through its affidavit submitted that the Guidelines will be notified in January, 2020. On 24.10.2019, the Supreme Court ordered that all pending cases related to the issue of traceability be transferred before it.

In the WhatsApp traceability case, the primary question that the court is trying to resolve is whether any feature could be added to the WhatsApp platform so as to enable tracing out the originator of any message.

Enabling traceability of messages would affect E2EE of the platform as per a spokesperson from the company(57). Any demand for enabling traceability into a communication platform which provides E2EE is a strike at encryption itself because platforms that provide such encryption do not have access to the content and the originator of the message and in order to access that it has to weaken the encryption or install a back-door. There are proponents of the argument that traceability can be enabled without having to break E2EE. However, there is no consensus on that argument and the mandate to enable traceability is seen as an attack on encryption as a whole.

2.2 Prof. Kamakoti's Solutions

Prof. Kamakoti, submitted to the Madras High Court an expert opinion titled 'Report on Originator traceability in WhatsApp messages'(58) which suggested two methods by which the originator can be traced out without breaking encryption. The first method, that he suggested essentially proposes that every time a message is created in WhatsApp, the user who creates the message shall be designated as the 'originator' of the message and the originator information (metadata) and the message are encrypted and sent together to every recipient. Every receipient of the forwarded message shall receive the originator information and can be decrypted by their device. In this method, he states that when the original message is modified (by adding a picture or a video or copying or pasting the original message), the user that brings about the modification will be designated as the 'originator'.

As per Prof. Kamakoti's second method (this he had put forth in case the Madras High Court was not willing to let originator information be disclosed to everyone), he propsed that every time a message is created in WhatsApp, the originator information is encrypted with the message using a private-public key pair. However, the key pair is to be generated by WhatsApp servers and the private key is to be retained by WhatsApp in escrow. In effect, Prof. Kamakoti's second solution suggests that only WhatsApp can know the originator of the message and can decrypt such information at the request of law enforcement agencies. Both the methods suggested by Prof. Kamakoti suggests revealing the originator and embedding such information with the message. However, these solutions have been commented upon by WhatsApp and others to be erroneous on different counts.

In another expert opinion submitted by one of the intervenors(59), supplied by IIT Bombay's professor Manoj Prabhakaran, the solutions offered by Prof. Kamakoti were questioned of their implications on user privacy and also raised concerns regarding their effectiveness. Mr. Prabhakaran ends his opinion commenting that including a mechanism for traceability is a mild modification to the WhatsApp ecosystem, however is skeptical of its long term effectiveness. He also points out that the solutions offered by Prof. Kamakoti can be thwarted by non-technical methods such as hiring proxy originators, and also the technical method of reverse engineering the WhatsApp client.

---

(57) WhatsApp Rejects India's Demand For Message Traceability *https://www.ndtv.com/india-news/whatsapp-rejects-indias-demand-for-message-traceability-1905217*

(58) 'Report on Originator traceability in WhatsApp messages', https://docs.google.com/viewerng/viewer?url=*https://www.medianama.com/wp-content/uploads/Dr-Kamakotisubmission-for-WhatsApp-traceability-case-1.pdf&hl=en*

(59) 'On a Proposal for Originator Tracing in WhatsApp', *https://drive.google.com/file/d/1B2ShWywwVpPX1zTz25UgPMSOokZbcJBx/view*

In WhatsApp's response(60) to the solutions offered by Prof. Kamakoti, both solutions were criticised for lacking effectiveness and also for potentially disrupting WhatsApp's infrastructure. The challenges pointed out by WhatsApp are - the technical implementation and also the practical difficulty of implementing the feature for its huge database and its selective implementation only for Indian citizens, when WhatsApp's system is not designed to verify a user's nationality.

2.3 Global Perspective

The traceability issue, though centered around the WhatsApp traceability question is not essentially Indian. Neither is it recent. In 2015 and 2016, the world witnessed a standoff between Apple Inc. and FBI, in which Apple refused to develop and install specific software to access an encrypted iPhone when it was requested by the FBI pursuant to an order by a US magistrate directing Apple to assist the FBI for an investigation. The iPhone in question allegedly belonged to one of the attackers of the 2015 San Bernardino terrorist attack. Apple refused to install a back-door into the iPhone to enable the FBI access to the phone's data. Eventually, the FBI backed-off from the demand by employing a third party solution.

This was not the first time debates and concerns over encryption have occurred. Nor is this is the first time methods have been considered to create back-doors to communication systems.(61) Now, world over, governments are trying to force companies to provide access to messages that are allegedly communicated by perpetrators of serious offences such as terrorism, illegal narcotics trade, and the sexual exploitation and abuse of children.

Recently, the US-UK governments entered into a executive Data Access Agreement(62), under the US Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018 that will allow duly authorised US and UK law enforcement agencies to ask technology companies based in their partner country for electronic data related to serious crimes, such as terrorism, sexual abuse of children, and cybercrimes. This is intended to boost the speed of legal assistance on the occurrence of such aforementioned crimes without having to approach the government of the tech company's parent country.

In the meantime, the US, UK and Australian governments issued an open-letter(63) to Mark Zuckerberg urging the founder of Facebook to retract from the company's plan to enable encryption across all its platforms. As published by the Guardian, through the letter the governments have demanded Facebook (and other companies) to take the following steps:

" Embed the safety of the public in system designs, thereby enabling you to continue to act against illegal content effectively with no reduction to safety, and facilitating the prosecution of offenders and safeguarding of victims;*

** Enable law enforcement to obtain lawful access to content in a readable and usable format;*

** Engage in consultation with governments to facilitate this in a way that is substantive and genuinely influences your design decisions; and*

** Not implement the proposed changes until you can ensure that the systems you would apply to maintain the safety of your users are fully tested and operational."*

This open letter has received much disapproval from the international community and this act is seen as a threat to encrypted commu-

---

(60) 'WhatsApp's response to Dr. Kamakoti's submission', *https://www.medianama.com/2019/08/223-exclusivewhatsapps-response-kamakotis-submission/*

(61) "Nervous System: Clipping the Wings of the Clipper Chip", *https://www.law.com/legaltechnews/2019/09/03/nervous-system-clipping-the-wings-of-the-clipper-chip/?slreturn=20191103062952*

(62) "Cloud Act Resources", *https://www.justice.gov/dag/cloudact*

(63) *"US/UK/Australia letter to Zuckerberg 10.4.19", https://www.documentcloud.org/documents/6450624-US-UKAustralia-letter-to-Zuckerberg-10-4-19.html*

nication services. It is not hard to predict that other countries will rely on the same arguments raised by the US, UK and Australia in the open letter to Mr. Zuckerberg. Germany, has followed suit in calling Facebook to refrain from incorporating encryption into its platforms.(64) Germany, like its allies, is also pushing for back-door access to encrypted messages in Facebook's platforms.

The argument raised in favour of providing back-door access to encrypted messages is that law enforcement agencies in these countries would want to trace down and indict perpetrators of serious crimes such as terrorism and sexual abuse of children.

In Australia, a broad amendment Act titled, the Telecommunications and Other Legislation Amendment (Assistance and Access) Act, 2018(65) ("the Australian Assistance and Access Act") which is designed to enable law enforcement agencies to get access to encrypted data in relation to investigations into the conduct of serious crimes was passed in 2018. This law, has also received much criticism from different quarters and concern has been raised regarding the future of encryption in Australia. Though, the act enables judicial oversight, there are chances that the act

might get amended(66).

2.4 Legal Issues and Implications

The cardinal question that snares the traceability debate is whether the State has the power under law to mandate traceability as a feature upon intermediaries. Traceability of users of intermediaries, arguably goes beyond the rule making power of the government and cannot be mandated.

Firstly, the intermediary liability law in India treats at par almost every enterprise actor that comes under the definition of an 'intermediary'. The mandate of traceability should not be imposed on all kinds of intermediaries if at all a traceability provision is implemented. But before, there is also a need to ascertain whether law under the Constitution of India and other laws enable the State to mandate such a requirement of traceability.

The most concerning aspect of this requirement is how it will affect intermediaries like WhatsApp and Signal that provide personal communication services (over the Internet) which are E2EE i.e. wherein even the service provider does not have access to the content of messages/ information which flows through their platform. For reference,

"WhatsApp's end-to-end encryption ensures only you and the person you're communicatingwith can read what's sent, and nobody in between, not even WhatsApp. Your messages aresecured with locks, and only the recipient and you have the special keys needed to unlockand read your messages. For added protection, every message you send has an unique lock and key."(67)

Introducing a traceability requirement for E2EE services will lead to breaking of such encryption and thus compromising the privacy of individuals making use of such services for their private communication.

In the landmark judgment in *K. S. Puttaswamy v. Union of India*(68) ("the Privacy Judgment"), the Supreme Court of India held that:

"the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III (fundamental rights) of the Constitution."

---

(64) "Germany calls for Facebook to nix encryption plans", *https://www.dw.com/en/germany-calls-for-facebookto-nix-encryption-plans/a-50809450*

(65) "Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018", *https://www.legislation.gov.au/Details/C2018A00148*

(66) "Law in Australia - DLA Piper Global Data Protection Laws of the World", *https://www.dlapiperdataprotection.com/index.html?c2=&c=AU&t=law*

(67) Explanation of the End-to-end encryption used by WhatsApp on its service, available at *https://faq.whatsapp.com/en/android/28030015/*.

(68) K. S. Puttaswamy v. Union of India & Others, (2017) 10 SCC 1

The judgment comprises of six different opinions, but at various points, the judges have held that informational and communicational privacy forms a part of the overall privacy of a person and unauthorised use or use of such information without the informed consent of users violates their privacy.

In his judgment, F. Nariman J. has stated that one of the aspects that a fundamental right to privacy would cover in the Indian context would be,

"Informational privacy which does not deal with a person's body but deals with a person's mind, and therefore recognizes that an individual may have control over the dissemination of material that is personal to him. Unauthorised use of such information may, therefore lead to infringement of this right".(69)

Similarly, S. K. Kaul J. opined that,

"The State must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent it was disclosed. Thus, for e.g., if the posting on social media websites is meant only for a certain audience, which is possible as per tools available, then it cannot be said that all and sundry in public have a right to somehow access that information and make use of it."(70)

D.Y.Chandrachud J. (for himself and three other judges) in his judgment stated that,"Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well."(71)

While discussing the various types of privacy, he observed that communicational and informationalprivacy are a part of nine primary types of privacy(72) -

"communicational privacy which is reflected in enabling an individual to restrict access to communications or control the use of information which is communicated to third parties" and "informational privacy which reflects an interest in preventing information about the self from being disseminated and controlling the extent of access to information."

In *Puttaswamy* (Privacy), the court also established a four-pronged test for the legitimate invasion of the fundamental right to privacy(73):

1. The action must be sanctioned by law;

2. The proposed action must be necessary in a democratic society for a legitimate state aim;

3. The extent of such interference must be proportionate to the need for such interference. There should be a rational nexus between the objects and the means adopted to achieve them; and

4. There must be procedural guarantees against abuse of such interference.(74)

Thus, any regulation proposed by the government, which has the purport of violating the privacy of individuals needs to pass this four-pronged test enunciated by the Supreme Court in the *Puttaswamy* judgment. The traceability requirement proposed under the Draft Intermediaries Guidelines, will not be a proportionate or necessary measure if it has the implication of breaking E2EE on messaging services. The draft guidelines also do not provide any procedural guarantees against the possible abuse of a process like traceability of originator of information, as required by the test laid down in the Puttaswamy (Privacy) judgment.

Section 69 of the IT Act gives powers to authorised representatives of Central and State

---

(69) Ibid, para 81 of Justice Nariman's judgment
(70) Id., para 70 of Justice Kaul's judgment.
(71) Id., para 3 (H) of the Conclusion to Justice Chandrachud's judgment.
(72) Id., para 142 of Justice Chandrachud's judgment.
(73) Id., Justice Chandrachud's judgment representing 4 judges [Conclusion Para 3(H)] clubbed with Justice Kual's judgment (at Para 71), which forms the majority opinion of the Puttaswamy case on this point.
(74) Id., Para 71 of Justice Kaul's judgment.

governments to intercept, monitor, or decrypt information stored in any computer resource(75) in the interest of sovereignty or integrity of India, defence of India, security of the State, public order or for investigation of any offence (among other things). The Rules which lay down the procedure and safeguards for such interception, monitoring and decryption of i formation(76) ("the Interception Rules") authorise the Ministry of Home Affairs and the Home Department of the Central and State governments respectively as the competent government authorities to issue orders for such interception of information.(77) The traceability requirement under Rule 3(5) of the Draft Intermediaries Guidelines, if it intends to break encryption or request intermediaries for decryption of information then such powers already exist under a separate provision of the parent statute (i.e. as per Section 69 of the IT Act). The scope of decryption cannot be enlarged in subordinate legislation under a different provision (i.e. Section 79 of the IT Act in relation to the Draft Rules). The Interception Rules provides the procedure for demanding decryption of any information. As per Rule 17 of these Rules decryption key holder has to disclose such key or provide decryption assistance on receiving a decryption direction. In the case of an E2EE messaging application like WhatsApp or Signal, the platform does not have the decryption key and the key lies only with the user. Thus, the user is the decryption key holder in this case and the intermediary cannot be held responsible for any such direction. Any changes addressing the decryption of information will necessarily have to be amendments to either Section 69 of the IT Act or/ and the Interception Rules notified therein.

Delegated legislation cannot go against the substantive provisions of the statute and they must be read in context of the primary / legislative act. In *ITW Signode India Ltd. v. Collector of Central Excise*(78), the Supreme Court stated that,

"It is a well-settled principle of law that in case of a conflict between a substantive act and delegated legislation, the former shall prevail inasmuch as delegated legislation must be read in the context of the primary / legislative act and not the vice-versa."

Similarly, Section 69B of the IT Act deals with monitoring and collection of traffic data or information for the enhancement of cyber security in the country. The term 'traffic data' as defined under the Section 69B(79) includes any data identifying or purporting to identify any person, location to or from which the communication is transmitted and includes communications origin, destination and time (among other things). The Information Technology (Procedure and Safeguard for monitoring and Collecting Traffic Data or Information) Rules, 2009 provide the procedure and safeguards for monitoring of traffic data under Section 69B. These Rules authorize the Secretary to the Government in the Department of Information Technology under MeitY to pass an order for such monitoring. In as much as Rule 3(5) of the Draft Rules pertains to cyber security, it cannot override and enlarge the scope of Section 69B or the Rules framed under it.

Moreover, as per Rule 13 of the Interception Rules, there is the mandate that intermediaries must provide all facilities, co-operation and assistance for interception or monitoring or decryption. This mandate was discussed on during the admisssion hearings(80) of the transfer petition in the Supreme Court seeking tranfer of cases in the Madras, Bombay, and Madhya Pradesh (at Jabalpur) High Courts which were discussed earlier.

---

(75) The definition of 'computer resource' as per Section 2 (1) (k) of the IT Act: "computer resource means computer, computer system, computer network, data, computer data, base or software".
(76) Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, available at *http://meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf.*

The Attorney General of India, Mr. K. K. Venugopal (who was actually appearing for the state of Tamil Nadu whereas Mr. Tushar Mehta, the Solicitor General of India appeared for the Union), referred to Prof. Kamakoti's solutions and suggested that the government should have an external agency to decrypt information. The Attorney General, went further to say that Rule 13 calls for a mandate on intermediaries from which they cannot digress and cannot seek exemption from liability claiming impossibility to decrypt.

However, it is important to note that the Interception Rules, do not impose such a mandate. The definition clause itself in the 2009 IT Rules Rule 2(g)(i) states as follows:

"...(g) "decryption assistance" means any assistance to--

*(i) allow access, **to the extent possible**, to encrypted information; or..."*
[emphasis supplied]

Also, Rule 13 (3) states as follows:

*"...(3) Any direction of decryption of information issued under rule 3 to intermediary shall be limited to **the extent the information is encrypted by the intermediary or the intermediary has control over the decryption key."***

This exemption was also pointed out by Mr. Mukul Rohatgi who was appearing for Facebook(81) stating that "the intermediary, that is Facebook in the case of WhatsApp (which employs E2EE), does not have the keys!." It is to be inferred from the above two provisions [2(g)(i) and 13 (3)] that legislative intent was to allow intermediaries to deploy services which cannot be decrypted later by the intermediary itself. These discussions still await conclusion in the Supreme Court.

Lastly, the Draft Intermediaries Guidelines seek to expand the powers of the government for law enforcement by replacing the phrase 'government agencies who are lawfully authorised' to 'any government agency'. Such expansion of the scope of powers of the government for investigation or prosecution purposes go beyond the scope of the Intermediaries Guidelines under Section 79 of the IT Act and are changes that need to form a part of the parent legislation. As argued, specific provisions of the IT Act provide for procedural safeguards for enabling access to information by law enforcement agencies. These safeguards are missing in the Draft Intermediaries Guidelines. The draft rules potentially go beyond the scope of Section 79 and other core provisions of the IT Act such as Section 69 and 69B of the IT Act.

In *National Stock Exchange Member* v. *Union of India*(82), the High Court of Delhi held that, "...in every legal system there is a hierarchy of laws, and the general principle is that if there is a conflict between a norm in a higher layer of the hierarchy and a norm in a lower level of the hierarchy, then the norm in the higher layer prevails, and the norm in the lower layer becomes ultra vires" the court elaborated on the hierarchy of laws as: 1) The Constitution of India; 2) Statutory Law; 3) Delegated Legislation; and 4) Administrative Instructions.

Thus, it is clear that subordinate/ delegated legislation cannot go beyond the scope of the substantive provisions of the main law and in the hierarchy of laws, statutory law will always prevail over delegated legislation.

Although Section 87(2)(za) enables the government to come out with rules relating to modes or methods of encryption under Section 84A, no such rules have been issued till now. The government should stop trying to

---

(77) Id. at Rule 3.
(78) ITW Signode India Ltd. v. Collector of Central Excise, (2004) 3 SCC 48
(79) See Explanation appended to Section 69B of the Information Technology Act, 2000.
(80) 'Tamil Nadu govt makes a U-turn on Facebook transfer petition, asks for decryption',
https://www.medianama.com/2019/10/223-whatsapp-traceability-case-transferred-to-supreme-court/
(81) Ibid.
(82) National Stock Exchange Member v. Union of India, 125 (2005) DLT 165

slip through a back-door what cannot be done through the front door.
In the *Privacy*(83) and *Aadhaar*(84) judgments the Supreme Court of India created treatises on the issues of privacy, security, and identity. However the Court did not resolve in clear terms the "right to remain anonymous" or the ability to employ anonymity.

The judgments did affirm the right to privacy as a fundamental right and did discuss its contours. The Privacy judgment held that privacy has distinct connotations including (i) spatial control; (ii) decisional autonomy; and (iii) informational control. Evidently, the right to remain anonymous comes under the purview of informational control. The court drew insights from Jeffrey M. Skopek(85) regarding the distinctions between privacy and anonymity. The court held that:

"Both anonymity and privacy prevent others from gaining access to pieces of personal information yet they do so in opposite ways. Privacy involves hiding information whereas anonymity involves hiding what makes it personal. An unauthorised parting of the medical records of an individual which have been furnished to a hospital will amount to an invasion of privacy. On the other hand, the State may assert a legitimate interest in analysing data borne from hospital records to understand and deal with a public health epidemic such as malaria or dengue to obviate a serious impact on the population. If the State preserves the anonymity of the individual it could legitimately assert a valid State interest in the preservation of public health to design appropriate policy interventions on the basis of the data available to it."

The Supreme Court, however, did not dive into discussing the broader issues of anonymity. So, the court did not dive into discussions regarding the issues surrounding encryption though in the Aadhaar judgment the court talked about the use of encryption for the Aadhaar system such as PKI- 2048 encryption and the fact that it is virtually impossible to decipher the same.

Encryption on the other hand, takes in the facets of privacy and anonymity and enhances them. Essentially, encryption enables privacy, integrity, and identification. Encryption, in communication, ensures that no one who is unauthorised can listen in or read messages which consequentially ensures that no one can tamper with the message being sent and finally it ensures that the receiver of a message can confirm the identity of the sender.

The Electronic Frontier Foundation had submitted comments in 2015 to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on the questions of anonymity and encryption. The comments titled, "Anonymity and Encryption"(86) dives into a comprehensive discussion on the human right to be anonymous and employ encryption for the expression of the right. To quote the comments,

"[a]nonymity is vital for an open and free society. We care about anonymity offline and online because it allows individuals to express unpopular opinions, honest observations, and otherwise unheard complaints. It allows them to avoid potential violent retaliation from those who they may offend, and it plays a central role in the fight to expose crimes and abuses of power."

The traceability requirement is technically impossible to satisfy for many online intermediaries. No country is demanding such a broad level of traceability as envisaged by the Draft Intermediaries Guidelines. Though, traceability dilutes safe-harbour, the conversation around it, including the debate on encryption, is much larger than just safe harbour protection. This affects basic free speech and privacy rights on the Internet. Even on un-encrypted channels,

---

(83) K. S. Puttaswamy v. Union of India & Others, (2017) 10 SCC 1
(84) K. S. Puttaswamy v. Union of India & Others, (2019) 1 SCC 1
(85) Jeffrey M. Skopek, Reasonable Expectations of Anonymity, Virginia Law Review (2015), Vol. 101, at pp. 691-762
(86) "EFF Comments Submitted to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", *https://www.eff.org/document/eff-comments-submitted-united-nations-specialrapporteur-promotion-and-protection-right*

traceability will have the effect of chilling speech. Traceability doesn't only affect smaller players but may also be crippling to larger intermediaries.

2.5 Metadata

Another important issue with mandating traceability within messaging platforms is the usual casualness with which metadata is treated in relation with privacy issues. Metadata is any data that gives information about other data. For example, if person A sends a message to person B, then the content of the message will be data and the data such as the time and date of sending and receiving the message, information about the devices from which the message was sent and received, profile information, etc. would be the metadata. Amassing metadata in large volumes reveals a fabric of information unexpected by average users. Metadata, though ancillary to personal data can reveal behavioral patterns, liking, affiliations and opinions of a user, which are usually not observed and analyzed by the user itself and which is not information that the user would wish to be available publicly.

The view that metadata was not protected from State intrusion (4th amendment protection in the United States of America), was the ground resorted to by the NSA in collecting bulk telephony metadata from Verizon.(87) Aggregating information on an individual was held to be equivalent of search under the 4th amendment to the US Constitution by the US Supreme Court in United States v. Jones.(88) Metadata can potentially reveal more personal and intimate information than what actual personal data can sometimes reveal though the contents of the message which constitutes personal data will not be revealed in the metadata. To illustrate, imagine if one were to see the call/ email records of a person being contacted by a health clinic through email, and him calling a doctor and forwarding the email from the health clinic and him contacting his insurance company, and his probate lawyer on the same day in sequence. Though the contents of the communication between these actors are not visible, they spun a story which may not be true and a person seeing the records can act in prejudice against the man. There is a huge pool of inferences that can be made from metadata amassed in large volumes. Metadata is relied on by almost any Internet company (at the least in the form of metadata collectedby the basic form of HTTP cookies). Law enforcement agencies can plug into corporate silos of metadata or also roll out its own interception, monitoring and decryption systems (in India this is done through the enabling provision of Section 5(2) of the Indian Telegraph Act, 1885). Law enforcement agencies can map out social networking graphs of individuals corroborating amassed metadata, can zoom in on mass surveillance, and when in excess can execute arbitrary and prejudiced enforcement actions such as preventive detention and impose curfews.

2.6 Facebook's Discussions in India

Earlier in 2019, the global head of WhatsApp, Will Cathcart met with the Union Minister for Electronics and Information Technology and assured that the issues of traceability and the appointment of grievance officer for India will be addressed by WhatsApp.(89) This was followed by the visit of Nick Clegg, former Deputy Prime Minister of the UK and the current Vice-President of Facebook's global communications to India to meet with Amit Shah, the Home Minister of India, Ravi Shankar Prasad, the Union Minister for Electronics and Information Technology, and India's National Security Advisor Ajit Doval.(90)

Nick Clegg, in his meeting has not offered a solution to the traceability issue similar to what Prof. Kamakoti has suggested. What Mr. Clegg has suggested is that Facebook/WhatsApp will share metadata with the government regarding suspicious users. Now, this has also unclear aspects as to what will be contents of the metadata that will be shared with government law enforcement agencies. In the meantime, the traceability matters are awaiting resolution in the Supreme Court.

2.7 Insights from Stakeholder Interviews on

Traceability

•The traceability requirement is technically impossible to satisfy for many online intermediaries. No country is demanding such a broad level of traceability as envisaged by the Draft Intermediaries Guidelines.

•Though, traceability dilutes safe-harbour, the conversation around it, including the debate on encryption, is much larger than just safe harbour protection. This affects basic free speech and privacy rights on the Internet. Even on un-encrypted channels, traceability will have the effect of chilling speech.

•Traceability doesn't only affect smaller players but may also be crippling to larger intermediaries.

2.8 Policy Recommendation on Traceability

A requirement of traceability will be in violation of informational privacy, which has beenrecognized as a fundamental right by the Supreme Court in the *Puttaswamy* judgment. Thus, such a provision should be removed from the Draft Intermediaries Guidelines.

---

(87) Joseph D. Mornin, NSA Metadata Collection and the Fourth Amendment, 29 Berkeley Tech. L.J. (2014).

(88) United States v. Jones, 565 U.S. 400 (2012)

(89) "WhatsApp assures India of 'prompt action' on traceability of messages", *https://economictimes.indiatimes.com/tech/internet/whatsapp-assures-india-of-prompt-action-on-traceability-of-messages/articleshow/70400961.cms*

(90) "Battle for privacy and encryption: WhatsApp and government head for a showdown on access to messages", *https://prime.economictimes.indiatimes.com/news/71367088/corporate-governance/battle-for-privacy-and-encryptionwhatsapp-and-government-head-for-a-showdown-on-access-to-message s*

CHAPTER 3

3. LOCAL OFFICE THRESHOLD

The local office threshold requirement under the Draft Intermediaries Guidelines, is evidently the Indian government's response to companies playing the game of "lexi loci server" and the claims ofhaving only a "sales office" in India.

Rule 3 (7) of the Draft Intermediaries Guidelines requires all intermediaries with more than 5 million users in India to be incorporated, have a permanent registered office in India with a physical address and appoint a nodal officer and a senior functionary for 24-hour coordination with Law Enforcement Agencies ("LEA"). The Current Rules do not have such obligations.

For clarity, Rule 3 (7) is reproduced here:

"...(7) The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall:

(i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013;
(ii) have a permanent registered office in India with physical address; and

(iii) Appoint in India, a nodal person of contact and alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules...."

Firstly, there is ambiguity regarding the meaning of "users" under this Rule. This Rule applies to all intermediaries with more than 5 million (50 lakh) users in India. At present there is lack of clarity about what this number of users refers to i.e. whether it refers to daily, monthly or yearly users, or the number of total registered users. To understand the implication of this requirement, reference to the user base of popular messaging apps is pertinent. WhatsApp, India's most popular chatting app, has around 200 million users in India. Relatively newer chatting applications Hike and ShareChat have 100 million and 25 million users respectively. The 5 million users specified in the Draft Intermediaries Guidelines represent a little more than 1% of the Internet user base in India which might bring a substantial number of intermediaries under a new set of compliance requirements. This may cause many start-ups to bear the brunt of high costs stemming from incorporation under Companies Act, 2013.

Additionally, the provision does not cite any reason for putting the number "50 (fifty) lakh" as the threshold limit for triggering the mandate under this provision. An intermediary

with a user base (registered or unregistered) lesser than the mandated number of 50 lakh may still offer a platform which will trigger intermediary liability issues. So, the prescribed number is arbitrary and does not achieve the objective sought to be achieved through the sub-rule. This can also invite problems of illegitimate classification under Article 14 of the Constitution of India where intermediaries with a user base of less than 50 (fifty) lakh can avoid the mandate under this sub-rule and a similar intermediary with a user base more than the prescribed number would have to follow the mandate, when the number set by the draft sub-rule and the resulting classification of intermediaries into two groups based on the number of users does not have any rational nexus with the object sought to be achieved.

Moreover, if the provision is enacted as it stands, there is no prescribed method to determine the actual number of users the intermediary has If the only recourse is to resort to the number published by the intermediary, then it invites the chance of intermediaries fudging the number of users they have to avoid intermediary liability.

The Draft Intermediaries Guidelines stipulate appointment of different officers to ensure compliance with the orders/ requisitions by law enforcement agencies in accordance with provisions of law or rules. To meet this objective, Draft Rule 3(7) requires the intermediary to appoint a nodal officer and a senior functionary for 24-hour coordination with LEA. Draft Rule 3(12) also mandates the appointment of grievance officer to address the complaints against violation of Draft Rule 3. Multiple appointments may increase procedural burdens for intermediaries and create possibilities of overlap in their functions.

Indian business laws offer foreign companies different options of incorporating and conducting business in India. They are offered the options for setting up business in India by either incorporating a company under Companies Act, 2013 or a limited liability partnership under the Limited Liability Partnership Act, 2008. This operational convenience afforded to foreign companies/ businesses are limited by the Draft Intermediaries Guidelines in mandating the incorporation of the business of the intermediary as a company under the Companies Act, 2013. Failure to do so will ascribe liability on the intermediary thus laying burden of additional regulatory compliance. Such restrictions will stifle business in India. This will also cause substantial barriers of entry for businesses that cannot afford incorporation and other consequential requirements of the Companies Act, 2013 and setting up physical offices in India. The convenience available for companies to operate remotely and offer quality services will be under jeopardy if the mandates under the sub-rule are implemented.

These restrictions will adversely affect open source applications like Diaspora and Mastodon which are maintained by Communities of software developers and enthusiasts. Many of these platforms are becoming popular especially with growing dissent against policies of centralised platforms.

3.1 Insights from Stakeholder Interviews on Local Office Threshold

• This is a burdensome compliance, many International entities will not be able to comply with this requirement.The current law in India is sufficient for enforcing requirements with international companies.

• If the government wishes to introduce such a requirement, the threshold must be increased, local office and mandatory company registration removed, and nodal officer should be not mandated to be in India.

3.2 Policy Recommendations on Local Office Threshold

• To avoid confusion created due to multiplicity of authorities, a single officer can be appointed to fulfill compliance with the obligations.

• The provision requiring incorporation of intermediaries can lead to compliance burden and should be made voluntary for intermediaries.

CHAPTER 4

4. 24-HOUR TAKE DOWN

Rule 3(8) of the Draft Intermediaries Guidelines prescribes a 24-hour timeline for removal of content, once notified by a court or an appropriate government agency. The Current Intermediaries Guidelines, as per Rule 3(4) places a responsibility on intermediaries to 'act' within 36-hours of being notified. The draft rules propose to bring this down to 24-hours and make it obligatory for intermediaries to remove content within the stipulated time frame.

The 24-hour take down suggestion in the draft rules isn't a novel recommendation. Germany's Network Enforcement Act of 2017 (popularly known as the 'NetzDG' law)(91) places an obligation on providers of a social network to remove/ block content within 24-hours of notification. The EU's Draft Terrorist Content Regulation(92), which lays down rules for content hosting platforms (including social media) to curb dissemination of terrorist content online makes it mandatory for platforms to remove/ disable content within an hour of notification. Australia's new law to regulate terrorist content online requires intermediaries to 'expeditiously' remove abhorrent violent content.(93) Rule 3(8) of the Draft Intermediaries Guidelines, does not prescribe different timelines for various categories of content such as – terrorist content, child exploitation imagery, defamatory content etc. It does not provide for instances where intermediaries could 'stop the clock' due to challenges in the nature of – erroneous orders or capacity constraints.

Laws in other countries like NetzDG and EU's Draft Terrorist Content Regulation contain procedural safeguards and checks and balances while prescribing strict timelines for content take downs. NetzDG allows social networks to extend the 24-hour/ 7-day timeline in consultation with law enforcement agencies. The 24-hour timeline under NetzDG is only for content that is 'manifestly unlawful' and other categories of unlawful content could be removed within 7 days. Similarly, the Draft Terrorist Content Regulation lays down guidelines for removal orders issued to hosting platforms by authorities. Removal orders must contain specifics like – a statement of reasons for content take downs, URLs for identification of content, information about redress available to hosting platforms and content provider etc. The Regulation also contains provisions for 'stopping the clock' by allowing hosting platforms to intimate the authorities in case they

are unable to comply with the removal order due to de facto impossibility or if the order contains manifest errors.

Smaller intermediaries and community networks, that might not have the institutional capacity to respond in an expedited manner might risk losing their safe-harbour protection increasing the risk of non-compliance multifold. Without a mechanism for 'stopping the clock' this provision might end up disproportionately harming small intermediaries.

Due to the lack of procedural safeguards, a strict obligation to take down content within 24-hours of notification would not just take away the right of the intermediary to reasonable recourse, but would also harm free speech online.

4.1 Insights from Stakeholder Interviews on 24-hour Take Down

• Short timelines for content removal are basically ways of enforcing the automated filtering requirement. With such timelines, purging of content can only happen by using automated filters (which have their various challenges).

• There is no mechanism of stopping the clock or provision for working with authorities in cases where content cannot be taken down within 24-hours of reporting.

• Only bigger companies will be able to take down content within 24 hours, as they have dedicated teams. This will severely impact smaller companies, specially the ones working around the world.

4.2 Policy Recommendations on 24-hour Take Down

• Timelines for content take down orders, which are linked to safe-harbour, must be differentiated according to category of content. Content which has the propensity to cause disproportionately more harm such as – terrorist content or child exploitation imagery could have a stricter time line for take down as compared to categories like defamatory content.

• There must be procedural safeguards, such as – mechanisms to 'stop the clock' in case of disagreement or capacity constraints to account for arbitrary take down orders.

---

(91) Germany's Network Enforcement Act of 2017 - *https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2*

(92) EU's Draft Terrorist Content Regulation - *https://www.europarl.europa.eu/doceo/document/TA-8-2019-0421_EN.pdf*

93 (Supra) Note 45

CONCLUSION

The Government of India (through the MeitY) is poised to notify the Draft Intermediaries Guidelines by the end of January(94). As highlighted, the proposed rules will severely impact the future of India's Internet. The enforcement of the rules, could censor speech and dilute privacy of Indians on the Internet.

Any rules or regulations drafted by the State, which have the effect of limiting the fundamental rights of Indians must follow the doctrines of necessity and proportionality as established by the Supreme Court of India. The Supreme Court in various judgments has also emphasised on the importance of adhering to procedural safeguards, as they ensure procedural justice at the time of limiting or restricting fundamental rights of citizens. There must be a nexus between the objective of the State and the method used to restrict fundamental rights and such means should be the least restrictive in nature.(95)

Recently, the government tabled the Personal Data Protection Bill, 2019 in India's lower house of Parliament, the Lok Sabha. This version of India's premier data protection legislation introduces a mechanism of social media verification, wherein social media companies will be required to provide 'voluntary' modes of verification to their users where they can identify themselves and obtain a mark of verification. Though such requirements of social media verification tools do not belong in a comprehensive data protection framework, these, clubbed with the requirements of traceability and upload filters in Draft Intermediaries Guidelines, will make the Internet a less free and open space in India. These restrictions could also have an adverse impact on innovation, adversely affecting start-ups and the Free and Open Source Software (FOSS) ecosystem. As the draft guidelines are violative of established principles of free speech and privacy, these are sure to be challenged before courts in India.

Both, governments and technology companies, need to make policy changes while taking into account user/ citizen rights and requirements. Currently, specially due to the non-transparent mechanisms technology companies use for regulating content on their services, there is little say users have in the way policies which regulate content are being drawn up. Govern-

ments must ensure that they conduct open and transparent public consultations before bringing out policy changes and tech companies must introduce mechanisms to incorporate user voices when amending internal rules and regulations.

The evolution of technology law and policy in India is heavily influenced by the discourse in Western countries. Recently, the Delhi High Court issued a global take down order for content which was held to be defamatory in India. (96) The court relied heavily on recent judgments of the CJEU in Eva Piesczek(97) v. Facebook and Google v. CNIL(98), where it approved the power of European courts to issue global take down orders. Similarly, the Government of India's stand on bringing in traceability requirements targeting E2EE protected platforms and calls for introducing back-doors in such technology got emboldened by the open letter sent to Facebook by the US, UK and Australia, not to introduce E2EE on all its platforms.

There is a greater need for technology companies, civil society organisations and academia across the world to work together with the governments to ensure that policy developments in the technology sphere do not result in erosion of rights of users in the online space.

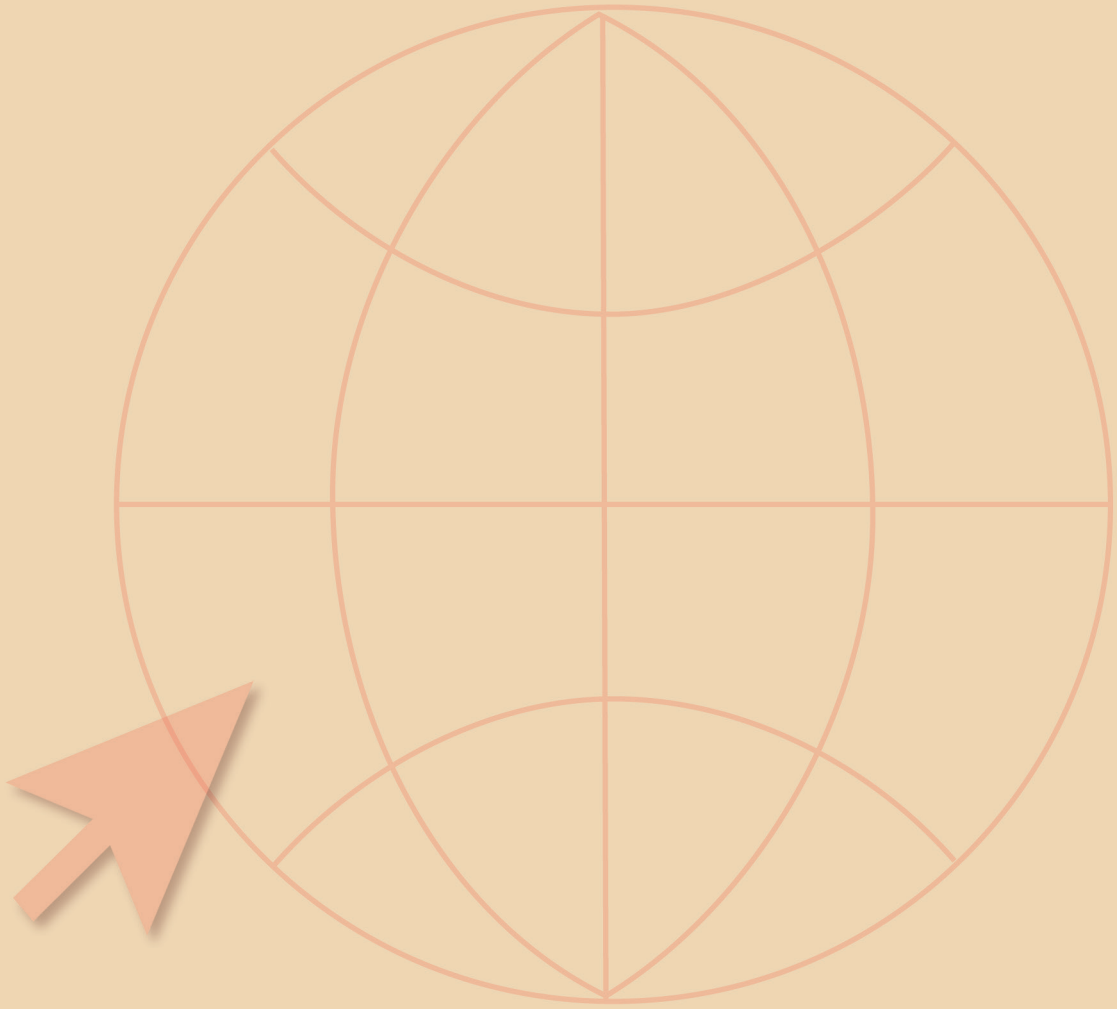
(94) (Supra) Note 40

(95) The doctrines of necessity and proportionality and the importance of procedural safeguards were recently reiterated by the Supreme Court in the matter of Anuradha Bhasin v. Union of India [Write Petition (Civil) No. 1031 of 2019], while assessing the constitutionality of the Kashmir communications blackout.

(96) An Analysis of Swami Ramdev v. Facebook – The Existential Risk of Global Take Down Orders - *https://sflc.in/detailed-analysis-swami-ramdev-v-facebook-judgment*

(97) Eva Glawischnig-Piesczek v. Facebook Ireland Limited - *http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7636193*

(98) CJEU rules that search engines cannot be asked to de-list information globally under EU right to be forgotten requests - *https://sflc.in/cjeu-rules-search-engines-cannot-be-asked-delist-information-globally-under-eu-right-beforgotten*



sflc.in

SFLC.IN is the first Indian legal services organization tthat works exclusively on technology, law, and policy. As a not-for-profit organization engaged in the empowerment of Indian citizens about their digital freedom and rights, it operates as a collective bringing together different stakeholders to a common platform to further the cause of digital rights. SFLC.in promotes innovation and open access to knowledge by helping policy makers make informed and just decisions regarding the use and adoption of technology. As of 2020 SFLC.in is the only Indian organization to be inducted as a member of the IFEX, a global network to defend the right to freedom of expression and information.

www.sflc.in