Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI SILICON VALLEY BANGALORE SINGAPORE NEW DELHI MUNICH / AMSTERDAM NEW YORK GIFT CITY

Research

Make It or Fake It

Tackling Online Misinformation in India

July 2022

Research

Make It or Fake It

Tackling Online Misinformation in India

July 2022

ndaconnect@nishithdesai.com

Asia-Pacific
Most Innovative Law Firm: 2016
Second Most Innovative Firm: 2019
Most Innovative Indian Law Firm: 2019, 2017, 2016, 2015, 2014

Asia Pacific
Band 1 for Employment, Lifesciences, Tax, TMT:
2021, 2020, 2019, 2018, 2017, 2016, 2015

Tier 1 for Private Equity, Project Development: Telecommunications Networks:
2020, 2019, 2018, 2017, 2014

Deal of the Year: Private Equity, 2020

Asia-Pacific
Tier 1 for Dispute, Tax, Investment Funds, Labour & Employment, TMT, Corporate M&A:
2021, 2020, 2019, 2018, 2017, 2016, 2015, 2014, 2013, 2012

Asia-Pacific
Tier 1 for Government & Regulatory, Tax: 2020, 2019, 2018

Ranked
'Outstanding' for Technology, Labour & Employment, Private Equity, Regulatory, Tax:
2021, 2020, 2019

Global Thought Leader — Vikram Shroff
Thought Leaders, India — Nishith Desai, Vaibhav Parikh, Dr. Milind Antani
Arbitration Guide, 2021 — Vyapak Desai, Sahil Kanuga

Fastest growing M&A Law Firm: 2018

Asia Mena Counsel: In-House Community Firms Survey:
Only Indian Firm for Life Science Practice Sector: 2018

ndaconnect@nishithdesai.com

Disclaimer

Contact

For any help or assistance please email us on **ndaconnect@nishithdesai.com**
or visit us at **www.nishithdesai.com**.

Acknowledgements

Aarushi Jain
aarushi.jain@nishithdesai.com

Indrajeet Sircar
indrajeet.sircar@nishithdesai.com

Gowree Gokhale
gowree.gokhale@nishithdesai.com

Ashish Sodhani
ashish.sodhani@nishithdesai.com

Tanisha Khanna
tanisha.khanna@nishithdesai.com

Contents

Background

Over the past couple of years, the issue of curbing misinformation or "fake news" has featured as one of the top regulatory priorities for Governments across the world.[1] Apart from traditional mediums of consuming news, people have also begun to rely on other channels such as social media platforms and news aggregator platforms to consume news.[2]

While the problem of misinformation has been around since as early as the 16th Century,[3] the urgency with which Governments are viewing the problem stems from the ease of access to information through digital platforms. Here, the general members of the public act as creators and /or distributors of news. There is disintermediation of distribution as also the possibility of virality of content. One study has noted that it may take true stories about 6 times as long to reach 1500 people as it takes for fake stories.[4]

The nature of this issue is such, that there is still no clear definition of fake news. Neither is there any illustrative list of circumstances in which, or the entities and individuals who, should be penalized for misinformation.

India has witnessed several instances where misinformation has led to real-world harm to individuals and communities. These include instances of mob-lynching and Covid-19 pandemic related misinformation.[5] Courts in India were early to recognize the problem. Following a spate of mob lynching incidents, the Supreme Court of India, in the case of *Tehseen S. Poonawalla v. Union of India*,[6] prescribed guidelines to State Governments to pre-empt and redress mob lynching incidents. In its guidelines, the Supreme Court specifically required the police to register a First Information Report (**FIR**) *"under Section 153A*[7] *of the IPC and/or other relevant provisions of law, against persons who disseminate irresponsible and explosive messages and videos having content which is likely to incite mob violence and lynching of any kind."* [8]

1 See, Kalra A., "Exclusive: In heated meeting, India seeks tougher action from U.S. tech giants on fake news", Reuters, 2 February 2022, Available at URL: https://www.reuters.com/world/india/exclusive-heated-meeting-india-seeks-tougher-action-us-tech-giants-fake-news-2022-02-02/

2 See, Krishnan A., India Chapter, Digital News Report 2021, Reuters Institute, Available at URL: https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2021/india

3 See, Standage T., "The True History of Fake News", The 1843 Magazine (The Economist), 5 July 2017; Available at URL: https://www.economist.com/1843/2017/07/05/the-true-history-of-fake-news

4 See, Dizikes P., "Study: On Twitter, Fake News Travels Faster Than True Stories", MIT News, 8 March 2018, Available at URL: https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308

5 See, Keppler D., Mehrotra N., "Misinformation Surges Amid India's Covid-19 Calamity", Associated Press, 14 May 2021, Available at URL: https://apnews.com/article/misinformation-surges-india-covid-c52d04de1c3b2332d572736ee069a495; See also, Menon S., "Coronavirus: The Human Cost of Fake News in India", BBC, 1 July 2020, Available at URL: https://www.bbc.com/news/world-asia-india-53165436

6 See, Tehseen S. Poonawalla v. Union of India, (2018) 9 SCC 501

7 Section 153A of the IPC – Promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony.

8 Ibid.

Since then, the Supreme Court routinely makes observations on the need to curb the dissemination of fake news online.[9] The Government was also called to address the issue in Parliament.[10] These developments have ultimately culminated in the Ministry of Electronics and Information Technology (**MeitY**) issuing the Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021 (**IG & DMEC Rules**) in February 2021.

Although not directly addressing fake news, the IG &DMEC Rules require intermediaries[11] (such as social media platforms) and publishers of news content to undertake certain baseline compliance measures to address the issue of fake news and misinformation.

9 See, Jamiat Ulama-I-Hind & Anr. v Union of India & Anr., W.P.(C) No. 787 of 2020, Ajit Mohan and Ors. v. Legislative Assembly National Capital Territory of Delhi and Others, W.P.(C) No. 1088 of 2020

10 See, Rajya Sabha Expresses Concern Over Social Media Platforms Spreading Fake News, 28 July 2018, Available at URL: https://rstv.nic.in/113588.html

11 Section 2(1)(w) of the Information Technology Act, 2000, defines an "intermediary" as "any person who on behalf of another person receives, stores or transmits (an electronic) record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes"

Dimensions of the Problem of Misinformation

At the outset, it is important to appreciate the difference between 'misinformation' and 'disinformation', terms that are often used interchangeably. While 'misinformation' could refer to all information that is false, irrespective of the intention to mislead the audience, 'disinformation' is the intentional propagation of maliciously false information with the intent to deceive or mislead the audience, such that their subsequent actions are guided by such false information.[1] In that sense, information constituting 'disinformation' forms a sub-set of misinformation, which is intentional or coordinated in nature.

A lot of misinformation/disinformation propagated online is targeted towards re-enforcing existing biases held by people.[2] Amplification of such misinformation is typically motivated by economic and political incentives held by certain actors. At times fake news is also used to harass a particular individual or group of individuals. The emergence of technologies that enable better identification of user preferences and consequently better targeting of content, have enhanced the ability to accurately identify user biases, and consequently manipulate and leverage such biases to pre-determined ends.

User biases can also encourage the dissemination of misinformation in the absence of any perverse incentives. For instance, in the context of an interpersonal communications platform, misinformation is more likely to spread, if the user believes the information presented to him or her, as confirming their existing biases, since in such situations, the user is likely to share such information with other like-minded individuals.

Resultantly, one way of viewing the problem of misinformation, is that it has at least two distinct dimensions. The first, relates to the ability of stakeholders to trace and remove misinformation, and the second relates to the existence of actionable grounds to act against any given piece of misinformation.

The ease of tracing and detection of misinformation is a key determinator of success for strategies to tackle misinformation. Individuals today, have the ability to publish content in the nature of news and disseminate it rapidly through social media platforms. Such misinformation can potentially be traced and acted against. Given that such content is openly accessible, and platforms have visibility over such content and its publishers. However, the same cannot be said of off-platform and cross-platform sharing of misinformation through inter-personal communications platforms, where platforms themselves have little visibility over the content shared, owing to the deployment of privacy-enhancing encryption protocols.[3] Moreover, in the Indian context, the diversity of regional language and dialectic content, and culturally relevant idioms and phrases, can make automated detection of misinformation difficult. Resultantly, strategies to tackle misinformation have to take into consideration the medium and language over which misinformation is disseminated. Low literacy level and lack of awareness around fake news further perpetrates the issue.

1 See, Gebel M., "Misinformation vs. disinformation: What to know about each form of false information, and how to spot them online", Business Insider, 16 January 2021, Available at URL: https://www.businessinsider.in/tech/how-to/misinformation-vs-disinformation-what-to-know-about-each-form-of-false-information-and-how-to-spot-them-online/articleshow/80295200.cms

2 See, Ciampaglia G.L., Menczer F., "Misinformation and biases infect social media, both intentionally and accidentally", The Conversation US, 20 June 2018, Available at URL: https://theconversation.com/misinformation-and-biases-infect-social-media-both-intentionally-and-accidentally-97148

3 See, Barik S., "Explained: What the challenges to end-to-end encryption in India mean for users rights and national security", Entrackr, 8 June, 2021, Available at URL: https://entrackr.com/2021/06/explained-what-the-challenges-to-whatsapp-end-to-end-encryption-in-india/

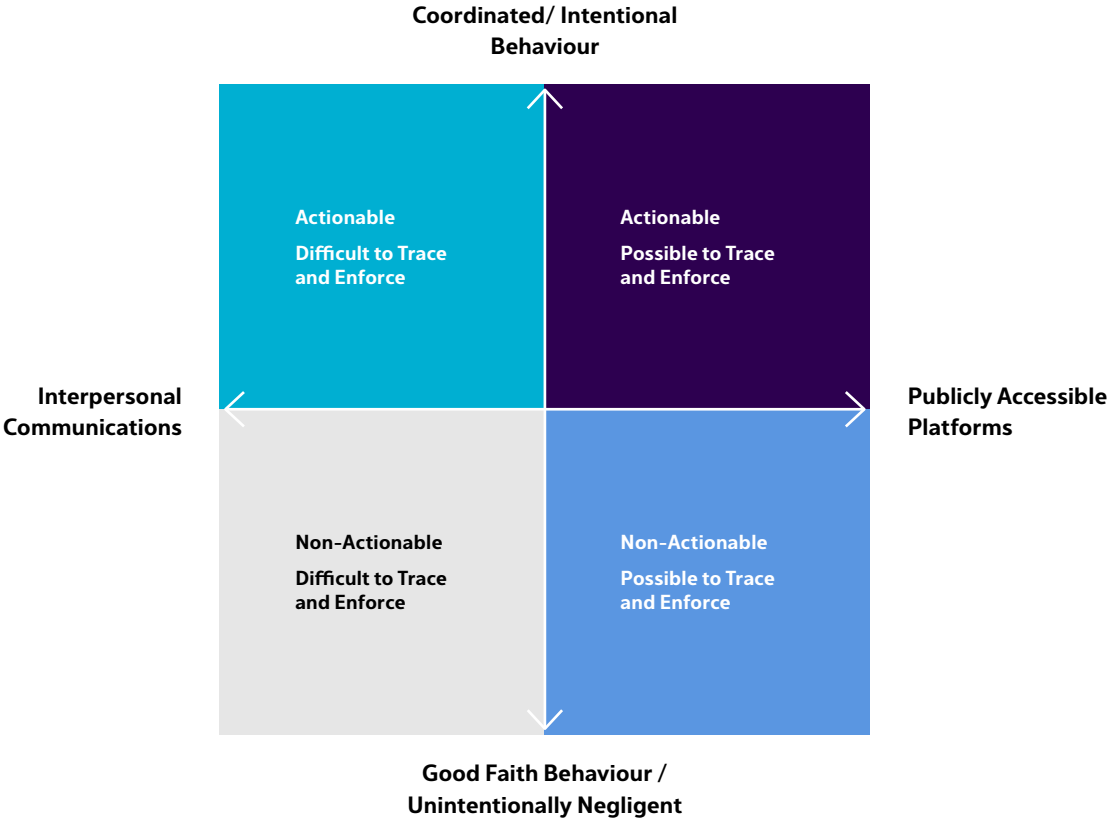


Figure 1: Dimensions of the Problem of Misinformation: Quadrants of Enforceability

The second important factor relates to the actionability of content. While disinformation is more likely to arise from organised or coordinated inauthentic behaviour by certain actors, misinformation may originate either due to lack of knowledge of complete facts or unintentional negligence.

For instance, citizen journalists have routinely taken to video-sharing and micro-blogging platforms to report on-site witness reports for major occurrences,[4] which in turn have been relied upon by law enforcement agencies as evidence.[5] While the mere reporting of facts in itself is unlikely to trigger concerns, any mischaracterisation of facts (including instances where false news is genuinely believed to be true by the user) can be quickly amplified through available online platforms. This can be of particular concern when significant and influential nodes in networked platforms, i.e. users with significant number of connections, followers, etc., share misinformation without prior diligence to confirm accuracy. However, despite any potential implications on public order, in the absence of criminal intent, such content is unlikely to be actionable in view of Constitutional guarantees to freedom of speech and expression. (*See* discussion at page 17 below).

By contrast, certain factions of the society may leverage new technology for spread of targeted and organised disinformation campaigns. While technologies such as AI and Machine Learning may be leveraged to generate "deep fakes" and other forms of manipulated media,[6] online platforms can be misused to amplify such content

4 See, Sharma K., "How Citizen Journalists Documented India's Covid-19 Crisis", Frieze, 25 August, 2021, Available at URL: https://www.frieze.com/article/how-citizen-journalists-documented-indias-covid-19-crisis-2021

5 See, Bergengruen V., Hennigan W.J., "The Capitol Attack Was the Most Documented Crime in History. Will that ensure Justice?", Time, 9 April, 2021, Available at URL: https://time.com/5953486/january-capitol-attack-investigation/

6 See, MIT Media Labs, Detect DeepFakes: How to counteract misinformation created by AI, Available at URL: https://www.media.mit.edu/projects/detect-fakes/overview/

through the use of fake accounts and bots.[7] Such organised disinformation campaigns provide a distinct challenge for Governments across the world, and are likely to require technological solutions developed in collaboration with major online platforms. Under current law, such disinformation would be actionable under applicable criminal law provisions. However, the introduction of additional legal provisions may be required, to tackle disinformation which poses imminent threats to public order, without contravening extant criminal law provisions (*See* discussion at page 17 below).

7 See, Himelein-Wachowiak, M., Giorgi, S., Devoto, A., Rahman, M., Ungar, L., Schwartz, H. A., Epstein, D. H., Leggio, L., & Curtis, B. (2021). Bots and Misinformation Spread on Social Media: Implications for COVID-19. Journal of medical Internet research, 23(5), e26933, Available at URL: https://doi.org/10.2196/26933

Existing Legal and Regulatory Framework in India

Article 19(1)(a) of the Constitution of India bestows upon citizens the fundamental right to freedom of speech and expression. This constitutional right is only available to citizens of India, and is enforceable against the State. This right, however, is not absolute. The Government is permitted to enact laws which impose reasonable restrictions on exercise of this freedom on grounds specified under Article 19(2) of the Constitution, viz. in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or the incitement to an offence. Therefore, any law curbing free speech needs to satisfy this test.

In this context, the Supreme Court's decision in *Shreya Singhal*, is instructive. In this case, Section 66A of the Information Technology Act, 2000 (**IT Act**) was challenged. Section 66A of the IT Act imposed individual liability for sending any information which the sender knows to be false, but sends for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of computer resource or a communication device. The provision was held to be excessively vague and open to arbitrary State action, and resultantly was held to be unconstitutional. It also did not meet the test of reasonable restrictions under Article 19(2) of the Constitution as, according to the Court, the restrictions imposed by Section 66A did to meet the test of substantive and procedural proportionality. The Court further expressed that commission of an offence should be premised upon the existence of *mala fide* intent, and safeguards must be introduced for the protection of unintentional, accidental or good faith transmission of misinformation.

Penal Provisions Applicable to Misinformation

In India, the issue of fake news is attempted to be dealt with largely through (a) existing penal provisions that indirectly deal with "hate speech" and misinformation; (b) the IG & DMEC Rules issued under the IT Act and (c) other laws and codes of self-governance applicable to journalistic reporting, news broadcasting and election-related news.

Notably however, not all items of fake news may get covered under present penal provisions, e.g., when an individual citizen reports certain incidence, it may amount to misinformation (due to a mistaken interpretation of facts), however, it may be difficult to prove *mens rea* (guilty mind) required to establish an offence.

The most commonly invoked provisions flow from the Indian Penal Code (**IPC**), which penalises speech that: (a) amounts to sedition;[1] (b) promotes enmity between different groups on grounds of religion, race, place of birth, residence, language, etc. or that is prejudicial to the maintenance of harmony;[2] (c) makes imputations or assertions prejudicial to national integration;[3] (d) is deliberate, malicious and is intended to outrage religious

1 Section 124A of the IPC; Sedition is defined as speech that attempts to bring into hatred or contempt or excites or attempts to excite disaffection towards the Government established by law in India. In this context, the explanation to Section 124A clarifies that "disaffection" includes includes disloyalty and all feelings of enmity. Sedition does not however include comments expressing disapprobation of the measures or actions (administrative of otherwise) of the Government without exciting or attempting to excite hatred, contempt or disaffection.

2 Section 153A of the IPC

3 Section 153B of the IPC

feelings of any class, by insulting its religion or religious belief;[4] (e) amounts to a statement, rumour or report causing public mischief and enmity, hatred or ill-will between classes.[5]

Other penal provisions which criminalize certain forms of speech, flow from civil rights legislation, that have been enacted to prevent discrimination against classes of persons, and marginalised communities. These include the Protection of Civil Rights Act, 1955 [6] and the Scheduled Caste and Scheduled Tribe (Prevention of Atrocities) Act, 1989 [7], which have been previously invoked with respect to misinformation propagated towards backwards classes through online platforms.

The penal provisions and IG & DMEC Rules discussed above apply to journalist and non-journalist, alike.

Lastly, laws governing electoral speech, such as the Representation of People Act, 1951,[8] also prohibit certain forms of speech which amount to "corrupt practices" with respect to elections. This *inter alia* extends to any speech that is directed at promoting enmity on grounds of religion, race, caste, community or language in connection with election,[9] and deliberate and intentional statements of misinformation directed in relation to the personal character or conduct of any candidate, or in relation to the candidature, or withdrawal, of any candidate, being a statement reasonably calculated to prejudice the prospects of that candidate's election.[10]

Regulation of Journalists and News Publication Houses in relation to Misinformation

The Press Council of India Act, 1978 and the Norms of Journalistic conduct

The Press Council of India Act, 1978 (**PCI Act**) is the primary legislation governing journalism and press activities in India. The PCI Act establishes the Press Council of India (**PCI**) as a governing body, *inter alia* tasked with the objectives of maintaining press independence and framing a journalistic code of conduct for newspapers, news agencies and journalists.

Pursuant to the powers under the PCI Act, the PCI has issued, and periodically updated, the Norms of Journalistic Conduct (**PCI Norms**) .[11] The PCI Norms *inter alia* require journalist to conduct themselves in keeping with certain norms of professionalism such as accuracy and fairness, checking factual accuracy before publishing any news, etc.

Further, under the PCI Act, the PCI is empowered to (either suo-moto or upon receipt of a complaint), hold an inquiry against newspapers, news agencies, editors or journalists, and provide them with an opportunity of

4 Section 295A and 298 of the IPC

5 Sections 505(1) and (2) of the IPC

6 Section 7 of the Protection of Civil Rights Act, 1955 penalises incitement to, and encouragement of untouchability through words, either spoken or written, or by signs or by visible representations or otherwise. Untouchability is the practice of ostracization of communities perceived to be of a "lower caste".

7 Section 3(1)(u) of the Schedule Case and Scheduled Tribes (Prevention of Atrocities) Act, 1989 criminalises speech that promotes or attempts to promote feelings of enmity, hatred or ill-will against members of the Scheduled Castes or the Scheduled Tribes; Section 3(1)(r) criminalises speech that amounts to intentional insult or intimidation with an intent to humiliate a member of a Scheduled Caste or a Scheduled Tribe in any place within public view.

8 Representation of People Act, 1951 (RPA)

9 Section 123(3A) and Section 125 of the RPA

10 Section 123(4) of the RPA; This is also an offence under Section 171G of the IPC

11 Issued under Section 13(2)(b) of the PCI Act ; See, Press Council of India, Norms of Journalistic Conduct, Edition 2019, Available at URL: https://presscouncil.nic.in/WriteReadData/Pdf/NORMSTWOZEROONEININE.pdf

being heard[12]. Notably however, the PCI's powers under the PCA are limited **to censure**. The PCI can take no other deterrent action such as fines, punishment, etc., against violations of the PCI Journalistic Norms. Further, its jurisdiction is excluded in respect of matters in which any proceeding is pending in a court of law.[13]

The scope of PCI's powers was tested in the case of *Mr. Nilesh Navalakha & Ors. v Union of India*[14]. The proceedings, involving several public interest litigations (**PIL**) filed before the High Court of Bombay, raised issues regarding the role of the media in reporting investigations into suicides. The PCI was made a respondent in these proceedings. The PCI submitted before the High Court of Bombay that it could direct the relevant authority to initiate prosecution against any person under the PCI Act[15]. However, during the court proceedings, a notable gap in this framework was also revealed, i.e. the applicability of the PCI Act and the PCI Norms extend **exclusively to print media**. The Bombay High Court temporarily extended the Norms' applicability to electronic media (i.e., television) while reporting on death cases by suicide, till such time appropriate guidelines were framed for electronic media. PCI Act and PCI Norms do not extend to the digital media.

Programme Code issued under the Cable Television Network Regulation Act

The Cable Television Network Regulation Act, 1995 (**CTNR Act**) is the primary legislation regulating the operation of cable television networks in the country. Sections 5 and 6 of the CTNR Act, indirectly regulate broadcasting content, by prohibiting the transmission or re-transmission of television programs and advertisements, that do not confirm to the Program Code and Advertisement Code prescribed by the Central Government under the Cable Television Network Regulation, Act, 1994 (**CTNR Rules**).[16] The Central Government is empowered to order, regulate or prohibit the transmission or re-transmission of programs not in conformity with the Program Code.[17]

Corresponding to the provisions of Sections 5 and 6 of the CTNR Act, Rules 6 and 7 of the CTNR Rules set forth the criteria for determining conformity with the Program Code and Advertisement Code, respectively.[18] Indicatively, the Program Code[19] under Rule 6 of the CTNR Rules *inter alia* prohibits programs which contain anything *"obscene, defamatory, deliberate, false and suggestive innuendos and half-truths"*,[20] or contain content that *"criticizes, maligns or slanders any individual in person or certain groups, segments of social, public and moral life of the country;"*[21]

12 Section 14, PCI Act

13 See, Section 14(3) of the PCA

14 PIL (ST) No. 92252 of 2020

15 Section 15(4) PCI Act

16 See, Section 5 of the CTNR Act, "No person shall transmit or re-transmit through a cable service any programme unless such programme is in conformity with the prescribed programme code"; and Section 6 of the CTNR Act, "No person shall transmit or re-transmit through a cable service any advertisement unless such advertisement is in conformity with the prescribed advertisement code"

17 See, Section 20(3) of the CTNR Act; "Where the Central Government considers that any programme of any channel is not inconformity with the prescribed programme code referred to in section 5 or the prescribed advertisement code referred to in section 6, it may by order, regulate or prohibit the transmission or re-transmission of such programme"

18 See, Rules 6 and 7 of the CTNR Rules.

19 See, Rule 6(1) of the CTNR Rules; The Program Code prohibits the carriage of programs which – (a) Offends against good taste or decency: (b) Contains criticism of friendly countries; (c) Contains attack on religions or communities or visuals or words contemptuous of religious groups or which promote communal attitudes; (d) Contains anything obscene, defamatory, deliberate, false and suggestive innuendos and half-truths; (e) Is likely to encourage or incite violence or contains anything against maintenance of law and order or which promote-anti-national attitudes; (f) Contains anything amounting to contempt of court; (g) Contains aspersions against the integrity of the President and Judiciary; (h) Contains anything affecting the integrity of the Nation; (i) Criticises, maligns or slanders any individual in person or certain groups, segments of social, public and moral life of the country; (j) Encourages superstition or blind belief; (k) Denigrates women through the depiction in any manner of the figure of a women, her form or body or any part thereof in such a way as to have the effect of being indecent, or derogatory to women, or is likely to deprave, corrupt or injure the public morality or morals; (l) Denigrates children; (m) Contains visuals or words which reflect a slandering, ironical and snobbish attitude in the portrayal of certain ethnic, linguistic and regional groups (n) Contravenes the provisions of the Cinematograph Act, 1952; or (o) is not suitable for unrestricted public exhibition.

20 See, Rule 6(1)(d) of the CTNR Rules

21 See, Rule 6(1)(i) of the CTNR Rules

thereby being wide-enough to prevent instances of misinformation or disinformation (including as a part of news content) from being broadcasted over cable television.

Following the notification of the IG & DMEC Rules, the Ministry of Information and Broadcasting (**MIB**) moved to amend the CTNR Rules in June 2021, whereby a three-tiered grievance redressal system, similar to that introduced under Part – III of the IG & DMEC Rules *(See discussion below)* was replicated under the CTNR Rules, i.e. enabling grievance redressal through publishers in the first instance, followed by grievance redressal by self-regulatory bodies (**SRBs**), and ultimately through an oversight mechanism administered by the MIB and an Inter-Departmental Committee (**IDC**).[22]

Notably, the amendments introduced an obligation on the Central Government to afford cable networks with an opportunity to be heard before the IDC established under Rule 20 of the CTNR Rules, prior to establishing non-conformity with the Program Code/ Advertising Code.[23] Based on such hearings, the IDC may, supported by reasons recorded in writing, recommend the Central Government to *inter alia* direct censure,[24] deletion or modification[25] of such programs/advertisements, through appropriate directions issued under Section 20(3) of the CTNR Act.

The amendments to the CTNR Rules also introduce grievance redressal through SRBs, which act as a second level of grievance redressal, to redress grievances not resolved by the publishers in due time, or to address appeals arising out of a publishers' decision.[26] Thus far, two SRBs have registered themselves with the MIB, i.e. the News Broadcasting Federation (**NBF**)'s Professional News Broadcasting Standards' Authority,[27] and the Indian Broadcasting Federation (**IBF**)'s Broadcasting Content Complaints Council (**BCCC**).[28]

IG & DMEC Rules and the Extension of PCI Norms to Digital News Media

While the CTNR Rules were promptly amended to introduce a three-tiered grievance redressal mechanism, it appears that recognizing the regulatory gap relating to the enforcement PCI Norms, the IG & DMEC Rules, tried to address the issue of regulation of digital news media to some extent, through Part – III of the IG & DMEC Rules, to be implemented by the MIB.

Regulatory Mechanism under Part-III of the IG & DMEC Rules

Rule 8 of the IG & DMEC Rules, extends the applicability of Part – III to (a) publishers of news and current affairs content; (b) publishers of online curated content, and (c) with regard to certain provisions (i.e. Rule 15 relating to issuance of directions for deleting, modifying or blocking content; and Rule 16 relating to issuance of emergency orders for blocking content)[29]

22 See, MIB, Cable Television Network (Regulation) (Amendment) Rules, 2021, Notification G.S.R. 416(E), Dated 17 June 2021, Available at URL: https://mib.gov.in/sites/default/files/227661.pdf

23 Ibid., at Clause 2

24 See, Rule 20(4)(i) of the CTNR Rules

25 See, Rule 20(4)(iv) of the CTNR Rules

26 See, Rule 18 of the CTNR Rules

27 See, Letter of Approval of Registration dated 17 August 2021, Available at URL: https://mib.gov.in/sites/default/files/Registration%20of%20NBF-PNBSA%20as%20Self-Regulating%20Body%20under%20Rule%2018%20of%20the%20Cable%20Television%20Networks%20%28Amendment%29%20Rules%2C%202021.pdf

28 See, Letter of Approval of Registration dated 7 July 2021, Available at URL: https://mib.gov.in/sites/default/files/Registration%20of%20BCCC%20as%20Self-Regulating%20Body%20under%20Rule%2018%20of%20the%20Cable%20Television%20Networks%20%28Amendment%29%20Rules%2C%202021.pdf

29 See, Rule 8(1) of the IG & DMEC Rules.

The PCI Norms as well as the Programme Code under Section 5 of the CTNR Act, have been cross-referred in the Code of Ethics provided at the Appendix to the IG & DMEC Rules, thereby extending the applicability of the PCI Norms and the Programme Code to all publishers of news and current affairs content.[30] The applicability of the Part – III of the IG & DMEC Rules can be summarised as follows:

	Indian online news publishers	Offshore online news publishers*	Intermediaries
Observance of applicable codes of ethics,[31]	Yes	Yes	N/A
Furnishing information to MIB**	Yes	No	To inform the users that details of their user account should be furnished to MIB for registration***
To be part of three-tiered grievance redressal mechanism ****	Yes	No	N/A
Furnishing requisite compliance reports to the MIB with regard to their compliance with obligations under Part-III of the IG & DMEC Rules.[32]	Yes	No	N/A

Table 1: Applicability of Part – III of the IG & DMEC Rules

* Publishers, not being in India, but engaging in a systematic business activity of making their content available in India.[33]

** Publishers operating in India are required to inform the MIB about the details of its entity by furnishing information along with such documents as may be specified, for the purpose of enabling communication and coordination. Publisher of news and current affairs content and the publisher of online curated content are required to publish periodic compliance report every month mentioning the details of grievances received and action taken thereto.[34]

*** Intermediaries may voluntarily distinguish such user accounts with an appropriate visible mark of verification, to indicate the authenticity of user accounts operated by publishers of news and current affairs content.[35]

**** a three-tiered grievance redressal mechanism, with the first instance of redressal being implemented by the publisher,[36] and the subsequent levels being implemented through self-regulatory bodies[37] and an inter-ministerial committee established under the IG & DMEC Rules.[38]

30 See, Appendix to the IG & DMEC Rules, Part-I; Publishers of news and current affairs content are required to adhere to the Norms of Journalistic Conduct issued by the Press Council of India under the Press Council of India Act, 1978, and (in the case of broadcast news) the Program Code under Section 5 of the Cable Television Networks (Regulation) Act, 1995. Additionally, publishers are prohibited from publishing or transmitting any content which is prohibited under any laws for the time being in force

31 See, Rules 9(1) and 9(3) of the IG & DMEC Rules

32 See, Rule 18 of the IG & DMEC Rules

33 See, Rule 8(2) of the IG & DMEC Rules; The explanation to Rule 8(2) of the IG & DMEC Rules, defines "systematic business activity" as any structured or organized activity that involves an element of planning, method, continuity or persistence.

34 See, Rule 18 of the IG & DMEC Rules

35 See, Rule 5 of the IG & DMEC Rules

36 See, Rule 11 of the IG & DMEC Rules

37 See, Rule 12 of the IG & DMEC Rules; As on date, five (5) self-regulatory bodies have registered with the MIB, these are: (i) Media9 Digital Media Federation; (ii) The Confederation of Online Media India (COI-I)'s Indian Digital Publishers Content Grievance Council; (iii) The Web Journalists Association of India (WJAI)'s Web Journalists Standards Authority; (iv) The News Broadcasting Federation (NBF)'s Professional News Broadcasting Standards' Authority; and (v) The Internet and Mobile Association of India (IAMAI)'s Digital Publisher Content Grievance's Council, Available at URL: https://mib.gov.in/self-regulatory-bodies

38 See, Rules 13, 14 and 15 of the IG & DMEC Rules

Rules 14, 15 and 16 of the IG & DMEC Rules provide for action that may be taken in relation to non-compliant content published by publishers of news and current affairs content.

- Rule 14 establishes an Inter-Departmental Committee (**IDC**) chaired by the MIB's Authorised Officer,[39] for the purposes of periodically hearing complaints relating to contraventions of the IG & DMEC Rules, i.e., complaints that are referred to the IDC by the MIB, or appeals arising from first two levels of grievance redressal (i.e., by publishers and self-regulatory bodies), including for reasons of inaction. Rule 14 provides the procedures for filing of complaints before the IDC,[40] and requires the MIB to take all reasonable efforts to identify the entity that created/published or hosted the impugned content, and issue them with a duly signed notice to appear before the IDC and submit their reply or clarifications.[41] Based on the hearing, the IDC may issue its recommendations to the MIB. The IDC may *inter alia* recommend deletion/modification of content to prevent inciting the commission a cognizable offence relating to public order; or even recommend blocking of content under Section 69A of the IT Act, where it is satisfied that the grounds for blocking of content under Section 69A are met.[42] The MIB may, subject to the receipt of approval from the Secretary, MIB, issue appropriate directions/orders based on the recommendations of the IDC under Rules 14(6).[43]

- In instances where the recommendations of the IDC call for deletion/modification of content or blocking of content under Section 69A of the IT Act, Rule 15 specifically requires the Authorised Officer of the MIB, to place such recommendations for the consideration of the Secretary, MIB.[44] If approval for such recommendations is received from the Secretary, the Authorised Officer is required to direct the concerned publisher, Government agency or intermediary, to delete, modify or block such content, as the case may be.[45] The Authorised Officer is required to communicate the Secretary's decision to the IDC, if approval for the IDC's recommendations is not granted. Importantly, Rule 15 requires all directions to relate to a specific piece of actionable content or an enumerated list of such content and prohibits the Authorised Officer from compelling a publisher to cease operations.[46]

- Rule 16 enables the MIB to issue emergency orders to publishers or intermediaries to block content, when the need for blocking such content is emergent and appropriate in view of the grounds listed in Section 69A of the IT Act. The Authorised Officer may recommend the emergency blocking of content to the Secretary, MIB.[47] If satisfied that such emergency blocking is necessary or expedient and justifiable, the Secretary may, as an interim measure, issue direction for emergency blocking of content. Directions issued under Rule 16 need to be subsequently placed before the IDC for its recommendations within 48 hours of issuance of the directions.[48] Upon receipt of the recommendations of the IDC, the Secretary is required to pass a final order confirming or revoking the interim direction for blocking of content.

- All directions for blocking of content under Section 69A of the IT Act, which are issued by the Authorised Officer under the IG & DMEC, are subject to review by the Review Committee established under Rule 419A of the Indian Telegraph Rules, 1951.[49]

---

39 See, Rule 14(1) of the IG & DMEC Rules; The IDC is comprised of representatives from the MIB, Ministry of Women and Child Development, Ministry of Law and Justice, Ministry of Home Affairs, Ministry of Electronics and Information Technology, Ministry of External Affairs, Ministry of Defence, and such other Ministries and Organisations, including domain experts, that the MIB may decide to include in the Committee.

40 See, Rule 14(3) of the IG & DMEC Rules; Any complaint referred to the Committee, whether arising out of the grievances or referred to it by the Ministry, shall be in writing and may be sent either by mail or fax or by e-mail signed with electronic signature of the authorised representative of the entity referring the grievance, and the Committee shall ensure that such reference is assigned a number which is recorded along with the date and time of its receipt.

41 See, Rule 14(4) of the IG & DMEC Rules.

42 See, Rule 14(5)(e) and (f) of the IG & DMEC Rules

43 See, Rule 14(6) of the IG & DMEC Rules

44 See, Rule 15(1) of the IG & DMEC Rules

45 See, Rule 15(2) of the IG & DMEC Rules

46 See, Rule 15(3) of the IG & DMEC Rules

47 See, Rule 16(1) of the IG & DMEC Rules

48 See, Rule 16(3) of the IG & DMEC Rules

49 See, Rule 17 of the IG & DMEC Rules

Please refer to Chart at **Annexure – A** for an Overview of the Grievance Redressal Mechanism under the IG & DMEC Rules.

Present status

In separate petitions challenging the constitutional vires of the IG & DMEC Rules, the operation of certain provisions of Part – III of the IG & DMEC Rules, viz. Rules 9(1) and (3), have been stayed by way of separate Orders passed by the Bombay High Court and Madras High Court,.[50] By consequence, the applicability of the PCI Norms to digital media is currently in abeyance. In *Mr. Nilesh Navalakha & Ors.* (*supra*), the Bombay High Court while granting an interim stay on the enforcement of Part - III of the IG & DMEC Rules[51], held that the PCI Norms were framed under a different statutory regime, and independent legislations dealing with such fields could not be introduced under the rules, nor could substantive action for their contravention be taken under the rules. The IG & DMEC Rules have currently been challenged before the Supreme Court.[52]

The MIB continues to enforce certain provisions of the IG & DMEC Rules, to the extent that the same is required to address instances of misinformation by foreign digital news outlets.[53] Relying upon the emergency powers under Rules 16 of the IG & DMEC Rules, the MIB has issued orders to block content that is prejudicial to the grounds specified in Section 69A of the IT Act – both on the publishers' own platforms, as well their channels hosted by intermediaries. Thus, at present the blocking orders with respect to news and current affairs content on the intermediary platforms, can be asked to be blocked by the MeitY as well as MIB. This could lead to duplication of efforts in the event there is no coordination between the two ministries.

Regulation of Digital News Aggregators

Another significant set of stakeholders in the digital news media ecosystem, is news aggregators, who, while not involved in the publication of news and current affairs content (**NCAC**), are responsible for curation and aggregation of NCAC published by other publishers. The IG & DMEC Rules, defines "Publishers of News and Current Affairs Content" as including "news aggregators".[54] In turn, the IG & DMEC Rules defines "news aggregators" as entities that aggregate, curate and present NCAC.

Several intermediaries may meet the requirements of aggregating and presenting NCAC (such as RSS update dashboards), but may not necessarily be *curating* NCAC, i.e. actively selecting content presented on their platforms. Hence, such types of news aggregators should, technically, continue to be intermediaries and should not be categorised as publishers.

In any event, since news aggregators do not originate the content themselves, they should ideally not be subjected to the same compliance requirements as publishers. However, IG & DMEC Rules seem to suggest same level of compliance. E.g., News aggregators cannot be required to comply with Code of Ethics or be expected

50 See, Bhaumik A., "Bombay High Court's Stay on Enforcement of IT Rules 'Code Of Ethics' Against Digital Media Ought to have Pan-India Effect: Madras High Court", Live Law, 16 September 2021, Available at URL: https://www.livelaw.in/top-stories/madras-high-court-it-rules-2021-code-of-ethics-intermediaries-stayed-181762?infinitescroll=1

51 See, Ajit Promotion of Nineteenonea Media Ltd. & Ors. v Union of India & Anr WP (L) No. 14172 of 2021, Nikhil Mangesh Wagle v Union of India PIL (L) No. 14204 of 2021

52 See, Union of India & Anr etc. v Sudesh Kumar Singh & Ors., etc. TP (C) No. 100-105 of 2021

53 See, MIB, Ministry of I&B Blocks Pakistan Funded Fake News Networks, Press Release dated 21 January 2022, Available at URL: https://mib.gov.in/sites/default/files/Press%20release%20dated%2021.01.2022.pdf; See also, MIB, Ministry of Information and Broadcasting orders blocking of Apps, website and social media accounts linked to banned organization Sikhs For Justice, Press Release dated 22 February 2022, Available at URL: https://pib.gov.in/PressReleasePage.aspx?PRID=1800212

54 See, Rule 2(f) of the IG & DMEC Rules

to adhere to a three-tiered grievance redressal procedure. This is because, news aggregators do not originate content, and would therefore not be able to defend the content. Hence, they should only be required to take down content when ordered to do so.

Self-Regulatory Mechanisms Applicable to News Broadcasting

In addition to the above-mentioned rules generally applicable to publishers of news and current affairs content, there are other specific codes of self-regulation, such as the News Broadcasters and Digital Association (**NBDA**)'s Code of Ethics and Broadcasting Standards (**NB Code of Ethics**) which *inter alia* set forth norms on impartiality and objectivity of reporting, depiction and coverage of sensitive issues, considerations of national security, and considerations for viewer feedback.[55]

As a measure of enforcement, alongside the NB Code of Ethics, the NBDA has also adopted the News Broadcasting Standards Regulation (**NBSA Regulations**) which set forth the procedures for enforcing the NB Code of Ethics. The NBSA Regulations,, similar to the IG & DMEC Rules, enable the NBSA to censure, warn or impose monetary penalties on non-compliant members.[56] Past decisions of the NBSA have typically extended to censuring future re-broadcasts of objectionable segments, or removal of objectionable segments from online video-sharing platforms.[57] Notably however, the NBDA's self-regulatory mechanisms have no statutory backing. Resultantly, proceedings before the NBSA do not qualify as to admissions or findings for the purposes of determining civil or criminal liability in proceedings before Courts. In a recent Supreme Court proceeding, the NBDA urged the Supreme Court to issue directions for the incorporation of the NB Code of Ethics in the Program Code, and recognizing the NBSA under the CTNR Rules.[58] As mentioned earlier, recent amendments to the CTNR Rules by way of the issuance of the Cable Television Networks Regulation (Amendment) Rules, 2021 have since enabled the MIB to recognize self-regulatory bodies,[59] however, the NBSA, unlike other SRBs like NBF's PNBSA, is yet to register as a self-regulatory body under the amended CTNR Rules.

Regulation of User-Generated Misinformation

User-generated and transmitted misinformation is a matter of grave concern. In relation to such misinformation, the IT Act, contains two distinct provisions, Sections 69A and 79, wherein any misinformation, whether spread intentionally or not, needs to be blocked if it falls within the categories specified in Article 19 (2) of the Indian Constitution. The constitutionality of these provisions and rules framed thereunder was tested in *Shreya Singhal*

55 See, NBDA, Code of Ethics and Broadcasting Standards, 2008, Available at URL: http://www.nbanewdelhi.com/assets/uploads/pdf/1_CODE_OF_ETHICS_BROADCASTING_STANDARDS_1_4_081.pdf

56 See, NBDA, News Broadcasting Standards Regulation, Available at URL: http://www.nbanewdelhi.com/assets/uploads/pdf/2_News_Broadcasting_Standards_Regulations_1_4_08.pdf

57 See, Orders, NBSA, Available at URL: http://www.nbanewdelhi.com/decisions/orders

58 See, "Make ethics code must for all news channels, broadcasters' body tells Supreme Court", The Hindu, 20 September 2020, Available at URL: https://www.thehindu.com/news/national/make-ethics-code-must-for-all-news-channels-broadcasters-body-tells-supreme-court/article32653265.ece

59 See, Ministry of Information and Broadcasting, Cable Television Networks Regulation (Amendment) Rules, 2021, 17 June 2021, Available at URL: https://upload.indiacode.nic.in/showfile?actid=AC_CEN_29_41_00006_199507_1517807323097&type=rule&filename=cable_television_network_rules_1994_recognized.pdf

v. Union of India.[60] Section 69A and rules thereunder were upheld. As regards Section 79, and the rules issued thereunder, the Court clarified that intermediaries would be obliged to remove or block access to content, only where they have actual knowledge.[61] The rules under Section 79 were further amended in 2021, with the enactment of the IG & DMEC Rules.

Section 69A

Section 69A of the IT Act vests the Government with powers to block public access to information on grounds of *"sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing the incitement to the commission of any cognizable offence relating to the above."* Rules governing the procedural aspects of takedown under Section 69A of the IT Act, including notice, opportunity to show cause, etc, have been set out under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (**IT Blocking Rules**). The IT Blocking Rules are implemented by the MeitY,[62] and overseen by a Review Committee comprising of the Secretaries to the Union Cabinet, Ministry of Law and Justice and the Department of Telecommunications.[63]

Section 79

Section 79 of the IT Act provides intermediaries[64] with a safe harbour from liability with respect to third-party content. In order to qualify for the safe harbour, intermediaries are required to take down unlawful content in an expeditious manner, upon obtaining actual knowledge of such content being hosted on their platforms, by way of a notification from the Government or a Court order. Additionally, Section 79 also requires intermediaries to adhere to certain due diligence requirements. These requirements have been prescribed under the IG & DMEC Rules (and its predecessor the Information Technology (Intermediaries Guidelines) Rules, 2011 (**Old Intermediary Rules**). To this end, Section 79 is similar to Section 230 of the Communications Decency Act in the US, which grants providers of "interactive computer services" an immunity from liability on account of third-party content.[65]

Blocking Request

When Government agencies or the courts believe that the spread of misinformation has an adverse effect on: (a) sovereignty or integrity of India; (b) security of the State; (c) friendly relations with foreign states; (d) public order; or (e) the prevention of instigation to committing any cognizable offence relatable to the grounds under Article 19(2) of the Constitution, they are empowered under the IT Act, IG & DMEC Rules, and the IT Blocking Rules.[66] to notify and direct intermediaries to take down such content. Intermediaries are mandated to take

60 Shreya Singhal v. Union of India, (2015) 5 SCC 1; The Petition filed before the Supreme Court of India, challenged the constitutional validity of Sections 66A, 69A and 79 of the IT Act. The Supreme Court struck down the provisions of Section 66A of the IT Act, which criminalised the transmission of information by a person, who, knowing such information to be false, persistently transmits such information for the purposes of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will. The Court held terms such as "annoyance, inconvenience" as excessively vague, thereby allowing the possibility of arbitrary action. However, the Court upheld the constitutional validity of Sections 69A and 79, since the grounds therein were explicitly tied down to the reasonable restrictions permitted under Article 19(2) of the Constitution and were accompanied by procedural safeguards. The Court read down the provisions of Section 79 of the IT Act, dealing with an intermediary's obligations with regard to third party content hosted on their platform, such that their obligation to remove illegal content would be limited to instances where they obtain actual knowledge of illegality, by way of a Notification from the Government, or by way of a Court order.

61 Ibid.

62 See, Rules 8,9, 10 and 12 of the IT Blocking Rules

63 See, Rule 419A of the Indian Telegraph Rules, 1951

64 Section 2(1)(w) of the IT Act defines an "intermediary" as any person who on behalf of another person receives, stores or transmits an electronic message or provides any service with respect to that message;

65 See, Section 230, Communications Decency Act, Available at URL: https://www.law.cornell.edu/uscode/text/47/230

66 See, Section 69 A or Section 79 of the IT Act read with Rule 3(1)(d) of the IG & DMEC Rules

down such misinformation within 36 hours of receipt of the notification, or any Court Order directing such take-down.[67] The grounds under Section 79 are wider than Section 69-A.

Other Obligations of Intermediaries and Publishers relating to User-Generated Misinformation

Other ex-ante measures incorporated under the IG & DMEC Rules to mitigate the risks of misinformation being hosted on online platforms, include an obligation upon intermediaries to:

- inform users through their terms and conditions not to publish information which (a) is deceptive or misleading about the origin of the content, (b) is patently false or misleading in nature but may be perceived as a fact, (c) is patently false and untrue and published with the intent to mislead/ harass for financial gain or to cause injury to any person; or (d) otherwise inconsistent with any law in force.[68]
- inform users at least once a year that their use of the platform may be terminated, or non-compliant information may be removed in case of non-compliance of these terms.[69]

Voluntary Mechanisms and Codes of Conduct to Tackle Misinformation

Intermediaries are allowed to voluntarily remove non-compliant information either on their own, or on the basis of complaints received, without jeopardising their safe harbour under Section 79 of the IT Act, in line with its terms and conditions. [70]

Further, voluntary mechanisms have also been developed by the intermediaries in the past, to tackle misinformation during periods susceptible to public order issues, such as in the run-up to major elections. Against the backdrop of the 2019 General Elections in India, the Internet and Mobile Association of India (**IAMAI**) together with several social media platforms developed a Voluntary Code of Ethics, to work in conjunction with the Election Commission of India (**ECI**) (**Voluntary Code**)[71]. The Voluntary Code requires social media platforms to (a) process take down requests by the ECI within 3 hours, instead of 36 hours, (b) appoint dedicated teams to serve as point of contacts for the ECI during the election period for exchanging information, acting on take down requests, etc., (c) providing political advertisers to submit pre-certificates issued by the ECI in relation to election advertisement.[72] The ECI reported that during the election period, social media platforms took down content in over 900 cases. [73] The Voluntary Code was thereafter adhered to in consequent State elections as well.[74]

---

67 See, Second Proviso to Rule 3(1)(d) of the IG & DMEC Rules

68 See, Rule 3(1)(b)(ii), (vi) and (x) of the IG & DMEC Rules

69 See, Rule 3(1)(c) of the IG & DMEC Rules

70 See, third proviso to Rule 3(1)(d) of the IT Rules: "Provided also that the removal or disabling of access to any information, data or communication link within the categories of information specified under this clause, under clause (b) on a voluntary basis, or on the basis of grievances received under sub-rule (2) by such intermediary, shall not amount to a violation of the conditions of clauses (a) or (b) of sub-section (2) of section 79 of the Act;"

71 See, Press Information Bureau, "Social Media Platforms present "Voluntary Code of Ethics for the 2019 General Election to Election Commission of India", 20 March 2019, Available at URL: https://pib.gov.in/newsite/PrintRelease.aspx?relid=189494

72 See, IAMAI, Voluntary Code of Ethics for the General Elections 2019, Available at URL: https://static.pib.gov.in/WriteReadData/userfiles/Voluntary%20Code%20of%20Ethics%20for%20the%20G.E.%202019.pdf

73 See, PTI, "Over 900 Posts Taken Down From Social Media Platforms During 2019 Polls", NDTV, 19 May 2019, Available at URL: https://www.ndtv.com/india-news/lok-sabha-election-2019-over-900-posts-taken-down-from-social-media-platforms-during-national-polls-2039866

74 See, Election Commission of India, ""Voluntary Code of Ethics" by Social Media Platforms to be observed in the General Election to the Haryana & Maharashtra Legislative Assemblies and all future elections", Press Note, 26 September 2019, Available at URL: https://eci.gov.in/files/file/10659-%E2%80%9Cvoluntary-code-of-ethics%E2%80%9D-by-social-media-platforms-to-be-observed-in-the-general-election-to-the-haryana-maharashtra-legislative-assemblies-and-all-future-elections/

Analysis of Current India Legal Framework and Way Forward

The current legal framework to prevent the dissemination of misinformation in India is fairly extensive, albeit scattered across multiple sources of law, as explained earlier. However, as the Government's continued emphasis on the subject of tackling misinformation suggests, there remains scope for improving the legal framework, in order to effectively tackle and reduce the extent of misinformation disseminated.

Before commencing a review of existing gaps in the framework and identifying areas of improvement, one needs to recognize and reconcile with the fact that it would be an uphill task to address or remedy all misinformation currently in circulation, whether in the real world or digital. Hence, the exercise should focus on and prioritize misinformation that leads to material harm. Resultantly, the following discussion on potential solutions for tackling misinformation is limited to instances of misinformation which are clearly actionable owing to the risk of harm it may cause to life and/or property.

We have also assessed the need for explicitly defining additional categories of harms, for tackling instances of potentially harmful misinformation, which do not give rise to any pre-defined form of harm (such as disharmony, incitement to commission of a cognizable offence, etc.).

Review of Gaps in Current Legal Framework

Enforcement of Journalistic Norms and Framework for Tackling Misinformation by Citizen Journalists

Enforcement of Journalistic Norms in Print and Digital Media

As discussed above, both the MeitY and MIB are empowered to block access to misinformation under the provisions of the IT Act. While MeitY's powers flow from content that is actionable under Section 69A read with applicable provisions of the IT Blocking Rules, the MIB is empowered to direct the modification, deletion or blocking of actionable content, under Section 69A read with applicable provisions under Part – III of the IG & DMEC Rules. Notably however, while the MeitY's directions may only be extended to intermediaries, the MIB's directions extend to publishers of news and current affairs content, as well as intermediaries.

Moreover, the PCI Norms, which are sought to be applied to NCAC in both print and digital media by the IG & DMEC Rules, are adequately geared to address issues of misinformation/disinformation propagated by journalists and news media.

Resultantly, effectiveness of the extant framework geared at tackling misinformation/disinformation propagated by journalists and news media, is likely to be determined by the vigor of enforcement of the norms. While admittedly, the operation of Rules 9(1) and 9(3) of the IG & DMEC Rules, have been stayed by various High Courts, an eventual determination of the constitutional vires of the provisions, is likely to pave the way for wide-ranging enforcement of the PCI Norms in both print and digital media.

Tackling Misinformation generated by non-Journalists/ citizen journalists

Individuals or citizen journalists posting newsworthy information on various platforms, are not subject to journalistic norms such as the PCI Norms. Therefore, the possibility of generating and disseminating unverified and misleading information is higher. However, given the myriad channels for disseminating user-generated news content, it will not be practicable to introduce enforceable norms for citizen journalists and user-generated news content.

Resultantly, instances of misinformation generated by non-journalists, will need to be tackled under existing provisions of law. While in all cases, the continued circulation ought to be curbed, whether and to what extent individuals could be made liable would depend upon the existence of intent, thereby enabling law enforcement to distinguish innocuous misinformation, from malicious disinformation (See discussion below).

Ideally, strict liability i.e. imposition of liability irrespective of the presence of an intent to mislead, should be avoided. This approach may appear disproportionate except when the nature of harm is aggravated. In any event, in the Indian context, penal sanctions have not proved to be deterrent. Hence, holistic approach needs to be adopted.

Lack of Expressly Defined Individual Liability for Misinformation

In the absence of any provision criminalizing disinformation *per se*, disinformation which is not relatable to existing criminal law provisions, but still has a potential to adversely impact public order, is not met with any liability under the law. For example, misinformation relating to Covid-19 vaccination, which potentially dissuades the audience from obtaining vaccinations, could potentially exacerbate the Covid-19 crisis, without falling foul of speech-related provisions of the IPC and other criminal statutes. Resultantly, there is scope for including a standalone provision for imposing individual liability for disseminating disinformation.

Given that misinformation itself may present itself in various forms,[1] any offence introduced must narrowly define actionable types of misinformation, particularly targeting disinformation, and have a certain *de minimis* standard of harm to distinguish innocuous misinformation from disinformation that presents a clear and present danger to public order, integrity, defence or security of India or its relations with foreign states. In order to meet the test of substantive and procedural proportionality, the commission of an offence should be premised upon the existence of *mala fide* intent, and not prosecute unintentional, accidental or good faith transmission of misinformation.

Tackling Misinformation Disseminated over Interpersonal Communications

What one communicates to other over interpersonal communications platforms, how the news is perceived or interpreted, resulting in what sort of consequences, is not usually in control of private chat platforms who assure safety and privacy of communications through the deployment of end-to-end encryption (**E2EE**).[2] Currently,

1 See, Cunliffe-Jones, P. (2022b, projected). Types, drivers and effects of misinformation in Africa. University of Westminster Press; Misinformation has been variously defined to include information, which constitutes: (a) unproven claims stated as known fact; (b) claims that are outright false; (c) claims that mislabel or misattribute content such as photographs or videos; (d) claims that bear an element of truth but overstate or understate a position; (e) claims that bear an element of truth but are misleading in other ways; (f) claims that are accurate in themselves but conflate issues; (g) satire understood as true; (h) deliberately fabricated or manipulated content, where the intention is thus clearly to mislead; (i) imposter content; (j) hoaxes and scams; and (k) coordinated inauthentic behaviour – not misleading content as such but patterns of online behaviour intended to distort understanding

2 E2EE is a form of "zero-knowledge" encryption protocol, situations where the intermediary deploying the protocol, does not have any technical capability of monitoring or accessing the contents of communications transmitted on their platform.

no jurisdiction, apart from India, has provisions that seek to address such forms of dissemination of misinformation.

Rule 4(2) of the IG & DMEC Rules, require certain intermediaries which (a) have more than 5 million users in India; and (b) offer a platform in the nature of a messaging service, to enable the identification of the first originator of messages transmitted over the platform.[3]

However, this obligation has been met with significant pushback from privacy activists and the industry since, (a) there is a lack of evidence establishing the technological viability of complying with the obligation; and (b) since in the absence of any rules or safeguards explicitly governing bulk surveillance,[4] any solution to trace misinformation on interpersonal communications platforms, is unlikely to meet the muster of proportionality as required by the Court in *K.S. Puttaswamy v. Union of India* (**Puttaswamy**).[5] Notably, in a petition currently pending before the Kerala High Court, the petitioners have urged the Court to declare Rule 4(2) of the IG & DMEC Rules as being violative of the right to privacy, and to declare the right to encryption as a concomitant right.[6]

While legal solutions which prioritise a punitive approach (e.g. by tracing the originator of misinformation) are likely to remain challenging owing to privacy concerns,[7] alternate non-intrusive solutions to tackling misinformation on private interpersonal communications platform continue to be developed. For instance, in an attempt to counter the potential spread of misinformation over its platforms in the run up to the Indian General Elections on 2019, WhatsApp introduced a feature which enabled users to voluntarily fact-check messages, by forwarding them to a Checkpoint.[8] Forwarded messages were then labelled as either true, false, misleading or disputed. Similar services have recently been launched by certain news media outlets, enabling users to have forwarded messages verified by journalists.[9]

While such early attempts were seen by some as ineffective in curbing misinformation, the Checkpoint project did enable greater insights into patterns of misinformation, by enabling the creation of a significant database of messages voluntarily contributed by users.[10] This in turn can be used to device interventions which focus on providing accurate information to users, in a manner which does not risk intruding upon individual privacy. In fact, independent fact-checking services have been introduced by online platforms in other jurisdictions,

---

3 See, Rule 4(2) of the IG & DMEC Rules, See also, MeitY, Notification No. S.O. 942(E), Dated 25 February 2021, Available at URL: https://egazette.nic.in/WriteReadData/2021/225497.pdf; "In exercise of power conferred by clause (v) of sub-rule (1) of rule 2 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Central Government hereby specifies fifty lakh registered users in India as the threshold for a social media intermediary to be considered a significant social media intermediary."

4 See, Manohar Lal Sharma v. Union of India & Ors., W.P. (Crl.) No. 314 of 2021 (with connected matters), 27 October 2021, Available at URL: https://main.sci.gov.in/pdf/LU/27102021_082008.pdf; The Supreme Court of India has recently acknowledged the lack of a framework governing bulk surveillance, while considering the recent batch of petitions relating to the Government's alleged deployment of the Pegasus spyware for surveilling civilian subjects, and has directed a Committee of Experts to inter alia review and issue its findings on the need and design for a legal framework for bulk surveillance.

5 See, Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 at Para T.5 at p. 265, The Court in Puttaswamy acknowledged the need to balance the right to privacy with legitimate aims of the State, noting that objectives such as protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits, would all constitute legitimate aims. Additionally, the Court held that laws restricting the exercise of the fundamental right to privacy, must also meet the other two parameters of the three-fold test laid out in Puttaswamy, i.e., (i) legality, which postulates the existence of law; and (ii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.

6 See, Praveen A. vs. Union of India, WP(C) 9647 of 2021, a copy of the Petition filed before the Kerala High Court is available at URL: https://regmedia.co.uk/2021/04/12/wpc_praveen_08042021.pdf

7 See, Robertson A., "Apple's Controversial New Child Protection Features, Explained", The Verge, 10 August 2021, Available at URL: https://www.theverge.com/2021/8/10/22613225/apple-csam-scanning-messages-child-safety-features-privacy-controversy-explained

8 See, Porter J., "WhatsApp launches fact-checking service in India ahead of elections", The Verge, 2 April 2019, Available at URL: https://www.theverge.com/2019/4/2/18291880/whatsapp-fact-checking-checkpoint-tipline-misinformation-indian-elections-proto

9 See, TNN, "Times Verified tracks viral fake news, debunks 48% of over 24,000 messages", Times of India, 21 January 2022, Available at URL: https://timesofindia.indiatimes.com/city/mumbai/times-verified-tracks-viral-fake-news-debunks-48-of-over-24000-messages/articleshow/89029404.cms

10 See, IANS, "WhatsApp tipline of no use for 2019 Lok Sabha polls", Outlook, 5 April 2019, Available at URL: https://www.outlookindia.com/newsscroll/whatsapp-tipline-of-no-use-for-2019-lok-sabha-polls/1509735

and platforms continue to refine methods to study and tackle misinformation through timely fact-checking and similar interventions.[11]

Such innovations were adopted widely following the outbreak of the Covid-19 pandemic, where both Government and private stakeholders leveraged traditional and print media to dispel harmful misinformation relating to Covid-19. The Press Information Bureau (**PIB**)'s Fact Check service, launched in 2019, played a pivotal role in this regard.[12] The PIB's portal enables users to submit content for fact-checking by the PIB, which in turn leverages its social media accounts to call out misinformation. Social media platforms also deployed methods of scanning posts for Covid-19 related content and directed users to curated and trusted information relating to the Covid-19 pandemic from the World Health Organization.[13]

Manipulated Media on Online Platforms

Lastly, there is a lack of clear and precise rules governing the treatment of manipulated media, such as AI-generated "deep fakes" under the law. Rule 3(2)(b) of the IG & DMEC Rules addresses this issue in a limited context, by obligating intermediaries to take down content on the basis of complaints received – intimating the intermediary that the infringing content in the *"nature of impersonation in an electronic form, including artificially morphed images of such individual."* Additionally, Rule 3(1)(b)(x) of the IG & DMEC Rules requires intermediaries to inform their users to refrain from hosting/transmitting any content that *"is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person."* Additionally, and depending on the nature of content contained in such manipulated media, applicable penal provisions may be invoked.

However, these provisions are likely to have little impact in the timely detection and deletion of manipulated media. While the introduction of appropriately framed provisions on individual liability for disinformation are likely to serve as deterrent, technological solutions are likely to be more effective in addressing the issue of detecting manipulated media.

In the past, several platforms have deployed algorithms to identify and mark content as containing manipulated media.[14] However, concerns over consistency of application of platform specific rules for identifying manipulated media,[15] have led to calls for further regulation of the subject of voluntary identification of manipulated media on online platforms.[16] Hard-coding any obligations and liability in this regard should be avoided, since most technological solutions available for detecting manipulated media are prone to both type-I (or a false positive, when the system decides that a piece of content is problematic when it isn't) and type-II (a false negative, when the system decides that a piece of content isn't problematic, when it is) errors.[17] Concerns of consistency of application of rules can be potentially addressed through appropriate grievance redressal mechanisms, enabling users to appeal a platform's decision to mark content as manipulated media.

---

11 See, Facebook, Facebook's Third-Party Fact-Checking Program, Meta Journalism Project, Available at URL: https://www.facebook.com/journalism-project/programs/third-party-fact-checking

12 See, PIB Fact Check, Available at URL: https://factcheck.pib.gov.in/

13 See, Clegg N., "Combating Covid-19 Misinformation Across Our Apps", Meta, 25 March 2020, Available at URL: https://about.fb.com/news/2020/03/combating-covid-19-misinformation/; See also, Meta, "Keeping People Safe and Informed About the Coronavirus", 18 December 2020, Available at URL: https://about.fb.com/news/2020/12/coronavirus/

14 See, Twitter, Synthetic and Manipulated Media Policy, Available at URL: https://help.twitter.com/en/rules-and-policies/manipulated-media

15 See, Bhardwaj D., "'Dilutes your credibility': Government's notice to Twitter in toolkit case", Hindustan Times, 18 June 2021, Available at URL: https://www.hindustantimes.com/india-news/-dilutes-your-credibility-government-s-notice-to-twitter-in-toolkit-case-101623945978380.html

16 See, Agarwal S., "Govt weighs single policy for all social media firms", Economic Times, 5 October 2021, Available at URL: https://economictimes.indiatimes.com/tech/technology/govt-weighs-single-policy-for-all-social-media-firms/articleshow/86762379.cms

17 See, Bhavsar R., "Striking a Balance: Automated and human content moderation", Essence, 27 May 2021, Available at URL: https://www.essenceglobal.com/article/striking-a-balance-automated-and-human-content-moderation

Approach Adopted in Other Jurisdictions

Various ways to tackle misinformation have been implemented, or are under consideration, by jurisdictions around the world. These vary in their scope and implications significantly, but in most forms deploy a combination of either (i) individual liability for misinformation, (ii) obligations upon intermediaries to disable access to misinformation coupled with penalties for intermediaries for non-compliance of take-down obligations, (iii) proactive risk assessment and monitoring by intermediaries to tackle misinformation, and (iv) research and advocacy on curbing the spread of misinformation. We have provided details of laws in some of the jurisdictions in **Annexure – B**.

Takeaways from International Experience

Taken together, the various mechanisms adopted by jurisdictions around the world, can be bucketed into three approaches:

- The first, is the *censorship approach* of blocking public access to misinformation by issuing orders to intermediaries and publishers. However, this approach is at best curative, and requires stakeholders to limit the spread of misinformation on a case-by-case basis through constant monitoring of multiple channels of information.
- The second approach is the *punitive approach* which imposes liability on individuals or organizations originating or disseminating misinformation. However, given the myriad channels of dissemination of information, enforcement remains challenging, thereby undermining the deterrent effect of punitive approaches. Moreover, if appropriate definitions for *actionable* misinformation (i.e. disinformation) are not adopted under the law, this approach could have a chilling effect on speech, as individuals and organizations are likely to indulge in self-censuring.
- The third approach is the *intermediary regulation* approach, which operationalizes some combination of the first two approaches, by imposing additional obligations upon online intermediaries to expeditiously remove misinformation from their platforms, failing which they could incur liability for continuing to host such misinformation on their platforms.

Notably, however, none of these approaches address the harms arising out of misinformation or attempt to tackle the underlying incentives and mechanisms which enable the rapid dissemination of misinformation. Therefore, in addition to existing legal mechanisms, there is merit in considering additional or alternate solutions which take into consideration the underlying dynamics of misinformation, and supplement it with appropriately crafted technological and legal solutions.

Recommendations for Policy Makers and Industry

Re-Imagining the Government's Role:

The Government needs to re-imagine its role in the fight against misinformation. In addition to enforcement of existing laws, the Government should also encourage innovation and investments to create an ecosystem of stakeholders which leverages technology and manpower, to detect and act against misinformation in a timely manner. The economic cost of misinformation, by some estimates, costs the US an approximate amount of USD 78 billion annually (including stock market value and brand equity lost on account of misinformation, public health costs and other costs arising from disruptions to public order).[1]

Therefore, even by conservative estimates, the economic cost of misinformation in India, would represent a non-trivial percentage of India's GDP (estimated to be USD 2.66 trillion in current US dollar value).[2] Resultantly, the Government should consider earmarking budgetary resources for prioritizing investments directed at research, media awareness, and technology for tackling misinformation. Further, the Government could consider developing policy guidelines applicable to social media platforms, to suggest certain minimum criteria for checking accuracy of user generated content. This could be done by way of amendments to the IG & DMEC Rules.

Leveraging Technology to Detect Misinformation:

Considering the success of Arogya Setu and Cowin platforms, the Government, in collaboration with other stakeholders, could also create a set of dedicated apps to fact check information submitted by citizens. The apps could allow use of regional language and voice command functions from an ease of use perspective.

Given the prevalence of regional language content, and peculiarities in the Indian context, the Government could also develop a mechanism for accrediting privately developed fact checking apps. There could also be an India-specific ecosystem of Government-accredited, private, independent fact checking agencies, who could flag misinformation on private platforms. Such an ecosystem could be developed along the lines of existing international ecosystems, such as the International Fact Checking Network (**IFCN**).[3]

Illustratively, news content which breaches a certain level of outreach/ virality on private platforms, could be referred to such independent fact checking agencies for verification – who in turn could verify the accuracy of the content, and communicate the same to the Government. For users, the veracity of such content could be communicated through any visible mark of identification (as is the case for verified user accounts on social media). By extension fake news or unreliable information should be flagged as such, and platforms should

1 See, University of Baltimore, CHEQ, "The Economic Cost of Bad Actors on the Internet: Fake News", 2019, Available at URL: https://info.cheq.ai/hubfs/Research/THE_ECONOMIC_COST_Fake_News_final.pdf

2 See, World Bank Data, India GDP (current US$), Available at URL: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=IN

3 See, About IFCN, Available at URL: https://www.poynter.org/ifcn/about-ifcn/; IFCN is an initiative run by the Poynter Institute of Media Studies, a US-based not-for-profit organization. IFCN acts as a certifying / auditing international body for fact-checking organizations across the world. It has established a 'Code of Principles' which contains five broad principles: (i) Non-partisanship and fairness in conducting fact-checks: (ii). Standards and transparency of sources; (iii) Transparency of funding and organization structure; (iv) Standards and transparency of methodology; (v) Open and honest corrections policy. c. Organizations that wish to be certified by the IFCN are required to complete an application process which involves an application fee. Through this process, they have to demonstrate that they comply with IFCN's Code of Principles. These applications are evaluated by external assessors, whose recommendations are then approved or rejected by the IFCN Board of Directors. d. Once an organization is approved by the IFCN, it becomes an 'IFCN Signatory'. The organization can then display the 'IFCN Badge of Approval' on its website to show that it is IFCN-verified. Currently, there are 101 IFCN signatories, including 18 fact-checking organizations from India.

take proactive measures to ensure that such content is not recommended to users through their recommender systems and warn users of actual or potential inaccuracies when they attempt to share such content. Further, through innovative techniques such as gamification, citizens could be trained to detect / suspect fake news. The Government should consider working closely with relevant stakeholders including technology companies, social media platforms, universities and researchers, to create a technology-based ecosystem for monitoring and flagging misinformation. Supported by the Government of India, a fact-checking application has already been piloted by the IIT Delhi.[4]

Private entities such as the Times Group and other prominent media houses, have also been investing in technology to enable rapid fact checking. However, a centralized application, which collates insights into misinformation from both Government and private persons, is still needed. Such applications should adopt a "human in the loop" approach to detecting misinformation, i.e., allow users and independent fact checkers to report content that is suspected to be a product of coordinated inauthentic behaviour, in order to train AI and machine learning based algorithms to detect misinformation. Examples of early efforts in this regard, include Google and Facebook's collaboration with First Draft to train their systems to differentiate inauthentic content from human generated content, with a view to curbing the spread of fabricated misinformation and manipulated media.[5]

User Responsibility and Media Awareness:

The Government, together with other stakeholders such as social media platforms, should engage in awareness campaigns about the harmful impact of misinformation, the liabilities (civil and criminal) emanating from sharing/publishing misinformation, and good practices to ensure responsible generation of citizen journalist content. This should also be done in regional language for wider reach.

Dynamic elements such as gamification, animation, interactive campaigns, flyers, quizzes and fact-checking helplines, could supplement the effectiveness of media awareness campaigns. One study has revealed that by merely prompting participants to reflect on an attribute of their own personality—by completing a short personality questionnaire, the participants were able to accurately identify ads that were targeted at them by up to 26 percentage points.[6] Prominent examples of media awareness programs being used as a tool to tackle misinformation are found in several other jurisdictions including the EU and Finland. Finland incorporates critical reading programs in school and adult education curriculums, helping citizens to distinguish between fact from misinformation or disinformation.[7] The program is supplemented by voluntary fact-checking platforms operated by journalists.

Research on Psychological and Sociological Factors Underlying Dissemination of Misinformation:

Complementary strategies to tackle misinformation, should be based on research into the psychological factors (such as individual and societal biases) and sociological factors (such as the risk of certain communities, groups, classes of people, being impacted or motivated disproportionately through the consumption of misinformation)

4 See, Sahoo P., "IIT Bombay launches fact-checking platform that helps verify fake COVID-19 news", Hindustan Times, 1 April 2020, Available at URL: https://www.hindustantimes.com/it-s-viral/iit-bombay-launches-fact-checking-platform-that-helps-verify-fake-covid-19-news/story-m3KuiO0xvz-kvCOGGH7KcQM.html

5 See, Gehrmann S., Strobelt H., and Rush A., "GLTR: Statistical Detection and Visualization of Generated Text," (Ithaca, NY: Cornell University, June 2019), Available at URL: https://arxiv.org/abs/1906.04043.

6 See, Lorenz-Spreen, P., Geers, M., Pachur, T. et al. Boosting people's ability to detect microtargeted advertising. Sci Rep 11, 15541 (2021), Available at URL: https://doi.org/10.1038/s41598-021-94796-z

7 See, Mackintosh E., "Finland is winning the war on fake news. What it's learned may be crucial to Western Democracy", CNN, May, 2019, Available at URL: https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/; See also, FactBar EDU, Fact Checking for Educators and Future Voters, 2018, Available at URL: https://www.faktabaari.fi/assets/FactBar_EDU_Fact-checking_for_educators_and_future_voters_13112018.pdf

underlying the dissemination of misinformation. Such strategies can aid the Government and Law Enforcement Agencies to pre-empt the rapid dissemination of misinformation amongst communities and mitigate potential harms in a timely manner.

Individual Liability:

To deter the dissemination of disinformation that is currently not actionable under Indian law, the Government should consider introducing a standalone provision for attributing individual liability for the dissemination of disinformation. The trigger for individual liability should be based on the level of harm caused or likely to be caused as a consequence of the dissemination of disinformation. Liability should arise only for harm that is directly relatable to the grounds listed under Article 19(2).

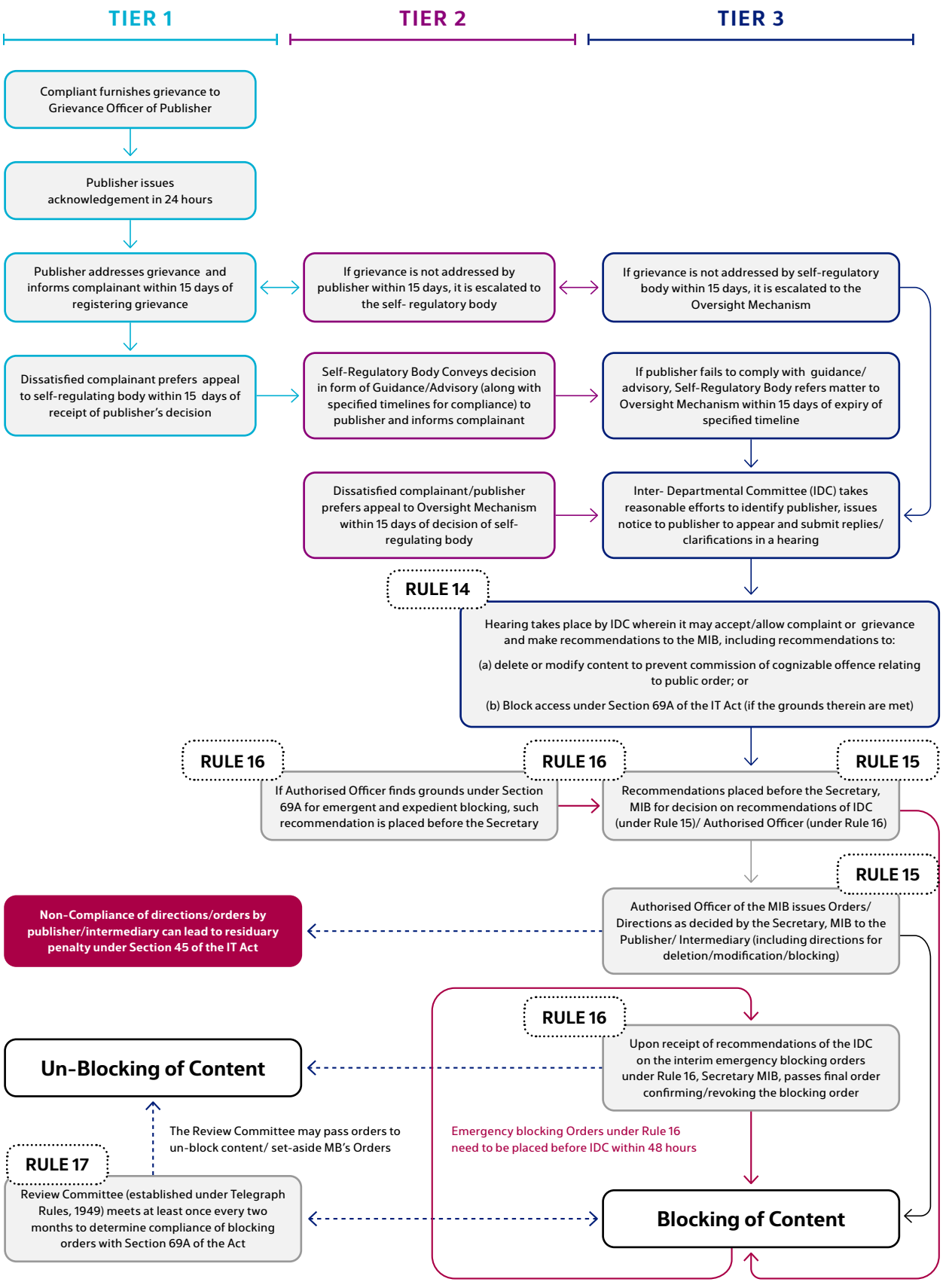
Instances of unintentional, accidental or good faith transmission/publication of misinformation, which is a manifestation of general belief (i.e., without the intent of instigating others to act on such misinformation) should be excluded from the scope of individual liability – irrespective of the level of harm. The liability could be civil in nature where only penalty is imposed and the enforcement should be expeditious. Existing provisions of the IT Act (Sections 69A, 79) may be resorted to, in order to block public access to such misinformation, in order to mitigate the impact of harmful misinformation shared/published in good faith.

Widening Applicability and Strengthening Enforcement of Journalistic Norms:

Norms of journalistic conduct applicable to print media and broadcast media (to the extent recognized by the Bombay High Court) are already in existence in the form of the PCI Norms issued under the PCI Act. Subject to the eventual outcome of ongoing judicial proceedings evaluating the constitutional vires of the IG & DMEC Rules, the framework may be extended to digital news media.

Should the Courts ruling hold that extension of the PCI Norms to digital media by way of the IG & DMEC Rules is invalid, the PCI Act may have to be amended to extend the PCI's regulatory remit to all forms of news media. Similarly, recognizing the NBSA under the provisions of the CTNR Rules, can provide legislative basis for the enforcement of the NB Code of Ethics, which set out journalistic norms for news broadcasters. The Government should consider reviewing existing laws relating to news media, and develop effective enforcement mechanisms, to ensure stricter enforcement of journalistic norms across all forms of news media.

Annexure A
Grievance Redressal Mechanism under IG & DMEC Rules



Annexure B
Overview of Laws in Other Jurisdictions

Germany's Network Enforcement Act (NetzDG)

In what is considered in many instances as one of the first legislative attempts to formally address the issue of misinformation online, Germany enacted the Network Enforcement Act, 2017 (**NetzDG**).[1]

The law, initially contemplated as a measure of outlining intermediaries' obligations with regard to hate speech[2] and misinformation online,[3] requires intermediaries to promptly remove content relatable to 22 provisions of the German Criminal Code,[4] within 24 hours of identification of such manifestly illegal content, in order to avoid penalties ranging up to 50 million Euros.[5] Similar to the approach adopted in India, the Criminal Code of Germany declares unlawful speech that is prejudicial to the security of the State, relates to the commission of offences, and jeopardizes the maintenance of public peace (including through speech that indulges in the revilement of religious sentiments).

The NetzDG requires *"social networks"* (defined as telemedia[6] service providers operating online platforms, which enable users to share any content with other users or to make such content available to the public) having more than two million registered users in the Federal Republic of Germany, to adhere to certain obligations to tackle unlawful content.

Under the provisions of the NetzDG, social networks are required to maintain an effective and transparent procedure for handling complaints about unlawful content, and supply users with an easily recognisable, directly accessible and permanently available procedure for submitting complaints about unlawful content.[7] Unlawful content may be identified and notified to social networks by users or Government agencies. Content which is manifestly illegal[8] needs to be removed within 24 hours of being identified as such. However, other

1 See, Bundesministerium der Justiz, "Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act, NetzDG) - Basic Information (2017)", Available at URL: https://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html; An English translation of the law is available at: https://perma.cc/7UCW-AA3A

2 German Law does not define "hate speech". However, the Criminal Code does enable the State to proceed against speech that constitutes Volksverhetzung (translating to "incitement to hatred"). For any hate speech to be punishable as Volksverhetzung, the law requires that said speech be "disturbing public peace" either by inciting "hatred against a national, racial, religious group or a group defined by their ethnic origin, against sections of the population or individuals on account of their belonging to one of the aforementioned groups or sections of the population, or calls for violent or arbitrary measures against them" or "violates the human dignity of others by insulting, maliciously maligning or defaming one of the aforementioned groups, sections of the population or individuals on account of their belonging to one of the aforementioned groups or sections of the population" (s.130 of the Criminal Code)

3 Interestingly, "misinformation" or "fake news" has not been defined under the Network Enforcement Act, 2017. However, the falsity of the content, is a factor relevant to determination of unlawfulness of the content (under s. 3(2)(3)(a) of the Network Enforcement Act). Additionally, the s.186 of the German Criminal Code also penalizes "malicious gossip" (üble Nachrede), defined as the assertion or dissemination of a fact about another person, which is suitable for degrading that person or negatively affecting public opinion about that person, unless this fact can be proved to be true.

4 The law bears reference to the following provisions of the German Criminal Code (Strafgesetzbuch – StGB) – 86. Dissemination of propaganda material of unconstitutional organisations; 86a. Use of symbols of unconstitutional organisations; 89a. Preparation of serious violent offence endangering state; 91. Instructions for committing serious violent offence endangering state; 100a Treasonous forgery; 111. Public incitement to commit offences; 126. Disturbing public peace by threatening to commit offences; 129. Forming criminal organisations; 129a. Forming terrorist organisations; 129b. Foreign criminal and terrorist organisations; confiscation; 130. Incitement of masses; 131. Depictions of violence; 140. Rewarding and approval of offences; 166. Revilement of religious faiths and religious and ideological communities; 184b. Dissemination, procurement and possession of child pornography; 185. Insult (committed by means of assault); 186. Malicious gossip (üble Nachrede); 187. Defamation; 241. Threatening commission of serious criminal offence; 269. Forgery of data of probative value; Available at URL: https://www.gesetze-im-internet.de/englisch_stgb/

5 See, Available at URL: https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law

6 See, Bösling T., Weisser R., "New German telemedia legislation clarifies some issues; clouds others", Lexology, 7 June 2007, Available at URL: https://www.lexology.com/library/detail.aspx?g=2bc98a4a-3b5f-451a-8f71-171cac8b7e12; The German Telemedia Act, 2007 (TMA), does not define the term "telemedia". However, Section 1 of the TMA, extends the applicability of the law to electronic information and communication services, to the extent that they are not telecommunications service providers (i.e. pure intermediaries involved in the transmission of electronic signals through telecommunications networks) or broadcasting service providers.

7 See, Section 3(1) of NetzDG

8 The NetzDG does not define what content is considered to be "manifestly illegal".

unlawful content, needs to be removed within 7 days of being identified and notified to a social network, unless – (a) the determination of illegality of such content is contingent upon underlying factual circumstances, in which case, the publisher of such content may be provided an opportunity to respond to the complaint received; or (b) where the determination of illegality is referred to an independent self-regulatory institution, recognized under the NetzDG, for its opinion, which is required to be furnished within 7 days.[9]

This approach, however, has been widely criticized, on account of demonstrated over-censure practiced by intermediaries. Some of the key concerns voiced, include the possibility of over censorship by online platforms hosting third party content, owing to the steep penalties coupled with short timelines to make fairly complex determinations regarding the extent of manifest illegality, nature of mischaracterisation conveyed through hosted content, and the lack of judicial oversight over the take-downs effected by platforms.[10]

Such criticism has prompted a legislative review of existing provisions.[11] More recently in 2020, Germany introduced a proposed amendment to the law, to introduce more user-friendly[12] notice and take-down and appeals procedures, together with an obligation on intermediaries to share transparency reports.[13] It also enables the Federal Office of Justice to monitor compliance.[14]

At the same time, however, concerns have been raised over the disclosures required to be made by intermediaries pursuant to their transparency obligations, since they could potentially require intermediaries to share personal identifiers pertaining to their users, with the regulator and other users.[15]

European Union

The European Union has adopted a multi-pronged approach to addressing misinformation. At the first level, this approach relies on self-regulatory mechanisms – through the adoption of the Code of Practice against Disinformation by social network operators and the advertising industry. At the second level, the approach focusses on analysing and assessing misinformation risks through various research projects, and the adoption of awareness programmes. And finally, it relies on a Union-wide strategy to counter misinformation under the European Democracy Action Plan (**EDAP**) and the proposal for the Digital Service Act (**DSA**) package.[16]

9 See, Section 3(3) of NetzDG

10 Ibid.

11 See, Available at URL: https://www.reuters.com/article/us-germany-hatespeech/germany-looks-to-revise-social-media-law-as-europe-watches-idUSKCN1GK1BN

12 Section 3, Paragraph 1 of the Network Enforcement Act, requires the complaint submission process to be "easily recognizable, directly accessible, and permanently available." The amendments additionally require such processes to be "easy to use."

13 The Network Enforcement Act requires social media networks that receive more than 100 complaints about illegal content in a calendar year, to publish biannual reports in German on how they deal with these complaints. The amendments expand the scope of disclosures required, and now require social media networks to disclose – (a) procedures for automated detection, together with disclosures on training data, and quality monitoring and evaluation for such procedures; (b) number of actioned take-down requests classified based on response time (within 24 hours, 48 hours, a week, or more than a week); (c) number of appeals against the networks decision, and the number of appeals in which the original decision was revised; See also Facebook, NetzDG Transparency Report January 2021, Available at URL: https://about.fb.com/de/wp-content/uploads/sites/10/2021/01/Facebook-NetzDG-Transparency-Report-January-2021.pdf (As a sample Transparency Report)

14 See, Available at URL: https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/

15 See, Available at URL: https://cpj.org/2020/10/germany-revisits-influential-internet-law-as-amendment-raises-privacy-implications/; The NetzDG amends Section 14 of the TMA, enabling the Government or an aggrieved party to compel social networks to share subscriber data within its possession, insofar as this is necessary for the enforcement of civil law claims arising from the violation of absolutely protected rights by unlawful content. However, such disclosures must be preceded by an Order of a regional court.

16 See, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, "The fight against disinformation and the right to freedom of expression", July 2021, Available at URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695445/IPOL_STU(2021)695445_EN.pdf

The DSA proposes to introduce user-friendly notice and takedown mechanisms which are easy to access and enable the submission of notices exclusively through online means,[17] coupled with an obligation for online platforms to provide an explanation to users on the reasons for such take-down.

In a first, the DSA also considers the nexus between misinformation and sponsored content, including the possibility of misinformation being disseminated through sponsored content on online platforms, as a part of larger coordinated campaigns.

Existing research indicates that the practice of placing "advertorials" (a portmanteau of "editorial" and "advertising") has blurred the lines between news reportage and sponsored content.[18] With such business models increasingly finding their place in monetization strategies adopted by mainstream media outlets, users are unable to distinguish genuine editorials from sponsored content.[19] On the other hand, brands are increasingly concerned with reputational risks their advertisements being featured on online sites featuring misinformation.[20]

Therefore, and given documented instances of misinformation being promoted through targeted advertisements,[21] and instances of sites hosting misinformation benefiting from advertising revenue, the DSA also introduces an obligation for online platforms to publish transparency reports and provide additional information and explanations on methods of targeting advertisements or paid content to users.[22]

Additionally, the DSA suggests due diligence requirements for "very large online platforms", i.e., platforms with more than 45 million active monthly users within the EU,[23] requiring such platforms to: (i) analyse any systemic risk stemming from the use of platforms and put in place effective content moderation policies; (ii) provide additional disclosures relating to the primary parameters considered by decision making algorithms on their platform, and provide users the option to modify such parameters; (iii) maintain public repositories of online advertisements served for the past year, and make it accessible via application programming interfaces (**APIs**);[24] and (iv) sharing platform-related data required for assessing systemic risks available to the European Commission and academics.

Interestingly, the DSA also proposes to put in place an ecosystem of entities with demonstrated expertise and competence in identifying and flagging illegal content on online platforms, to assist online platforms in their efforts to counter misinformation. Entities may by awarded the status of a "Trusted flagger" by the Digital Services Coordinator (**DSC**) of the relevant Member State, upon being able to demonstrate that the entity: (a) has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content;

---

17 See, Article 14(1) of the Proposal for Digital Services Act, "Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means."; Article 14(2) of the Proposal for Digital Services Act elaborates that the mechanism in order to be user-friendly, must "(...) facilitate the submission of sufficiently precise and adequately substantiated notices, on the basis of which a diligent economic operator can identify the illegality of the content in question."

18 See, Pelle J., "Fake news and the ugly rise of sponsored content", PR Daily, 17 January 2018, Available at URL: https://www.prdaily.com/fake-news-and-the-ugly-rise-of-sponsored-content/

19 See, Mcalpine-Boston K., "9 In 10 People Can't Tell Sponsored Stuff From Real News Online", Futurity, 18 January 2019, Available at URL: https://www.futurity.org/sponsored-content-real-news-1961062/

20 See, Bhushan R., "HUL to cut online ads if toxic content not weeded out", Economic Times, 14 February 2018, Available at URL: https://economictimes.indiatimes.com/industry/services/advertising/hul-to-cut-online-ads-if-toxic-content-not-weeded-out/articleshow/62908933.cms?from=mdr

21 See, Ravel A.M, Wood A.K., "Fool Me Once: Regulating Fake News and Other Online Advertising", 91 S. Cal. L. Rev. 1223 (2017-2018)

22 See, European Commission, Proposal for a Regulation of The European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC; Available at URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

23 Ibid. Article 25(1)

24 Based on the Recitals to the DSA, this obligation has been introduced for the purposes of enabling greater transparency in online targeted advertising and recommender systems, so as to enable meaningful engagement by stakeholders (Recitals 58 and 62). While not directly addressed at tackling misinformation, it is likely to provide insights for all stakeholders into fake or inauthentic information campaigns.

(b) represents collective interests and is independent from any online platform; and (c) carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner.[25] In order to safeguard against any conflicts of interest, the DSA enables the relevant DSC to revoke the status of "trusted flagger" if any entity fails to continue meeting the criteria for being designated as such.[26]

At the same time, online platforms are required to put in place necessary technical and organisational measures to ensure that notices submitted by trusted flaggers are processed and decided upon with priority and without delay.[27] Online platforms may also initiate or increase cooperation with trusted flaggers, organise training sessions and exchanges with trusted flagger organisations, and cooperate with other service providers, including by initiating or joining existing codes of conduct or other self-regulatory measures.[28]

The DSA is currently under the consideration of the Council of Europe and the European Parliament.[29] Some of the concerns surrounding the DSA package, as highlighted by dissidents, include the risk of over-censuring by very large online platforms in a bid to reduce overall risks of misinformation hosted on their platforms.[30]

Singapore

Singapore has enacted the Protection from Online Falsehoods and Manipulation Act, 2019, which introduces wide-ranging measures to curb fake news[31] – such as imposing criminal liability upon individuals and other entities sharing misinformation on their own or through the deployment of bots, coupled with powers to correct or takedown misinformation, and blacklist online resources which repeatedly host misinformation.[32]

The grounds for triggering the applicability of the law have been limited to balance the law's impact on freedom of speech and expression, and the law may only be triggered where the impugned information is false and is prejudicial to: (i) the security of Singapore or any part of Singapore; (ii) public health, public safety, public tranquillity or public finances; or (iii) the friendly relations of Singapore with other countries; or is likely to (a) influence the outcome of an election to the office of President, a general election of Members of Parliament, a by-election of a Member of Parliament, or a referendum; (b) incite feelings of enmity, hatred or ill-will between different groups of persons; or (c) diminish public confidence in the performance of any duty or function of, or in the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board.

---

25 Supra Note. 130 at Article 19(2)

26 Supra Note. 130 at Article 19(6)

27 Supra Note. 130 at Article 19(1)

28 Supra Note. 130 at Recital 58

29 See, European Parliament, "Legislative Train Schedule: A Europe Fit for the Digital Age: **Proposal for a regulation of the European Parliament and of the Council on a single market for digital services (digital services act) and amending Directive 2000/31/EC**"; Available at URL: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-services-act; The Internal Market and Consumer Protection (ICMO Committee) of the European Parliament adopted on 13 December 2021 its position on the DSA by 36 votes in favor, 7 against and 2 abstentions. Parliament will debate and vote on the IMCO's report during the January 2022 plenary session. The Council of Europe agreed its position ('general approach') on the proposal for a Digital Services Act in November 2021. The Council wants, inter alia, to amend the scope of the DSA to explicitly include online search engines, better protect minors online, add obligations for online marketplaces and search engines, as well as stricter rules for very large online platforms, and confer some exclusive enforcement powers to the European Commission.

30 See, Erixon F., ""Too Big to Care" or "Too Big to Share": The Digital Services Act and the Consequences of Reforming Intermediary Liability Rules", European Centre for International Political Economy, April 2021, Available at URL: https://ecipe.org/publications/digital-services-act-reforming-intermediary-liability-rules/

31 The Online Falsehoods and Manipulation Act, 2019 does not define "fake news" or "misinformation". However, Article 2(2) of the Act, clarifies that: (a) a statement of fact is a statement which a reasonable person seeing, hearing or otherwise perceiving it would consider to be a representation of fact; and (b) a statement is false if it is false or misleading, whether wholly or in part, and whether on its own or in the context in which it appears. Article 7 of the Act contains a general prohibition on the publication of statements which the publisher knows to be, or has reasons to believe, is a false statement of fact, relatable to grounds for triggering the applicability of the Act.

32 See, Protection from Online Falsehoods and Manipulation Act, 2019, Available at URL: https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625170000?ProvIds=P11-#P11-

However, despite the narrow tailoring of the circumstances in which the law may be enforced, the law has been criticised for obligating online platforms to first take-down content before directing an individual through a complicated appellate process to restore such content.[33] Moreover, the law has also invited opposition on account certain controversial events, where the enforcement of the law has been seen as a tool to supress dissent in the media and curb press freedoms – given especially the wide definition of what constitutes a "false statement of fact".[34] Several posts on social media platforms were notified by the Government for correction under the provisions of the law, thereby forcing journalists to post a version of Government-approved "corrected facts". The absence of narrowly tailored guidelines to prevent the arbitrary determination of what constitutes a "false statement of fact", continues to be a concern voiced by the press.[35]

Malaysia

Malaysia enacted the Anti-Fake News Act 2018, introducing criminal liability for intentional publication of misinformation, and for the intentional financing of such publication.[36] The law defines "fake news" as *"any news, information, data and reports, which is or are wholly or partly false, whether in the form of features, visuals or audio recordings or in any other form capable of suggesting words or ideas."*, and proceeds to criminalise the malicious creation, offering, publication, printing, distribution, circulation or dissemination of fake news.[37] Notably, while an earlier draft of the law criminalised "knowing" creation, publication, etc. of misinformation, the enacted legislation substituted the term "knowingly" with "maliciously" – aiming to set a higher standard of intent for triggering the offence.

The law was subsequently, repealed[38] citing change in Government policy, which sought to address misinformation through existing laws including the Penal Code, the Printing Presses and Publications Act 1984 and the Communications and Multimedia Act 1998.[39]

However, more recently in 2020, the law was revived through an ordinance to tackle Covid-19 related misinformation.[40] The Ordinance penalizes the creation, offering, publication, printing, distribution, circulation or dissemination of any fake news or publication containing fake news, if the same is *"carried out with intent to cause, or which is likely to cause fear or alarm to the public."* Notably, the requirement of such publication being "malicious" has been diluted, since even in the absence of intent, fake news that is considered as *"likely to cause fear or alarm to the public"*, can be proceeded against. The Ordinance also permits complainants to seek an order against the publisher of fake news (and not intermediaries) to remove such fake news from publication.

33 See, Mahmud A.H., Kit T.S., "'Very onerous' process to challenge order on content deemed as online falsehood: Sylvia Lim", Channel News Asia, 9 May 2019, Available at URL: https://www.channelnewsasia.com/singapore/online-falsehoods-bill-workers-party-onerous-appeal-process-877101

34 See, Reporters Sans Frontières, "Singapore uses "anti-fake news" law to eliminate public debate", 6 December 2019, Available at URL: https://rsf.org/en/news/singapore-uses-anti-fake-news-law-eliminate-public-debate

35 See, Reporters Sans Frontières, "RSF explains why Singapore's anti-fake news bill is terrible", 8 April 2019, Available at URL: https://rsf.org/en/news/rsf-explains-why-singapores-anti-fake-news-bill-terrible

36 See, Buchanan K., "Malaysia: Anti-Fake News Act Comes into Force", Library of Congress, Available at URL: https://www.loc.gov/item/global-legal-monitor/2018-04-19/malaysia-anti-fake-news-act-comes-into-force/

37 Ibid. ss. 2 and 4 of the Anti-Fake News Act, 2018

38 See, ANN, "Anti-fake news Act in Malaysia scrapped", Straits Times, 20 December 2019, Available at URL: https://www.straitstimes.com/asia/se-asia/anti-fake-news-act-in-malaysia-scrapped

39 See, Buchanan K., "Malaysia: Bill to Repeal Anti-Fake News Act Passed", Library of Congress, Available at URL: https://www.loc.gov/item/global-legal-monitor/2019-10-24/malaysia-bill-to-repeal-anti-fake-news-act-passed/

40 See Emergency (Essential Powers) (No. 2) Ordinance 2021, Available at URL: https://drive.google.com/file/d/1ZOWsLPsqNL-fulcS3w7LRsmYn-qeRWk__/view; See also, Schuldt L., "The rebirth of Malaysia's fake news law – and what the NetzDG has to do with it", Verfassungsblog, 13 April 2021, Available at URL: https://verfassungsblog.de/malaysia-fake-news/

Other Jurisdictions

Several other jurisdictions have enacted or are in the process of enacting laws to address online harms arising from illegal content online, including misinformation. For instance, the United Kingdom has recently introduced the Online Safety Bill, 2021 before the House of Commons. While the Bill does not target misinformation directly, it imposes a duty of care upon the providers of search services and user-to-user search services (i.e. online platforms that enable users to access content posted by other users), obligating them *inter alia* to act against harmful content, while protecting the right to freedom of speech and expression, and the right to privacy of individuals on their platforms.[41]

The Bill also proposes the establishment of an Advisory Committee on Disinformation and Misinformation, to advice the Office of Communications (**OFCOM**), the designated regulator for online harms, on its actions with regard to curbing misinformation.[42]

Similarly, in 2018, France proposed two Bills, i.e. the Proposed Organic Law against Manipulation of Information,[43] and the Proposed Bill on the Fight Against the Manipulation of Information,[44] before the Assemblée Nationale, with the latter addressing measures to counter misinformation relating to elections,[45] and the former proposing to amend applicable election laws to effect the change.[46]

The law requires online platforms to remove misinformation that is likely to lead to troubling public order or the sincerity of ballots,[47] enables greater transparency with regard to sponsored content and recommender algorithms,[48] and vests the Conseil Supérieur de l'Audiovisuel (**CSA**) to be able to prevent, suspend or terminate the broadcasting of television services controlled by a foreign state in the event of an infringement of the French state's fundamental interests.[49]

While the law was met with significant opposition from Senators, the Constitutional Council upheld the law given its limited scope, and subject to the condition that for the applicability of the law to be triggered, the inaccuracy or misleading nature of the allegations or imputations of fact should be obvious.

41 See, UK Draft Online Safety Bill, 2021, May 2021, Available at URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

42 Ibid. at Chapter 7, Section 98

43 See, Assemblée Nationale, Proposition de Loi Organique, N° 1268, Available at URL https://www.assemblee-nationale.fr/dyn/15/textes/l15b1268_texte-adopte-commission.pdf

44 See, Assemblée Nationale, Proposition de Loi relative à la lutte contre la manipulation de l'information, N° 190, Available at URL: https://www.assemblee-nationale.fr/dyn/15/textes/l15t0190_texte-adopte-provisoire.pdf

45 See, Fiorentino M, "France passes controversial 'fake news' law", EuroNews, 22 November 2018, Available at URL: https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law

46 See, Tiourtite D., Pilain P., "What does the future hold for French anti fake news laws?", Lexology, 3 January 2019, Available at URL: https://www.lexology.com/library/detail.aspx?g=2bd6dde0-6e3c-4055-bce5-fcf3a31b868a

47 Supra Note. 152 at Article 11

48 Supra Note. 152 at Article 14

49 Supra Note. 152 at Article 12

Annexure C
Relevant Legal Provisions

Indian Law

Indian Penal Code

Section 124A: Sedition

Whoever by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Government established by law in India, shall be punished with imprisonment for life, to which fine may be added, or with imprisonment which may extend to three years, to which fine may be added, or with fine.

Explanation 1 — The expression "disaffection" includes disloyalty and all feelings of enmity.

Explanation 2 — Comments expressing disapprobation of the measures of the Government with a view to obtain their alteration by lawful means, without exciting or attempting to excite hatred, contempt or disaffection, do not constitute an offence under this section.

Explanation 3 — Comments expressing disapprobation of the administrative or other action of the Government without exciting or attempting to excite hatred, contempt or disaffection, do not constitute an offence under this section.

Section 153A: Promoting enmity between different groups on ground of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony

1. Whoever —

   a) by words, either spoken or written, or by signs or by visible representations or otherwise, promotes or attempts to promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, disharmony or feelings of enmity, hatred or ill will between different religious, racial, language or regional groups or castes or communities, or

   b. commits any act which is prejudicial to the maintenance of harmony between different religious, racial, language or regional groups or castes or communities, and which disturbs or is likely to disturb the public tranquillity, or

   c) organizes any exercise, movement, drill or other similar activity intending that the participants in such activity shall use or be trained to use criminal force or violence or knowing it to be likely that the participants in such activity will use or be trained to use criminal force or violence, or participates in such activity intending to use or be trained to use criminal force or violence or knowing it to be likely that the participants in such activity will use or be trained to use criminal force or violence, against any religious, racial, language or regional group or caste or community and such activity for any reason whatsoever causes or is likely to cause fear or alarm or a feeling of insecurity amongst members of such religious, racial, language or regional group or caste or community,

   shall be punished with imprisonment which may extend to three years, or with fine, or with both.

2. Offence committed in place of worship, etc.— Whoever commits an offence specified in sub-section (1) in any place of worship or in any assembly engaged in the performance of religious worship or religious ceremonies, shall be punished with imprisonment which may extend to five years and shall also be liable to fine.

Section 153B: Imputations, assertions prejudicial to national integration

1. Whoever, by words, either spoken or written or by signs or by visible representation or otherwise, —

   a) makes or publishes any imputation that any class of persons cannot, by reason of their being members of any religious, racial, language or regional group or caste or community, bear true faith and allegiance to the Constitution of India as by law established or uphold the sovereignty and integrity of India, or

   b) asserts, counsels, advises, propagates or publishes that any class of persons shall, by reason of their being members of any religious, racial, language or regional group or caste or community, be denied, or deprived of their rights as citizens of India, or

   c) makes or publishes and assertion, counsel, plea or appeal concerning the obligation of any class of persons, by reason of their being members of any religious, racial, language or regional group or caste or community, and such assertion, counsel, plea or appeal causes or is likely to cause disharmony or feelings of enmity or hatred or ill-will between such members and other persons,

   shall be punished with imprisonment which may extend to three years, or with fine, or with both.

2. Whoever commits an offence specified in sub-section (1) in any place of worship or in any assembly engaged in the performance of religious worship or religious ceremonies, shall be punished with imprisonment which may extend to five years and shall also be liable to fine.

Section 171G: False statement in connection with an election

Whoever with intent to affect the result of an election makes or publishes any statement purporting to be a statement of fact which is false and which he either knows or believes to be false or does not believe to be true, in relation to the personal character or conduct of any candidate shall be punished with fine.

Section 295A: Deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs

Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of citizens of India, by words, either spoken or written, or by signs or by visible representations or otherwise, insults or attempts to insult the religion or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

Section 298: Uttering words, etc., with deliberate intent to wound religious feelings

Whoever, with the deliberate intention of wounding the religious feelings of any person, utters any word or makes any sound in the hearing of that person or makes any gesture in the sight of that persons or places any object in the sight of that person, shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.

Section 505: Statements conducing to public mischief

1. Whoever makes, publishes or circulates any statement, rumour or report, —

   a) with intent to cause, or which is likely to cause, any officer, soldier, sailor or airman in the Army, Navy or Air Force of India to mutiny or otherwise disregard or fail in his duty as such; or

   b) with intent to cause, or which is likely to cause, fear or alarm to the public, or to any section of the public whereby any person may be induced to commit an offence against the State or against the public tranquillity; or

   c) with intent to incite, or which is likely to incite, any class or community of persons to commit any offence against any other class or community, shall be punished with imprisonment which may extend to three years, or with fine, or with both.

2. Statements creating or promoting enmity, hatred or ill-will between classes. —

   Whoever makes, publishes or circulates any statement or report containing rumour or alarming news with intent to create or promote, or which is likely to create or promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, feelings of enmity, hatred or ill will between different religious, racial, language or regional groups or castes or communities, shall be punished with imprisonment which may extend to three years, or with fine, or with both.

3. Offence under sub-section (2) committed in place of worship, etc.—

   Whoever commits an offence specified in sub-section (2) in any place of worship or in any assembly engaged in the performance of religious worship or religious ceremonies, shall be punished with imprisonment which may extend to five years and shall also be liable to fine.

   Exception — It does not amount to an offence, within the meaning of this section, when the person making, publishing or circulating any such statement, rumour or report, has reasonable grounds for believing that such statement, rumour or report is true and makes, publishes or circulates it in good faith and without any such intent as aforesaid.

Protection of Civil Rights Act, 1955

Section 7: Punishment for other offences arising out of "untouchability"

1. Whoever —

   (...)

   c) by words, either spoken or written, or by signs or by visible representations or otherwise, incites or encourages any person or class of persons or the public generally to practice "untouchability" in any form whatsoever; or

   d) insults or attempts to insult, on the ground of "untouchability", a member of a Scheduled Caste;

   shall be punishable with imprisonment for a term of not less than one month and not more than six months, and also with fine which shall be not less than one hundred rupees and not more than five hundred rupees.

Explanation I —A person shall be deemed to boycott another person who —

e) refuses to let to such other person or refuses to permit such other person, to use or occupy any house or land or refuses to deal with, work for hire for, or do business with, such other person or to render to him or receive from him any customary service, or refuses to do any of the said things on the terms on which such things would be commonly done in the ordinary course of business; or

f) abstains from such social, professional or business relations as he would ordinarily maintain with such other person.

Explanation II — For the purpose of clause (c) a person shall be deemed to incite or encourage the practice of "untouchability"—

i. if he, directly or indirectly, preaches "untouchability" or its practice in any form; or

ii. if he justifies, whether on historical, philosophical or religious grounds or on the ground of any tradition of the caste system or on any other ground, the practice of "untouchability" in any form.

Schedule Case and Scheduled Tribes (Prevention of Atrocities) Act, 1989

Section 3: Punishment for offences of atrocities

1. Whoever, not being a member of a Scheduled Caste or a Scheduled Tribe –

(...)

u) by words either written or spoken or by signs or by visible representation or otherwise promotes or attempts to promote feelings of enmity, hatred or ill will against members of the Scheduled Castes or Scheduled Tribes;

(...)

Shall be punishable for a term which shall not be less than six months, but which may extend to five years with a fine.

Representation of People Act, 1951

Section 123: Corrupt Practices

(...)

3A) The promotion of, or attempt to promote, feelings of enmity or hatred between different classes of the citizens of India on grounds of religion, race, caste, community, or language, by a candidate or his agent or any other person with the consent of a candidate or his election agent for the furtherance of the prospects of the election of that candidate or for prejudicially affecting the election of any candidate.

(...)

4) The publication by a candidate or his agent or by any other person with the consent of a candidate or his election agent, of any statement of fact which is false, and which he either believes to be false or does not

believe to be true, in relation to the personal character or conduct of any candidate, or in relation to the candidature, or withdrawal, of any candidate, being a statement reasonably calculated to prejudice the prospects of that candidate's election.

(...)

Section 125. Promoting enmity between classes in connection with election

Any person who in connection with an election under this Act promotes or attempts to promote on grounds of religion, race, caste, community or language, feelings of enmity or hatred, between different classes of the citizens of India shall be punishable, with imprisonment for a term which may extend to three years, or with fine, or with both.

The Press Council Act, 1978

Section 14: Power to Censure

1. Where, on receipt of a complaint made to it or otherwise, the Council has reason to believe that a newspaper or news agency has offended against the standards or journalistic ethics or public taste or that an editor or a working journalist has committed any professional misconduct, the Council may, after giving the newspaper, or news agency, the editor or journalist concerned an opportunity of being heard, hold an inquiry in such manner as may be provided by regulations made under this Act and, if it is satisfied that it is necessary so to do, it may, for reasons to be recorded in writing, warn, admonish or censure the newspaper, the news agency, the editor or the journalist or disapprove the conduct of the editor or the journalist, as the case may be: Provided that the Council may not take cognizance of a compliant if in the opinion of the Chairman, there is no sufficient ground for holding an inquiry.

2. If the Council is of the opinion that it is necessary or expedient in the public interest so to do, it may require any newspaper to publish therein in such manner as the Council thinks fit, any particulars relating to any inquiry under this section against a newspaper or news agency, an editor or a journalist working therein, including the name of such newspaper, news agency, editor or journalist.

3. Nothing in sub-section (1) shall be deemed to empower the Council to hold an inquiry into any matter in respect of which any proceeding is pending in a court of law.

4. The decision of the Council under sub-section (1), or sub-section (2), as the case may be, shall be final and shall not be questioned in any court of law.

Section 15: General Powers of the Council

1. For the purpose of performing its functions or holding any inquiry under this Act, the Council shall have the same powers throughout India as are vested in a civil court while trying a suit under the Code of Civil Procedure, 1908 (5 of 1908), in respect of the following matters, namely:—

   a) summoning and enforcing the attendance of persons and examining them on oath;

   b) requiring the discovery and inspection of documents;

   c) receiving evidence on affidavits;

   d) requisitioning any public record or copies thereof from any court or office;

e) issuing commissions for the examination of witnesses or documents; and

f) any other matter, which may be prescribed.

2. Nothing in sub-section (1) shall be deemed to compel any newspaper, news agency, editor or journalist to disclose the source of any news or information published by that newspaper or received or reported by that news agency, editor or journalist.

3. Every inquiry held by the Council shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228 of the Indian Penal Code (45 of 1860).

4. The Council may, if it considers it necessary for the purpose of carrying out its objects or for the performance of any of its functions under this Act, make such observations, as it may think fit, in any of its decisions or reports, respecting the conduct of any authority, including Government.

Information Technology Act, 2000

Section 2: Definitions

1. (w) "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

Section 69A: Power to issue directions for blocking for public access of any information through any computer resource

1. Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

2. The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

3. The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

Section 79: Exemption from liability of intermediary in certain cases

1. Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third-party information, data, or communication link hosted by him.

2. The provisions of sub-section (1) shall apply if-

a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

b) the intermediary does not-

i) initiate the transmission,

ii) select the receiver of the transmission, and

iii) select or modify the information contained in the transmission

c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

3. The provisions of sub-section (1) shall not apply if-

a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act

b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation: For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

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

Rule 3: Due Diligence by an Intermediary

1) An intermediary, including social media intermediary and significant social media intermediary, shall observe the following due diligence while discharging its duties, namely:

a) the intermediary shall prominently publish on its website, mobile based application or both, as the case may be, the rules and regulations, privacy policy and user agreement for access or usage of its computer resource by any person;

b) the rules and regulations, privacy policy or user agreement of the intermediary shall inform the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that, —

(...)

ii) is defamatory, obscene, pornographic, paedophilic, invasive of another's privacy, including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force;

(...)

v) violates any law for the time being in force;

vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;

vii) impersonates another person;

viii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation;

(...)

ix) is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person;

c) an intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the Act, shall not host, store or publish any unlawful information, which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force:

Provided that any notification made by the Appropriate Government or its agency in relation to any information which is prohibited under any law for the time being in force shall be issued by an authorised agency, as may be notified by the Appropriate Government:

Provided further that if any such information is hosted, stored or published, the intermediary shall remove or disable access to that information, as early as possible, but in no case later than thirty-six hours from the receipt of the court order or on being notified by the Appropriate Government or its agency, as the case may be:

Provided also that the removal or disabling of access to any information, data or communication link within the categories of information specified under this clause, under clause (b) on a voluntary basis, or on the basis of grievances received under sub-rule (2) by such intermediary, shall not amount to a violation of the conditions of clauses (a) or (b) of sub-section (2) of section 79 of the Act;

(...)

f) the intermediary shall periodically, and at least once in a year, inform its users of its rules and regulations, privacy policy or user agreement or any change in the rules and regulations, privacy policy or user agreement, as the case may be;

g) where upon receiving actual knowledge under clause (d), on a voluntary basis on violation of clause (b), or on the basis of grievances received under sub-rule (2), any information has been removed or access to which has been disabled, the intermediary shall, without vitiating the evidence in any manner, preserve such information and associated records for one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by Government agencies who are lawfully authorised;

(...)

j) the intermediary shall, as soon as possible, but not later than seventy two hours of the receipt of an

order, provide information under its control or possession, or assistance to the Government agency which is lawfully authorised for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents:

Provided that any such order shall be in writing stating clearly the purpose of seeking information or assistance, as the case may be;

2) Grievance redressal mechanism of intermediary:

a) The intermediary shall prominently publish on its website, mobile based application or both, as the case may be, the name of the Grievance Officer and his contact details as well as mechanism by which a user or a victim may make complaint against violation of the provisions of this rule or any other matters pertaining to the computer resources made available by it, and the Grievance Officer shall –

i) acknowledge the complaint within twenty-four hours and dispose off such complaint within a period of fifteen days from the date of its receipt;

ii) receive and acknowledge any order, notice or direction issued by the Appropriate Government, any competent authority or a court of competent jurisdiction.

b) The intermediary shall, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it:

c) The intermediary shall implement a mechanism for the receipt of complaints under clause (b) of this sub-rule which may enable the individual or person to provide details, as may be necessary, in relation to such content or communication link.

Rule 4: Additional due diligence to be observed by significant social media intermediary

1) In addition to the due diligence observed under rule 3, a significant social media intermediary shall, within three months from the date of notification of the threshold under clause (v) of sub-rule (1) of rule 2, observe the following additional due diligence while discharging its duties, namely:

a) appoint a Chief Compliance Officer who shall be responsible for ensuring compliance with the Act and rules made thereunder and shall be liable in any proceedings relating to any relevant third-party information, data or communication link made available or hosted by that intermediary where he fails to ensure that such intermediary observes due diligence while discharging its duties under the Act and rules made thereunder:

Provided that no liability under the Act or rules made thereunder may be imposed on such significant social media intermediary without being given an opportunity of being heard.

Explanation — For the purposes of this clause, "Chief Compliance Officer" means key managerial personnel or such other senior employee of a significant social media intermediary who is resident in India;

b) appoint a nodal contact person for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders or requisitions made in accordance with the provisions of law or rules made thereunder.

Explanation — For the purposes of this clause, "nodal contact person" means the employee of a significant social media intermediary, other than the Chief Compliance Officer, who is resident in India;

c) appoint a Resident Grievance Officer, who shall, subject to clause (b), be responsible for the functions referred to in sub-rule (2) of rule 3.

Explanation — For the purposes of this clause, "Resident Grievance Officer" means the employee of a significant social media intermediary, who is resident in India;

d) publish periodic compliance report every month mentioning the details of complaints received and action taken thereon, and the number of specific communication links or parts of information that the intermediary has removed or disabled access to in pursuance of any proactive monitoring conducted by using automated tools or any other relevant information as may be specified;

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

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

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

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

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

3) A significant social media intermediary that provides any service with respect to an information or transmits that information on behalf of another person on its computer resource

a) for direct financial benefit in a manner that increases its visibility or prominence, or targets the receiver of that information; or

b) to which it owns a copyright, or has an exclusive license, or in relation with which it has entered into any contract that directly or indirectly restricts the publication or transmission of that information through any means other than those provided through the computer resource of such social media intermediary,

shall make that information clearly identifiable to its users as being advertised, marketed, sponsored, owned, or exclusively controlled, as the case may be, or shall make it identifiable as such in an appropriate manner;

4) A significant social media intermediary shall endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary under clause (d) of sub-rule (1) of rule 3, and shall display a notice to any user attempting to access such information stating that such information has been identified by the intermediary under the categories referred to in this sub-rule:

Provided that the measures taken by the intermediary under this sub-rule shall be proportionate having regard to the interests of free speech and expression, privacy of users on the computer resource of such intermediary, including interests protected through the appropriate use of technical measures:

Provided further that such intermediary shall implement mechanisms for appropriate human oversight of measures deployed under this sub-rule, including a periodic review of any automated tools deployed by such intermediary:

Provided also that the review of automated tools under this sub-rule shall evaluate the automated tools having regard to the accuracy and fairness of such tools, the propensity of bias and discrimination in such tools and the impact on privacy and security of such tools.

(...)

6) The significant social media intermediary shall implement an appropriate mechanism for the receipt of complaints under sub-rule (2) of rule 3 and grievances in relation to the violation of provisions under this rule, which shall enable the complainant to track the status of such complaint or grievance by providing a unique ticket number for every complaint or grievance received by such intermediary:

Provided that such intermediary shall, to the extent reasonable, provide such complainant with reasons for any action taken or not taken by such intermediary in pursuance of the complaint or grievance received by it.

7) The significant social media intermediary shall enable users who register for their services from India, or use their services in India, to voluntarily verify their accounts by using any appropriate mechanism, including the active Indian mobile number of such users, and where any user voluntarily verifies their account, such user shall be provided with a demonstrable and visible mark of verification, which shall be visible to all users of the service:

Provided that the information received for the purpose of verification under this sub-rule shall not be used for any other purpose, unless the user expressly consents to such use.

8) Where a significant social media intermediary removes or disables access to any information, data or communication link, under clause (b) of sub-rule (1) of rule 3 on its own accord, such intermediary shall, —

   a) ensure that prior to the time at which such intermediary removes or disables access, it has provided the user who has created, uploaded, shared, disseminated, or modified information, data or communication link using its services with a notification explaining the action being taken and the grounds or reasons for such action;

b) ensure that the user who has created, uploaded, shared, disseminated, or modified information using its services is provided with an adequate and reasonable opportunity to dispute the action being taken by such intermediary and request for the reinstatement of access to such information, data or communication link, which may be decided within a reasonable time;

c) ensure that the Resident Grievance Officer of such intermediary maintains appropriate oversight over the mechanism for resolution of any disputes raised by the user under clause (b).

9) The Ministry may call for such additional information from any significant social media intermediary as it may consider necessary for the purposes of this part.

Rule 5: Additional due diligence to be observed by an intermediary in relation to news and current affairs content

In addition to adherence to rules 3 and 4, as may be applicable, an intermediary shall publish, on an appropriate place on its website, mobile based application or both, as the case may be, a clear and concise statement informing publishers of news and current affairs content that in addition to the common terms of service for all users, such publishers shall furnish the details of their user accounts on the services of such intermediary to the Ministry as may be required under rule 18:

Provided that an intermediary may provide such publishers, who have provided information under rule 18 with a demonstrable and visible mark of verification as being publishers, which shall be visible to all users of the service.

Explanation. —This rule relates only to news and current affairs content and shall be administered by the Ministry of Information and Broadcasting.

Rule 6: Notification of other intermediary.

1) The Ministry may by order, for reasons to be recorded in writing, require any intermediary, which is not a significant social media intermediary, to comply with all or any of the obligations mentioned under rule 4, if the services of that intermediary permits the publication or transmission of information in a manner that may create a material risk of harm to the sovereignty and integrity of India, security of the State, friendly relations with foreign States or public order.

2) The assessment of material risk of harm referred to in sub-rule (1) shall be made having regard to the nature of services of such intermediary, and if those services permit, —

a) interaction between users, notwithstanding, whether it is the primary purpose of that intermediary; and

b) the publication or transmission of information to a significant number of other users as would be likely to result in widespread dissemination of such information.

3) An order under this rule may be issued in relation to a specific part of the computer resources of any website, mobile based application or both, as the case may be, if such specific part is in the nature of an intermediary:

Provided that where such order is issued, an entity may be required to comply with all or any of the obligations mentions under rule 4, in relation to the specific part of its computer resource which is in the nature of an intermediary.

Rule 7: Non-observance of Rules

Where an intermediary fails to observe these rules, the provisions of sub-section (1) of section 79 of the Act shall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code.

ndaconnect@nishithdesai.com

About NDA

At Nishith Desai Associates, we have earned the reputation of being Asia's most Innovative Law Firm – and the go-to specialists for companies around the world, looking to conduct businesses in India and for Indian companies considering business expansion abroad. In fact, we have conceptualized and created a state-of-the-art Blue Sky Thinking and Research Campus, Imaginarium Aligunjan, an international institution dedicated to designing a premeditated future with an embedded strategic foresight capability.

We are a research and strategy driven international firm with offices in Mumbai, Palo Alto (Silicon Valley), Bangalore, Singapore, New Delhi, Munich, and New York. Our team comprises of specialists who provide strategic advice on legal, regulatory, and tax related matters in an integrated manner basis key insights carefully culled from the allied industries.

As an active participant in shaping India's regulatory environment, we at NDA, have the expertise and more importantly – the VISION – to navigate its complexities. Our ongoing endeavors in conducting and facilitating original research in emerging areas of law has helped us develop unparalleled proficiency to anticipate legal obstacles, mitigate potential risks and identify new opportunities for our clients on a global scale. Simply put, for conglomerates looking to conduct business in the subcontinent, NDA takes the uncertainty out of new frontiers.

As a firm of doyens, we pride ourselves in working with select clients within select verticals on complex matters. Our forte lies in providing innovative and strategic advice in futuristic areas of law such as those relating to Blockchain and virtual currencies, Internet of Things (IOT), Aviation, Artificial Intelligence, Privatization of Outer Space, Drones, Robotics, Virtual Reality, Ed-Tech, Med-Tech and Medical Devices and Nanotechnology with our key clientele comprising of marquee Fortune 500 corporations.

The firm has been consistently ranked as one of the Most Innovative Law Firms, across the globe. In fact, NDA has been the proud recipient of the Financial Times – RSG award 4 times in a row, (2014-2017) as the Most Innovative Indian Law Firm.

We are a trust based, non-hierarchical, democratic organization that leverages research and knowledge to deliver extraordinary value to our clients. Datum, our unique employer proposition has been developed into a global case study, aptly titled 'Management by Trust in a Democratic Enterprise,' published by John Wiley & Sons, USA.

Research@NDA

Research is the DNA of NDA. In early 1980s, our firm emerged from an extensive, and then pioneering, research by Nishith M. Desai on the taxation of cross-border transactions. The research book written by him provided the foundation for our international tax practice. Since then, we have relied upon research to be the cornerstone of our practice development. Today, research is fully ingrained in the firm's culture.

Over the years, we have produced some outstanding research papers, reports and articles. Almost on a daily basis, we analyze and offer our perspective on latest legal developments through our "Hotlines". These Hotlines provide immediate awareness and quick reference, and have been eagerly received. We also provide expanded commentary on issues through detailed articles for publication in newspapers and periodicals for dissemination to wider audience. Our NDA Labs dissect and analyze a published, distinctive legal transaction using multiple lenses and offer various perspectives, including some even overlooked by the executors of the transaction. We regularly write extensive research papers and disseminate them through our website. Our ThinkTank discourses on Taxation of eCommerce, Arbitration, and Direct Tax Code have been widely acknowledged.

As we continue to grow through our research-based approach, we now have established an exclusive four-acre, state-of-the-art research center, just a 45-minute ferry ride from Mumbai but in the middle of verdant hills of reclusive Alibaug-Raigadh district. Imaginarium AliGunjan is a platform for creative thinking; an apolitical eco-system that connects multi-disciplinary threads of ideas, innovation and imagination. Designed to inspire 'blue sky' thinking, research, exploration and synthesis, reflections and communication, it aims to bring in wholeness – that leads to answers to the biggest challenges of our time and beyond. It seeks to be a bridge that connects the futuristic advancements of diverse disciplines. It offers a space, both virtually and literally, for integration and synthesis of knowhow and innovation from various streams and serves as a dais to internationally renowned professionals to share their expertise and experience with our associates and select clients.

We would love to hear from you about any suggestions you may have on our research publications.
Please feel free to contact us at **research@nishithdesai.com**.

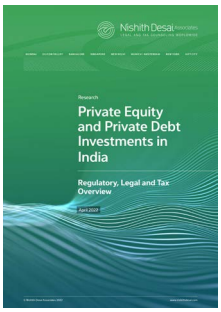
Recent Research Papers

Extensive knowledge gained through our original research is a source of our expertise.

June 2022

Mergers & Acquisitions

An India Legal, Regulatory and Tax Perspective



April 2022

Private Equity and Private Debt Investments in India

Regulatory, Legal and Tax Overview

February 2022

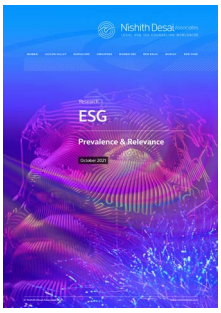
The Indian Pharmaceutical Industry

Regulatory, Legal and Tax Overview

November 2021

The Global Drone Revolution

Aerial Transport, Agritech, Commerce and Allied Opportunities



October 2021

ESG

Prevalence and Relevance

February 2021

Doing Business in India

The Guide for US Businesses and Organizations entering and expanding into India

For more research papers **click here**.

ndaconnect@nishithdesai.com

Nishith Desai Associates

LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI

93 B, Mittal Court, Nariman Point
Mumbai 400 021, India

Tel +91 22 6669 5000

SILICON VALLEY

220 S California Ave., Suite 201
Palo Alto, California 94306, USA

Tel +1 650 325 7100

BANGALORE

Prestige Loka, G01, 7/1 Brunton Rd
Bangalore 560 025, India

Tel +91 80 6693 5000

SINGAPORE

Level 24, CapitaGreen
138 Market St
Singapore 048 946

Tel +65 6550 9855

NEW DELHI

13-H, Hansalaya Building, 15
Barakhamba Road, Connaught Place
New Delhi 110 001, India

Tel +91 11 4906 5000

MUNICH / AMSTERDAM

Maximilianstraße 13
80539 Munich, Germany

Tel +49 89 203 006 268

NEW YORK

1185 6th Avenue, Suite 326
New York, NY 10036, USA

Tel +1 212 464 7050

GIFT CITY

408, 4th Floor, Pragya Towers
GIFT City, Gandhinagar
Gujarat 382 355, India

Make It or Fake It

Tackling Online Misinformation in India

ndaconnect@nishithdesai.com