On the legality and constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

June 21, 2021

By **Torsha Sarkar**, **Gurshabad Grover**, **Raghav Ahooja**, **Pallavi Bedi** and **Divyank Katira**

With assistance from **Tanvi Apte**

Edited and reviewed by **Amber Sinha**

The Centre for Internet and Society, India

Table of contents

Preliminary

On 25 February 2021, the Ministry of Electronics and Information Technology (Meity) notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[1] (hereinafter, '**the rules**'). In this note, we examine whether the rules meet the tests of constitutionality under Indian jurisprudence, whether they are consistent with the parent Act, and discuss potential benefits and harms that may arise from the rules as they are currently framed. Further, we make some recommendations to amend the rules so that they stay in constitutional bounds, and are consistent with a human rights based approach to content regulation. Please note that we cover some of the issues that CIS has already highlighted in comments on previous versions of the rules.[2]

Background

Regulatory apparatus for intermediaries

Section 79 of the Information Technology (IT) Act, 2000 forms the basis of online intermediary liability in India, granting immunity to intermediaries for third-party content provided they do not initiate the transmission, modify its contents, select its recipients, and observe due diligence in carrying out its functions. Standards of due diligence were previously laid out in the Information Technology (Intermediaries Guidelines) Rules, 2011 (hereinafter, '**the 2011 rules**').

Section 69A of the IT Act allows the government to order intermediaries to take down or block access to certain information.

The rules, notified in February 2021, have been issued by the rule-making power granted to the government under sections 69A and 79, referred to in Section 87(2)(zg) and Section 79(2) of the IT Act, and supersede the 2011 rules.

Amendments to the 2011 rules have been previously proposed in 2018. Following a calling attention motion on "Misuse of Social Media platforms and spreading of fake News" in the Parliament, the Ministry of Electronics and Information Technology (MeitY) had floated the The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 (hereinafter, '**the 2018 draft rules**'), which were subject to a period of public consultation.

---

[1] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, <http://egazette.nic.in/WriteReadData/2021/225464.pdf> ('IL Rules 2021').

[2] *See* Gurshabad Grover, Elonnai Hickok, et al, 'Response to the Draft of The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018', *The Centre for Internet and Society*, 31 January 2019, <https://cis-india.org/internet-governance/blog/response-to-the-draft-of-the-information-technology-intermediary-guidelines-amendment-rules-2018> ('CIS 2018 Comments'); Ujwala Uppaluri, 'Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011', *The Centre for Internet and Society*, 16 July 2012, <https://cis-india.org/internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules> ('CIS 2011 Analysis'); Pranesh Prakash, 'CIS Para-wise Comments on Intermediary Due Diligence Rules, 2011', *The Centre for Internet and Society*, 25 February 2011, <https://cis-india.org/internet-governance/blog/intermediary-due-diligence> ('CIS 2011 Comments').

Notably, the 2018 draft rules had concerned itself solely with the regulation of 'intermediaries' as defined within Section 2(w) of the IT Act.

Finally, in February, 2021, the MeitY released the rules under discussion here, with the stated aim of, among others, "*[social media] accountability against its misuse and abuse*" and the provision of a "*robust grievance redressal mechanism*" for "*digital media and OTT.*"[3]

Regulatory apparatus for online curated content and digital news

As per the Allocation of Business (AoB) Rules, 1961, the task of regulating matters relating to cyber laws, and administration of the Information Technology Act, 2000 (**IT Act**) and other IT related laws (which includes the regulation of the newer form of electronic media i.e the internet) had been allotted to the Ministry of Electronics and Information Technology[4] ('**MeitY**'). On the other hand, the regulation of traditional media, including print, radio and television, has been usually under the remit of the Ministry of Information and Broadcasting (**I&B Ministry**).[5]

Previously, the I&B Ministry has attempted to regulate both digital news content and online curated content (OCC). In 2018, an official order was issued by the Ministry to constitute a committee to frame rules for regulation of digital news portals and websites.[6] Further, the draft Registration of Press and Periodicals Bill, 2019 issued by the I&B Ministry had contained provisions for regulation of "news on digital media."[7]

In July 2020, the I&B Ministry had also proposed bringing digital content such as OCC within its ambit.[8] Subsequently, in November 2020, the President had amended the AoB

---

[3] PIB Delhi, 'Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021', 25 February 2021, <https://pib.gov.in/PressReleseDetailm.aspx?PRID=1700749>.

[4] The Government of India (Allocation of Business) Rules, 1961, <https://cabsec.gov.in/writereaddata/allocationbusinessrule/completeaobrules/english/1_Upload_2724.pdf> ('Business Rules').

[5] Business Rules, which include the power to make rules under the respective extant Acts of Parliament. For e.g., *see* Page no 16, point no. 5 of the 128th Report of the Department Related Parliamentary Committee on Subordinated Legislation <http://164.100.47.5/rs/book2/reports/subleg/128threport.htm>. Under the Business Rules, the concerned Ministry is expected to make rules under existing legislation whose administration has been handed over to it, enact and amend legislations and pass Bills on the subject matter under its remit, and then frame subordinate legislation in the form of rules under such Bills turned into Acts.

[6] The Wire Staff, 'Modi Government Turns Its Sights on Freedom of Digital Media', *The Wire*, 6 April 2018, <https://thewire.in/media/modi-regime-lays-the-web-to-curb-freedom-of-digital-media> ('The Wire, Freedom of Digital Media').

[7] Draft Registration of Press and Periodicals Bill, 2019, <https://prsindia.org/files/bills_acts/bills_parliament/Draft%20RPP%20Bill,%202019.pdf>.

[8] The Wire, Freedom of Digital Media notes that news agency Press Trust of India had then quoted I&B Ministry secretary Amit Khare as saying: "OTT being a digital platform will fall under the purview of the ministry of IT but now we are proposing a decision that the content should fall within the purview of I&B ministry." The statement that Online Curated Content Providers ('OCCPs') come under the purview of the IT Act is, arguably, incorrect as discussed later. The November 2020 amendment transpired as a result of the I&B Ministry asking the MeitY to identify ways for transfer of power so that the I&B Ministry could regulate such digital content "without the need for any amendments to the Information Technology Act, 2000".

Rules to place 'Digital/Online Media' under the ambit of I&B Ministry, which includes '*Films and Audio-Visual programmes made available by online content providers*' and '*News and current affairs content on online platforms.*'[9]

Now, Part III of the rules seeks to regulate OCC, digital news publishers and news aggregators, and will be administered by the I&B Ministry.

General comments

Vires of the Rules

The 2021 Rules fall foul in two ways; they are (i) unconstitutional and ultra vires the IT Act; and (ii) prescribe a Code of Ethics for regulating digital media, despite the fact that the parent Act does not recognise digital media as a separate category of entities and does not seek to subject them or their content to any set of special regulations.

A. Ultra Vires the IT Act

(i) Section 79(1) of the IT Act states that the intermediary will not be held liable for any third-party information if the intermediary complies with the conditions laid out in Section 79(2). One of these conditions is that the intermediary observe "*due diligence while discharging his duties under this Act and also observe such other guidelines as the Central Government may prescribe in this behalf.*" Further, Section 87(2)(zg) empowers the central government to prescribe "*guidelines to be observed by the intermediaries under sub-section (2) of section 79.*"

It has been held by the Supreme Court in *State of Karnataka and Another v. Ganesh Kamath & Ors* [10]that: "*It is a well settled principle of interpretation of statutes that conferment of rule making power by an Act does not enable the rule making authority to make a rule which travels beyond the scope of the enabling Act or which is inconsistent therewith or repugnant thereto.*" A combined reading of Section 79(2) read with Section 89(2)(zg) makes it clear that the power of the Central Government is limited to prescribing guidelines related to the due diligence to be observed by the intermediaries while discharging its duties under the IT Act. However, the 2021 guidelines have imposed additional requirements and widened the ambit of requirements to be fulfilled by the intermediary.

For instance, the rules include an obligation on a significant social media intermediary, primarily messaging services, to enable the identification of the first originator of the information on their service when required either by a government (under Section 69 of the IT Act) or court order. This obligation can only be fulfilled if messaging services

---

[9] Cabinet Secretariat, Notification S.O. 4040(E.), 9 November 2020, <https://cabsec.gov.in/writereaddata/allocationbusinessrule/amendment/english/1_Upload_2604.pdf> ('Notification S.O. 4040(E.)').

[10] 1983 SCR (2) 665

technically modify their platform to remove end-to-end encryption, or add additional metadata to each message in a way that undermines security and privacy guarantees that end-to-end encryption offers. As discussed above, the executive through subordinate legislation can only make rules that are consistent with the parent act and with the legislative policy enunciated by the central government. There is nothing in Section 79 of the IT Act to suggest that the legislature intended to empower the Government to to mandate changes to the technical architecture of services, or undermine user privacy .

(ii) Similarly, the IT Act does not prescribe for any classification of intermediaries. Section 2(1) (w) of the Act defines intermediaries as "*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".* Intermediaries are treated and regarded as a single monolithic entity with the same responsibilities and obligations.

The 2021 Intermediary Guidelines have now established and defined new categories of intermediaries; namely (i) Social Media Intermediary;[11] and (ii) Significant Social Media Intermediary.[12] This classification comes with an additional set of obligations for significant social media intermediaries as well as expansion of the obligations for social media intermediaries. The additional set of obligations placed on social media intermediaries finds no basis in the IT Act, which does not specify or demarcate between different categories of intermediaries.

The 2021 Rules have been prescribed under Section 87(1) and Section 87(2)(z) and (zg) of the IT Act. These provisions do not empower the Central Government to make any amendment to Section 2(w) or create any classification of intermediaries. As discussed previously, the rules cannot go beyond the parent act or prescribe policies in the absence of any law/regulation authorising them to do so.

Therefore, while we believe and agree that classification of intermediaries (instead of treating the disparate group of intermediaries as one category) is a more nuanced approach for their regulation, we recommend that such a classification should happen through an amendment to the parent act and the amendment should also prescribe the additional responsibilities and obligations of significant social media intermediaries. Documents obtained under the Right to Information Act reveal that advisors in the

[11] IL Rules 2021, Rule 2(w) states, "'Social Media Intermediary' means an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services."
[12] IL Rules 2021, Rule 2(v) states, "'Significant Social Media Intermediary' means a social media intermediary having number of registered users in India above such threshold as notified by the Central Government." The threshold for social media intermediary to be considered and regulated as a "significant social media intermediary" was notified on February 26, 2021, as fifty lakh (5 million) registered users.

Ministry of Law and Justice were also of the opinion that the changes brought through the rule went beyond the scope of the current IT Act.[13]

Note that many of the new obligations in the 2021 rules are outside the scope of delegated legislation. For brevity, this point is not repeated in our analysis of specific rules (in the next section).

B. The IT Act's lack of power to regulate 'digital media'

Part III of the 2021 Rules regulate 'digital media' which is defined as digitized content transmitted, processed, edited etc. by intermediaries and 'publishers'.[14] The rules further classify 'publishers' in two parts:

a) '*publisher of news and current affairs content*': which includes online papers, as well as intermediaries like news portals and aggregators, but not printed newspapers[15] or individuals who are *not* transmitting content in "*the course of systematic business, professional or commercial activity*".
b) '*publisher of online curated content*': which includes OCCPs, but does not include any individual or user who is not transmitting such content "*in the course of systematic business, professional or commercial activity*".

Section 69A and 79 (under which these rules are issued) of the IT Act are both very clear that they apply to intermediaries. Section 79 primarily discusses intermediary liability, and the conditions an intermediary has to meet to qualify for immunity from liability for third-party content. Section 69A is also clear that directions for content takedown may only be issued to intermediaries or government agencies. The provision further notes that the "intermediary" that does not comply with such orders will be criminally liable.

The rules define publishers and allow the government to send takedown notices to them, whereas these parent provisions in the Act do not envision such powers. As discussed previously, the subordinate legislation cannot through rules go beyond the remit of the parent act.[16] In regulating publishers under section 69A and 79 therefore, the rules exceed the ambit of the rule-making powers contained in the said sections read with section 87(2). Any regulation of the digital media is only possible through an amendment to the IT Act., so as to empower the government to regulate the content of publishers.

However, one might argue that the rules may be saved by the general rule-making power contained in a statute, provided the rules do not travel beyond the scope of the Act, as has been held by the SC in the case of *Academy of Nutrition Improvement v Union of*

---

[13] Saurav Das, '2 Modi Govt Advisers Warned New IT Rules Beyond Scope Of Law, Were Overruled', *Article 14*, 17 May 2021, <https://article-14.com/post/2-modi-govt-advisers-warned-new-it-rules-beyond-scope-of-law-were-overruled>.
[14] IL Rules 2021, Rule 2(i).
[15] IL Rules 2021, Rule 2(t), read with Rule 2(n).
[16] Union of India & Ors. v. S. Srinivasan, (2012) 7 SCC 683, <https://indiankanoon.org/doc/22125136/>.

India.[17] But even a general power to make rules or regulations for carrying out or giving effect to the Act, is strictly ancillary in nature and cannot enable the authority on whom the power is conferred to extend the scope of general operation of the Act. As it was relied upon in the case: "*Such a power will not support attempts to widen the purposes of the Act, to add new and different means to carrying them out, to depart from or vary its terms".*[18]

In this case, the general rule making power under the IT Act has been conferred under section 87(1). The scope and ambit of the Act may be inferred from other provisions in the Act, and the Statement of Objects and Reasons of the Act.[19] The relevant portion of the Statement of Objects and Reasons of the IT Act and the Amendment[20] that impose publisher liability are codified under sections 66, 67, 67A, and 67B , impose only criminal liability based on certain grounds on publishers. Moreover, these sections only lay down the offences, without laying down any power to make rules and without empowering the government to order them to take particular content down. Thus, these provisions as well as the Statement of Objects and Reasons do not foresee regulation of such 'publishers' under the Act or rules thereunder. As a consequence, part III of the rules fails in terms of validity and legality to that effect.

Moreover, through an amendment of 2020 to the AoB Rules, 'digital media' now comes under the purview and remit of the I&B Ministry.[21] Therefore, any legislative proposal to regulate such media should come from the I&B Ministry. The intent behind the amendment to the Business Rules was that the content by publishers (and consequently the publishers of such content) shall be regulated by the I&B Ministry, while 'platforms' (and consequently the content on platforms) shall be regulated by the MeitY.[22] Thus, the current framework for the rules results in the bypassing legislative and parliamentary procedure of enacting specific legislation that regulates digital news content, leading to abdication of legislative duties.

Since the entirety of Part III of the Rules suffers from illegality, in this note, we do not go into the specific merits of the framework that seeks to regulate digital news publishers and online curated-content platforms. Any such framework must find its foundation in a law duly deliberated and passed by the Parliament.

---

[17] Academy of Nutrition Improvement & Ors. v. Union of India, (2011) 8 SCC 274 <https://indiankanoon.org/doc/665756/> ('Academy of Nutrition Improvement Case').
[18] Academy of Nutrition Improvement Case.
[19] *See* The Information Technology Act, 2000, <https://www.meity.gov.in/writereaddata/files/itbill2000.pdf> ('IT Act') and The Information Technology (Amendment) Act, 2008, <https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf> ('IT Act, 2008 Amendment'); *also see* Dr. Mahachandra Prasad Singh v. Chairman, Bihar Legislative Council & Ors., (2004) 8 SCC 747, <https://indiankanoon.org/doc/1300862/>.
[20] IT Act, 2008 Amendment.
[21] Notification S.O. 4040(E.).
[22] *See* Scroll Staff, 'Centre's Move to Regulate OTT Platforms was to Bring Content Under One Place, says I&B ministry', *Scroll*, 17 December 2020, <https://scroll.in/latest/981513/centres-move-to-regulate-ott-platforms-was-to-bring-content-under-one-place-says-i-b-ministry>, where I&B Ministry Secretary has once again been quoted stating that the intent behind the said amendment was to regulate content at one place i.e the I&B Ministry, and platforms at another i.e MeitY. The Secretary said so at a summit, a recording of which is available with the Press Information Bureau.

Classification of intermediaries

One of the more significant changes brought about by the 2021 rules is the attempt at classifying the entities which would fall within the ambit of Part I-II of the rules. In the previous renditions of these rules, including the draft version floated in 2018, intermediaries were generally treated as a single, monolithic entity, much to the concern of civil society organizations and private companies, since the resulting regulation then became one-size-fits-all, erasing much of the nuances present in the internet ecosystem.[23]

With the operation of the 2021 rules, however, there are now a total of three categories of entities for the purposes of its operation:

a) 'Intermediary': As per the definition in the IT Act, an intermediary means "*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.*"[24]

b) 'Social Media Intermediary' (SMI): These are defined in the 2021 rules, as intermediaries which "*primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services.*"[25]

c) 'Significant Social Media Intermediary' (SSMI): Also defined within the 2021 rules, a SSMI is a social media intermediary with a certain user threshold, as would be notified by the Central Government.[26] As of the time of writing this, the government has notified this threshold to be 50 lakhs, or 5 million registered users.[27]

The attempt by the 2021 rules to introduce more nuance into the regulatory framework of intermediary liability brings with it certain concerns regarding the definitions and classifications, which we discuss here.

'Intermediary'

The 2021 rules envisage a variety of compliance requirements that these entities ought to adhere to. Of interest here, are the requirements surrounding content takedown. For the purposes of our discussion, 'content takedown requirements' are broadly defined to include any provision that either requires these entities to take steps towards regulating

---

[23] Torsha Sarkar, 'A Deep Dive into Content Takedown Timeframes', *The Centre for Internet and Society*, 3 December 2019, <https://cis-india.org/internet-governance/blog/torsha-sarkar-november-30-2019-a-deep-dive-into-content-takedown-timeframes>.
[24] IT Act, Section 2(w).
[25] IT Rules 2021, Rule 2(w).
[26] IT Rules 2021, Rule 2(v).
[27] Ministry of Electronics and Information Technology, Notification S.O. 942(E.), 25 February 2021, <http://egazette.nic.in/WriteReadData/2021/225497.pdf>.

user content on their platforms, or requires these entities to respond to legal, government notices for censorship of 'objectionable' user content. Significant portions of Rule 3, and Rule 4 comprise these content takedown requirements for these entities, and includes, for instance, publication of Terms and Conditions (ToC) listing certain kinds of content that the users would be prohibited from posting, responding to government notices on censorship ("takedown notices") within a specific time period, and so on.

The issue here, however, is that a majority of these requirements still continue to apply to 'intermediaries' as a whole. The definition of 'intermediaries' as it currently stands, encompasses a vast plethora of entities, including internet service providers, cyber cafes, and online payment services. While content takedown requirements make sense for entities like Facebook and Twitter — whose services concern user content (and which would, arguably fulfill the criteria of a SMI) — to be able to comply with these content takedown requirements, it would be absurd to expect, for instance, cyber cafes, or internet exchange providers, to comply with similar requirements and follow similar legal routes. Enforcing such a requirement would contribute to creation of further regulatory uncertainty amongst these services.

Recommendation

We have previously argued that content takedown requirements should be applied only to those intermediaries whose technical architecture allows them to comply with the same.[28] In light of the same, it is concerning to see that a significant amount of content takedown requirements continue to be applied to be the broad gamut of entities within the IT Act, including entities who do not have anything to do with user content. Accordingly, we recommend that these rules be modified to reflect this.

More specifically, we recommend that Rule 3(1)(b), (d), (g) and Rule 3(2) be modified to ensure that intermediaries are made to comply with these obligations only wherever it is technically possible.

'Social Media Intermediary' (SMI)

As indicated above, a SMI is defined as any intermediary who enables online interaction between two or more 'users'[29] and allows them to share, upload, modify 'information'[30], etc. Taken together, the ambit of a SMI becomes exceptionally broad, and would bring about nearly every entity engaged with facilitating any sort of 'interaction' between two or more users within its scope. Further, this conceptualization is absolute in nature and without any exceptions for either platforms operating without a profit motive (including online encyclopaedias like Wikipedia), or for entities solely facilitating private communication between users.

The draft Personal Data Protection (PDP) Bill, 2019 has an analogous definition of SMI. However, the definition embodied in that Bill contained certain exceptions, including:

---

[28] Torsha Sarkar, 'Why Should We Care About Takedown Timeframes?', *CyberBRICS*, 1 April 2020, <https://cyberbrics.info/why-should-we-care-about-takedown-timeframes/>.
[29] IL Rules 2021, Rule 2(1)(x).
[30] IT Act, Section 2(1)(v).

intermediaries who a) enable commercial/business transactions, b) provide access to the internet, or c) are search-engines, online encyclopedias, email services or online storage services.[31] Similar exceptions exist in other intermediary liability laws around the world, including the NetzDG in Germany[32], and the Digital Services Act in the European Union (EU)[33].

Additionally, given the broad definition, a substantive number of entities that are cited as illustrations of an 'intermediary' within the meaning of Section 2(w) of the IT Act, including, "*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*" would probably still fulfill the criteria of a SMI. In that case, this attempt at classification between an intermediary and a SMI becomes redundant.

Recommendation

We urge that the government reconsiders the classification between an intermediary and a SMI, and updates the latter definition with the underlying foundation that any legal obligations can be enforced only by those entities whose technical architecture would allow them to execute them.

'Significant Social Media Intermediary' (SSMI)

Finally, as indicated above, a SSMI is currently defined as a SMI with fifty lakh, or five million registered users in India. As per the operation of the rules *in toto*, SSMIs seem to bear an additional level of compliance around content takedown requirements, including a higher level of transparency and accountability towards its users. This is a step towards the right direction, and would bring these entities within adherence of Principle 14 of the UN Guiding Principles on Business and Human Rights, which emphasize that the "*means through which a business enterprise meets its responsibility to respect human rights will be proportional to, among other factors, its size.*"[34]

However, we note that the government notification to this effect is inadequate in terms of how this user threshold would be calculated. The NetzDG in Germany, for instance, which is supposed to be applicable to intermediaries with 2 million registered users, also ran into a similar problem, since it had not clarified whether the user-count would be

---

[31] The Personal Data Protection Bill, 2019, Section 26 *proviso*, <https://prsindia.org/files/bills_acts/bills_parliament/Personal%20Data%20Protection%20Bill,%202019.pdf> ('PDP Bill'). .

[32] Network Enforcement Act (Germany),Federal Law Gazette I, p. 3352, valid as from 1 October 2017, ,<https://germanlawarchive.iuscomp.org/?p=1245> ('NetzDG'), provides that 'telemedia service providers' *Includes* entities, who, "for profit-making purposes operate internet platforms which are designed to enable users to share any content with other users or to make such content available to the public", and *excludes,* a) "platforms offering journalistic or editorial content, the responsibility for which lies with the service provider", b) "platforms which are designed to enable individual communication or the dissemination of specific content".

[33] 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', Doc. 2020/0361 (COD), 15 December 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en>.

[34] Guiding Principles on Business and Human Rights, 2011, Principle 14, <https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf>.

calculated on the basis of an active user-base, or an average value calculated over time.[35] In a similar vein, the current framework for the calculation of user thresholds for SSMIs operating in India, is currently clouded in ambiguity.

Finally, we are also concerned with the specific details of the user threshold. The current threshold is set at 50 lakh, that translates to 5 million registered users. In comparison, the NetzDG has 2 million as its threshold in a country where 88% of the population[36] (out of a total of 83.1 million[37]) or 73 million people use the internet. The threshold set by the German Government is, thus, 2.7% of the digital population. Whereas, in India, the internet using population of approximately 776 million[38], the threshold is 5 million — which is less than 0.007% of the Indian digital population. Setting such a low threshold, therefore, might create additional hurdles for smaller social media intermediaries and in fact disincentivize growth in smaller SMIs.

Recommendation

Firstly, we recommend that the current user threshold for designating SSMIs be reconsidered, with due inputs from the industry, and comparative perspectives from legislations around the world.

Secondly, we recommend that the government publishes follow-up details that throw more light on the procedure utilized to determine SSMI, and that these details, should at the least, answer the following questions:

- How would the appropriate authority ascertain this user count? Would the relevant entities be required to file this information with the authority?
- Would all SMIs be required to file their registered user counts at the first instance for the government to determine the classification between SMIs and SSMIs?
- Would this calculation be a periodic exercise? If yes, then what would be the duration of each interval?
- Would the registered user counts be calculated on the basis of daily active users or monthly active users?

Lack of consultation

As stated earlier, the obligations with respect to intermediaries were subject to a consultative process in 2018. Given the extent of changes to the intermediary liability, and the large number of responses, we believe the Government should have initiated a second round of consultations before notifying the 2021 Rules.

---

[35] Subhodeep Jash, 'Outsourcing Citizenship, Attacking Civil Liberties: Germany's NetzDG', *The Governance Post*, 17 October 2017, <https://www.hertie-school.org/the-governance-post/2017/10/outsourcing-censorship-attacking-civil-liberties-germanys-netzdg/>.

[36] International Telecommunication Union (ITU) World Telecommunication/ICT Indicators Database, 'Individuals Using the Internet (% of Population) - Germany', *World Bank Data* (latest data as on 2019), <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=DE>.

[37] United Nations Population Division, Eurostat Demographic Statistics, et al, 'Population Total - Germany', *World Bank Data* (latest data as on 2019), <https://data.worldbank.org/indicator/SP.POP.TOTL?locations=DE>.

[38] Telecom Regulatory Authority of India, 'The Indian Telecom Services Performance Indicators July – September, 2020', 21 January 2021, <https://www.trai.gov.in/sites/default/files/QPIR_21012021_0.pdf>.

Additionally, it is important to note that the regulations on digital news publishers and online curated content platforms (in Part III of the 2021 rules) were not part of the consultation in 2018. These extensive regulations have been issued through executive notification with a short timeline for compliance, without a single consultation.

Rule-wise comments

Rule 2(1)(i): Definition of digital media

Rule 2(1)(i) defines 'Digital Media' as digitized content transmitted online, and includes any content processed by either an intermediary, 'Publishers of news and current affairs content' ('**publishers of news**') or a publisher of OCC[39]. This definition is worded in such broad terms to encompass nearly all online interactions that a user might have using digital entities.

To understand the ramifications of this rule, it is important to understand the definition of the entities used in the text of the rule. A publisher of news includes such other entities that are '*functionally similar*' to the illustrated publishers of news, though the rules do not delineate what the '*functionality*' test entails.

One way of interpreting this is to look at the IT Act for the definition of 'publishes', which has been defined (albeit for the purposes of provisions relating to sexual offences only) as "*reproduction in the printed or electronic form and making it available for public*"[40]. Since printed forms of publication have been excluded from the ambit of publishers of news under the rules, one interpretation of the 'functionality' test can be: reproduction in the electronic form and making it available for the public, whereas the content in question is 'news'. As a result of this interpretation, social media platforms like Twitter, Facebook which curate 'news feeds' could potentially come under this residue clause. This could also include analysis by individuals in the form of tweets, social commentary clips, stand up comedy, Instagram reels, and arguably, even messages (especially those that go viral) transmitted through private-messaging apps like Whatsapp, Telegram and Signal.

Further, publishers of news would include those users or individuals who are in fact transmitting news in the course of systematic business, professional or commercial activity[41]. This in turn, opens up the possibility for individual liability, under the rules,

---

[39] It has been defined with respect to (a) intermediaries (b) publishers. Further, there are two sub-categories of publishers that have been covered, namely: publishers of news and current affairs content and publishers of online curated content. Digital media is defined as digitized 'content', which is defined in rule 2(g) to mean an electronic record under section 2(t) of the IT Act. As per rule 2(m), 'news and current affairs content' ('**news**'), means any newly received or noteworthy content especially of socio-political, economic or cultural nature, including but not limited to analysis made available online which is processed, edited, transmitted, stored or received by an intermediary or a publisher of news and current affairs content.

[40] IT Act, Section 66E, Explanation (d).

[41] *See* the *Background* section for a full definition of 'publishers of news'.

which could also include an originator.[42] Thus, there could arise a situation where an originator of a message is treated as a publisher of news. For example, a person creating and forwarding a viral Whatsapp message in the course of systematic business, professional or commercial activity could be considered a publisher of news, whose content can be taken down under both part II and part III. Additionally, as laid down in Rule 9(2), there might be liability for '*consequential action*' on such an originator for contravention of any law in force.

On a perusal of the rules, it is evident that 'digital media' has not been used anywhere else except in the definition clauses, and its definition by itself has no repercussion of its own. But when the definition is read along with the definition of 'news and current affairs content', it takes on an all-encompassing meaning by a result of which it exceeds the scope of the IT Act (See *General Comments*).

Recommendation

Delete Rule 2(1)(i).

This would have the effect of nullifying the ramifications of part III, and would save the rules from illegality. As a whole, part III of the rules should be struck down, as it goes beyond the scope of the IT Act. We recommend regulating publishers, instead, through an Act of Parliament (if at all), introduced duly as per parliamentary and administrative procedures[43], and not through such rules issued under the IT Act.

Rule 3(1)(b): Users to not post certain content

Rule 3(1)(b) compels intermediaries to inform users not to post content that is *inter alia* "*racially, ethnically or otherwise objectionable*", "*relating or encouraging money laundering or gambling*", "*libellous*", "*obscene*", or "*insulting or harassing on the basis of gender.*"

These are undefined terms, unrelatable to specific offences in the Indian Penal Code (IPC) or any other statutes. Many of these grounds have no constitutional basis, and are not legal standards, but subjective indicators of personal sensitivities.[44] As ruled by the Supreme Court in *Shreya Singhal v. Union of India*, terms that are as vague and overbroad, create the possibility of over-censorship and a chilling effect on users.[45]

It should be further noted that the rule does not explicitly prohibit such speech or make it prosecutable. However, this rule must be read in conjunction with rule 3(d) that allows intermediaries to remove such content on a voluntary basis with impunity. It can be argued that the cumulative effect of these rules is that the state is encouraging the stifling

[42] IT Act, Section 2(za) defines 'originator', which has been included in the IL Rules 2021, Rule 2(x)'s definition of 'user'.
[43] This can be done upon introduction of a Bill in Parliament by the I&B Ministry as per the Business Rules.
[44] CIS 2011 Analysis.
[45] Shreya Singhal v. Union of India, (2015) 5 SCC 1, <https://indiankanoon.org/doc/110813550/> ('Shreya Singhal Case').

of such content by private companies, without any basis in law, which would amount to unconstitutional indirect censorship.[46]

Recommendation

Delete Rule 3(1)(b).

Rule 3(1)(d): Content takedown

Rule 3(1)(d) contains procedures that intermediaries (including SMI and SSMI) ought to follow while dealing with government takedown notices. An intermediary would be required to remove access to content upon receiving 'actual knowledge' about such content within a turnaround period of 36 hours. An intermediary would be said to possess actual knowledge only on the receipt of a government notification or a court order.[47]

Additionally, the rules mention that any legal takedown order, issued either by the government or the court, ought to be restricted to content that is prohibited in the interests of "*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*".

The need for harmonization of content takedown procedures

This provision moves the guidelines towards formal compliance with the Supreme Court's directions in *Shreya Singhal v. Union of India*[48], in ensuring that intermediaries are only legally required to act on content takedown orders from authorised government agencies or courts.

While such adherence with established judicial doctrine is the correct stance in law, we highlight that the content takedown procedure under Rule 3(1)(d) is currently not in harmony with the procedure laid down by section 69A of the IT Act, and the rules made thereunder ["the blocking rules"]. The framework created by section 69A and the blocking rules envisage a completely different procedure for removal of online content, which includes allowing the intermediary or the originator an opportunity to represent themselves, periodic review of the blocking orders issued by the government, and the provision of at least 48 hours for the concerned individual/entity to respond to a request for blocking.[49] Also, the scope of the grounds on which the government is empowered to send blocking orders under section 69A, also overlap with those delineated in Rule 3(1)(d), save 'decency and morality'.

---

[46] CIS 2011 Analysis.

[47] CIS 2011 Analysis.
[48] Shreya Singhal Case.
[49] *See* Gurshabad Grover and Torsha Sarkar, 'Content takedown and Users' Rights', *The Leaflet*, 12 February 2020, <https://www.theleaflet.in/content-takedown-and-users-rights/>, which shows that Section 69A has flaws of its own.

In light of this, we believe that it is important for the two legal frameworks to be harmonized, to ensure that the procedure for removal of online content is uniform and the same safeguards are available to the intermediary/originator of the information.

Voluntary removal by intermediaries

The provisions further clarify that any content removed by the intermediary on the basis of government or court orders, voluntarily under Rule 3(1)(b), or based on user grievances will not disqualify them from immunity from liability for third-party content. Such a clarification was critical to include given that the text of section 79 does not contain this clarity.[50]

However, there is a need for the rules to consider the fact that voluntary removal and flagging of content by lots of intermediaries goes beyond the categories mentioned in Rule 3(1)(b). Many online communities also have their own content rules, and may prohibit content beyond what is described under 3(1)(b). Spam is such an example, which may not meet any criteria under 3(1)(b), but is regularly monitored for and removed by social media intermediaries. Another example is online collaborative communities like Wikipedia would have other users edit and delete content based on the quality. We recommend that this editorial independence be protected to a large extent for all intermediaries dealing with third party content.[51]

There is a need to expand the scope of the provision to ensure that voluntary content removal and flagging by intermediaries is permissible in all cases.

Recommendations

1. Remove the content takedown provisions, as they create disharmony with Section 69A of the IT Act
2. Create a general exemption for good faith content moderation and flagging, clarifying that such actions will not cause an intermediary to lose immunity from liability for third-party content

Rule 3(1)(i): Security practices

This rule mandates intermediaries to follow security practices set out in the The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**'Security Practices Rules**') that have been issued under Section 43A of the IT Act. The rule creates a level of redundancy, because body corporates dealing with sensitive personal information are already obligated to follow the Security Practices Rules.

---

[50] *See* Anna Liz Thomas and Gurshabad Grover, 'Donald Trump is Attacking the Social Media Giants. Here's what India Should Do Differently", *Scroll*, 25 June 2020, <https://scroll.in/article/965151/donald-trump-is-attacking-the-social-media-giants-heres-what-india-should-do-differently>.

[51] This comment is not aimed to critique network neutrality regulations that obligate internet service providers to not block or throttle content without a legal basis.

On the other hand, the presence of the obligation creates inconsistencies with the parent Act in other cases. *First*, the obligations under Section 43A are only set out for "body corporates", whereas this provision seeks to impose them on all entities that may be performing an intermediary function. *Second*, and more importantly, Section 43A only imposes civil damages for the failure to protect information of individuals. The effect of Rule 3(1)(i) in that non-compliance by an intermediary can create opportunities for criminal liability for third-party content. Thus, this rule may be *ultra vires* the parent Act, as it tries to indirectly impose criminal liability for an act (i.e. failing to protect personal information stored in a computer resource) which the parent Act only prescribes civil damages.

Recommendation

Delete Rule 3(1)(i).

Rule 3(1)(j): Information requests

Rule 3(1)(j) obligates intermediaries to either provide 'information under its control' or 'assistance' to a government agency authorized for investigative or cyber security purposes, within 72 hours of receipt of an order to that effect. The *proviso* states that such order needs to be in writing and should clearly state the purpose for seeking this information/assistance.

The terms used in provision, including 'information under its control' and 'assistance' are broad and undefined. Further, while this rule identifies the issuing authority as a government agency authorized for specific purposes, this is still a broad ambit, capable of amassing a number of agencies within its remit. As a result, the scope of information that can be requested under this rule can potentially be anything. It is unclear whether this power to send information requests is referring to surveillance powers included in other provisions or legislation, or the rules create an independent power and procedure. This is further compounded by the fact that the rule does not envisage any oversight over the decision-making process for issuing such an order.

Consider Rule 419A of the Indian Telegraph Rules, 1951, which states that an interception order can be normally issued by only specific, identified government officials. Further, Rule 419A makes provision for a Review Committee who would be acting as an oversight authority for interception orders passed, and would also be empowered to set aside any orders it deems to be 'unlawful'. Similar procedural safeguards, including exact designation of the agency authorized to issue such orders, and oversight, can be found under section 69 of the IT Act and Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, made thereunder. The 2021 rules therefore raise potential conflicts with the 'blocking' rules, and may be *ultra vires* Section 69 of the Act.

The absence of such critical details from Rule 3(1)(j) raises serious concerns regarding user safety and privacy. We are also concerned that the period of seventy-two hours for

compliance may prove to be inadequate. As we have argued earlier[52], an intermediary's capacity to comply with such requests would depend on its size of organization, location and the complexity of the request. It is unclear if all intermediaries would have the capacity to comply with orders within the designated time period. Additionally, the rule does not provide a mechanism for the intermediary to ask for additional time. As a result, the pressure of complying within a specific timeframe may compel intermediaries to not undertake the required due diligence to verify the validity of the orders.

Finally, the parent provisions under which this rule is issued are section 79 and section 69A of the IT Act. Neither of these sections envisage any procedures regarding information requests that can potentially violate a user's right to privacy. As we have detailed above, the issue of interception orders are already covered by several other legislations, with detailed safeguards and oversight. In such light, the presence of Rule 3(1)(j) within the 2021 rules exceeds the scope of delegated legislation, thereby making it *ultra vires* the parent provision.

Recommendation

Delete Rule 3(1)(j).

Rule 3(2): User grievances and redressal mechanisms

Rule 3(2) obligates intermediaries to set up a mechanism for user 'grievance redressal'. Broadly, Rule 3(2) empowers users to be able to lodge complaints, or notify the intermediary with regards to a violation of any of the provisions of the rules.,It also obligates intermediaries to respond and dispose of these complaints within specified timeframes.

There are two possible interpretations of this rule with regards to the *nature of the content* which a user would be empowered to lodge/notify complaints.

First interpretation: Intermediaries legally obligated to act on grievances related to sharing of intimate or morphed media

The first possible interpretation comes from Rule 3(2)(b), whereby an intermediary is obligated to remove content depicting private sexual matters of an individual or artificially morphed images of such an individual, either on a complaint lodged by the individual themself or lodged on their behalf. This provision is enacted with an aim to curb non-consensual distribution of intimate images (commonly dubbed as 'revenge porn'). The Special Rapporteur to the Human Rights Council has previously noted that such distribution is often done with the purpose of "*shaming, stigmatizing or harming the victim.*"[53] A report by IT for Change on women students in Tamil Nadu found that one of the most concerning forms of technology-mediated violence was the sharing of morphed

[52] CIS 2018 Comments.
[53] Human Rights Council, 'Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective', Doc. A/HRC/38/47, 18 June 2018, <https://undocs.org/pdf?symbol=en/A/HRC/38/47>.

images and the subsequent blackmailing by their use.[54] In light of that, it is important to highlight an intermediary's obligation towards its users in respecting their privacy, dignity and autonomy by rapidly responding to such dissemination and distribution.

However, the language of the provision does not incorporate 'consent' within its framework. It is important for the law to highlight that the dissemination ought to be specifically *non-consensual*, before an intermediary's obligation is triggered. For contrast, consider that the element of consent is conspicuous in Section 66E of the IT Act, which criminalises non-consensual sharing of intimate imagery.

Further, we note that the authorization to send a takedown notice under this provision is extended to not only the person whose imagery is being circulated, but to '*any person on [their] behalf*'. This is an exceptionally broad scope, and we are concerned that this would allow for abuse of this provision to censor speech online. Historically, several online spaces have existed that have catered to marginalized communities in their attempts of defining their sexualities and their identities by way of, among others, photos, materials and images,[55] that would probably be caught under the ambit of this rule. The circulation of such images have been consensual within the communities they are part of, and have allowed them to understand and diversify what comprises 'acceptable' sexual practices.[56]

Therefore, it is critical that the law avoids situations where the rule is abused by users to simply report *any* explicit imagery that offends their sensibilities, thereby leading to coordinated flagging and erasure of content belonging to marginalized and vulnerable communities.[57] Intermediaries should be obligated to act *only* when the complaint originates from the concerned individual, or someone *legally authorized* on their behalf.

Finally, it needs to be noted that even if this rule is tailored to narrow categories of content, it may still run contrary to the Supreme Court's judgment in *Shreya Singhal*, which read down 'actual knowledge' in Section 79 of the Act and the 2011 rules. Intermediaries are only legally obligated to act on a content takedown order if it comes from an authorized government agency or a court. The Court has diluted the dictum in *Shreya*

---

[54] B. Radha, 'Gendered discourse: Technology mediated violence and women students', *National Dialogue on Gender-base Cyber Violence*, <https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Dr_Radha.pdf>.
[55] Vex Ashley, 'Porn on Tumblr - a eulogy / love letter', *VexAshley.medium.com*, 6 December 2018, <https://vexashley.medium.com/porn-on-tumblr-a-eulogy-love-letter-6d45e70fefff>; Julia Fawal, 'Queer Women Used Tumblr to Explore Sexuality. Now It's Over', *Out*, 4 December 2018, <https://www.out.com/news-opinion/2018/12/04/queer-women-used-tumblr-explore-sexuality-now-its-over>.
[56]Elanor J. Broker, 'One Fewer Space for #GirlsLikeUs', *Slate*, 17 December 2018, <https://slate.com/human-interest/2018/12/tumblr-adult-content-ban-trans-women.html>; also see Lauren Strapagiel, 'Influencers Say Instagram Is Biased Against Plus-Size Bodies, And They May Be Right', *BuzzFeed News*, 21 May 2020, <https://www.buzzfeednews.com/article/laurenstrapagiel/influencers-say-instagram-is-more-likely-to-remove-photos>.
[57] *See* Gautam Bhatia, 'Offend Shock or Disturb: Free Speech Under the Indian Constitution', Oxford University Press (2016) and Abhinav Chandrachud, 'Republic of Rhetoric: Free Speech and the Constitution of India', Penguin Random House India (2017), which note that especially in the context of India, where the right to speech and expression is not just curtailed by the State, but also by actions of private, non-state actors, it is important for any law guaranteeing user safeguards to ensure that the same does not become a tool for wielding the 'heckler's veto'.

Singhal, mostly notably in content takedown orders related to intellectual property (repeatedly allowing takedown orders from affected parties whose intellectual property was allegedly infringed). However, such judgments (in the context of copyright, at least) were based on a reading of the Copyright Act with the IT Act. Clear judicial principles have not emerged for how exceptions will be made to the Supreme Court's judgment in *Shreya Singhal* with regard to content takedown notices from third parties.

Second interpretation: Intermediaries legally obligated to act on a wide range of grievances

Rule 3(2)(a) is the primary provision with regards to the exact nature of the grievance redressal mechanism an intermediary ought to adopt. However, it also provides us with a second indication for what the scope of the rule can be. Read in total, Rule 3(2)(a) empowers users to lodge complaints regarding violations of 'this rule', which presumably would be the entirety of Rule 3(2), as well as, *'any other matters pertaining to the computer resources made available by it . . .'* While the first part of the clause restricts the application of the rule to only matters indicated in Rule 3(2)(b), the second part seems to extend the scope to a broad variety of content. As per the operation of Rule 3(2)(a) therefore, there would continue to exist a host of ambiguous, undefined subject-matters beyond those identified by Rule 3(2)(b), for which users would be entitled to file complaints with the intermediary and expect prompt responses and removal.

As we have mentioned already, *Shreya Singhal v Union of India*[58] restricts the scope of intermediary obligations under section 79 by two ways: a) by emphasizing that for takedown orders to be legally actionable, they must come only from government agencies or the court, and b) these orders can *only* restrict themselves to subject matters within Article 19(2) of the Indian Constitution. Both of these obligations are reflected within Rule 3(1)(d), as discussed above. While the nature of the takedown notices within Rule 3(1)(d) and Rule 3(2)(a) would be fundamentally different, we are nevertheless concerned that the vague, open-ended nature of the latter, may open up the possibility for users to be able to send complaints that overlap with subject-areas that ought to be solely restricted to the government or the court.

Recommendation

1. Modify Rule 3(2)(b) to reflect that a SMI's obligation would be triggered *only* when the individual themself or *a person legally authorized on their behalf*, notifies the SMI regarding the removal of their private/morphed materials.
2. Modify Rule 3(2)(a) to exclude the phrase '*any other matters pertaining to the computer resources made available by it . . .*' since it clouds the grievance redressal mechanism in broad ambiguity.

Rule 4(a), (b) and (c): Personnel localisation

This sub-rules require a SSMI to appoint certain personnel residing in India:

[58] Shreya Singhal Case.

- A **Chief Compliance Officer** will be responsible for ensuring compliance with the Rules. This person can become criminally liable for third-party information hosted by the intermediary in case the intermediary does not comply with the Rules.
- A **nodal contact person** will coordinate with law enforcement agencies.
- A **Resident Grievance Officer** will manage grievances and complaints received from users under Rule 3(2).

The regulatory concerns of this rule become more apparent when seen in the context of the government's powers of censorship and surveillance under the IT Act or otherwise.

Section 69A of the IT Act, for instance, has been abused by the Central Government to order intermediaries to take down swathes of content, even if it may be constitutionally-protected expression.[59] When intermediaries are of the opinion that the order they have received does not follow domestic law or is overbroad, they may contest these orders or work with the government to make them narrower before they implement it.[60] Note that the opportunity of a hearing to the originator and intermediary are elements of the blocking procedure under the provision.[61]

Thus, facing reprise in the form of the arrest of an employee, intermediaries will now be more likely to act on overbroad content takedown and surveillance orders, creating the possibility of illegitimate infringement of users' rights to freedom of expression and privacy.[62] The rule will thus also undermine companies' commitments to human rights.[63]

In the context of requests of information about users sent to intermediaries, the rule may also have the effect of undermining mutual legal assistance treaties (MLATs) that the Government of India is party to. When the information requested by the government agencies is not stored in India, such a request will go through specific MLAT procedures. However, with a tight timeline of responding to requests set by the rules and the fear of arrest of employees, intermediaries will be required to provide access to data (stored in servers outside India's jurisdiction) without the government having to participate in the MLAT procedure. This creates regulatory uncertainty where a set of municipal regulations

---

[59] Torsha Sarkar and Gurshabad Grover, 'How India is using its Information Technology Act to Arbitrarily Take Down Online Content', *Scroll*, 15 February 2020, <https://scroll.in/article/953146/how-india-is-using-its-information-technology-act-to-arbitrarily-take-down-online-content>.

[60] For example, see Lauren Frayer and Shannon Bond, ' Twitter In Standoff With India's Government Over Free Speech And Local Law', *NPR*, 18 February 2021, <https://www.npr.org/2021/02/17/968641246/twitter-in-standoff-with-indias-government-over-free-speech-and-local-law>.

[61] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 18, <https://cis-india.org/internet-governance/resources/information-technology-procedure-and-safeguards-for-blocking-for-access-of-information-by-public-rules-2009>.

[62] Vittoria Elliot, 'New laws requiring social media platforms to hire local staff could endanger employees', *Rest of World*, 14 May 2021, <https://restofworld.org/2021/social-media-laws-twitter-facebook/>.

[63] For one such articulation, *see* The GNI Principles on Freedom of Expression and Privacy (updated May 2017), <https://globalnetworkinitiative.org/gni-principles/>, which provide that "participating companies will respect and work to protect the freedom of expression of their users by seeking to avoid or minimize the impact of government restrictions on freedom of expression".

that intermediaries are subject to in India requires one thing, while a binding legal regulation such as a treaty that India is a party to may require another.

Rule 4(1)(d): Periodic compliance reports

SSMIs under Rule 4(1)(d) are obligated to publish "*periodic compliance reports*" every month that would detail, among other things, information regarding complaints received and action taken, and the number of specific links or parts of information removed by the entity in pursuance of any proactive automated tools deployed. The rule also makes it possible for the government to specify further details about these reports in the future.

The nature of information stipulated to be provided within these compliance reports, overlaps with the kind of information several intermediaries already provide voluntarily by way of 'transparency reports'. Google, for instance, provides information about "*data on content removal requests.*"[64] Similar efforts exist on part of Facebook[65] and Twitter[66] as well. Transparency reporting serves as an important tool in understanding the breadth of censorship carried out either by the government, or the platforms themselves, and in light of that, are an important component in the overall understanding of online content moderation.

Publication of more data around the use of such tools therefore, is also vital for understanding their efficacy and the role they play in regulating speech online. In light of this, it is commendable that the rules attempt to legitimize some of these voluntary production of data. This is even more important, because previous studies have revealed that there is a disparate gap between the kind of information several US-based intermediaries provide for their US users, and their Indian users.[67] Finally, the obligation under this rule is in-line with international best practices of content moderation, including the Santa Clara Principles on Transparency and Accountability and in Content Moderation,[68] which were adopted in 2018 and endorsed by more than seventy human rights groups.[69]

On the other hand, some of the finer details of this particular obligation require careful consideration. *Firstly*, the period of publishing these reports is currently stipulated to be monthly. Consider the following contrast: NetzDG's transparency obligations, require the relevant entities to make this information available six-monthly[70]; for intermediaries

---

[64] Google Transparency Report, <https://transparencyreport.google.com/?hl=en>.
[65] Facebook Transparency Reports, <https://transparency.fb.com/data/>.
[66] Twitter Transparency Center, <https://transparency.twitter.com/>.
[67] Torsha Sarkar, Suhan S and Gurshabad Grover, 'Through the Looking Glass: Analysing Transparency Reports', *The Centre for Internet and Society*, 30 October 2019, <https://cis-india.org/internet-governance/blog/torsha-sarkar-suhan-s-and-gurshabad-grover-october-30-2019-through-the-looking-glass>.
[68] The Santa Clara Principles on Transparency and Accountability in COntent Moderation, 2018, <https://santaclaraprinciples.org/> ('Santa Clara Principles').
[69] Article 19, Electronic Frontier Foundation, et al, 'An Open Letter to Mark Zuckerberg - The World's Freedom of Expression is in Your Hands', *Santa Clara Principles*, <https://santaclaraprinciples.org/open-letter/> ('Santa Clara Principles, Open Letter').
[70] NetzDG, Section 2.

adhering to the voluntary Code of Conduct on Countering Illegal Hate Speech Online, the monitoring period is yearly[71]. Most voluntary initiatives taken by intermediaries currently also produce this information on a six-monthly basis. In light of this, we are concerned that a much shorter time-frame of reporting, as stipulated by these rules may prove to be onerous and considerably raise the costs of compliance.

Given that Rule 6 empowers the government to compel other intermediaries that are not SSMIs, to comply with the conditions of Rule 4, such an onerous and strict period of compliance might still stand to disproportionately impact smaller intermediaries[72].

Secondly, while the rule states that SSMIs ought to provide details of 'complaints received', it does not clarify any further details of these complaints. Apart from removals pursuant to legal takedown orders (i.e., from governments and courts), intermediaries would remove content either: a) pursuant to complaints received users under Rule 3(2), or b) on a voluntary basis, as envisaged in *Proviso* to Rule 3(1)(d). Apart from this, a substantial number of intermediaries would also allow users to lodge report content found 'objectionable' under their own internal governance norms, termed as 'community standards'. Information around these complaints are also sometimes separately represented in the voluntary transparency report endeavours.

Recommendation

1. Reconsider the monthly period for filing compliance reports, and update it with inputs from the concerned intermediaries and civil society organizations.
2. Secondly, in light of the existence of several different sorts of complaints an intermediary (and a SSMI) may receive in the course of its service, we recommend that the concerned rule should strive for more detail and nuance in describing the exact obligations for compliance.

Rule 4(2): Tracing 'first originator' of messages[73]

This rule is applicable to SSMIs that primarily provide *messaging* services. Such a framing ostensibly targets popular instant messaging applications, such as WhatsApp and Telegram, but can also be construed to include all social media platforms that provide 'direct messaging' capabilities to their users (and possibly even email service providers).

It requires providers of these services to 'identify' the 'first originator' of the messages that traverse their platforms in response to a legal order.[74] The rule goes on to clarify that

---

[71] European Commission, 'The EU Code of Conduct on Countering Illegal Hate Speech Online, <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en>.

[72] See Nadika N., 'IT Rules 2021 Intermediary Guidelines: Concerns and recommendations from the community', *Has Geek*, 25 May 2021, <https://hasgeek.com/PrivacyMode/it-rules-il-guidelines-2021/sub/it-rules-2021-intermediary-guidelines-concerns-and-7swxnPZrCPooIUdLPPqz2u> ('Nadika N., IT Rules 2021 Recommendations').

[73] This section is a summary of a forthcoming paper by CIS.

[74] A legal order here is one that "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

SSMIs shall not be "required to disclose the contents of any electronic message", which suggests that it only applies in cases where law enforcement has gained access to the contents of an encrypted message through other means, such as gaining access to one of the devices sending or receiving a particular message, and only wants to identify the 'first originator' of a forwarded message. Here, the first originator is presumably the very first individual to introduce a message to the platform in question. However, there is also the possibility of multiple individuals independently sending the same message, leading to multiple, disparate forward chains of the same message. We refer to the very first individual to send the message as the "absolute originator" and any other senders as "relative originators".[75]

Many messaging service providers use an encryption mechanism known as 'end-to-end encryption', which precludes even service providers themselves from seeing the contents of a message. Since most messaging services of this nature do not currently have capabilities to identify the first originator, multiple technical methods have been proposed to implement this rule. These are described below along with the side-effects they have on the security and privacy of online communications.

- **Storing 'hashes' of all messages**: Government officials have suggested[76] that messaging applications could compute the 'hash' of messages prior to encryption, and service providers could store all 'hashes' along with information identifying the author. Hashing is a mathematical operation that converts any piece of information into a short, unique string of characters (a 'fingerprint', of sorts). It is a one-way operation, meaning that recovering the original text from its hash is generally considered computationally infeasible. Upon receiving a legal order, a service provider could compute the hash of the message in question and compare it to all the hashes in its database, allowing for the identification of all relative and absolute originators of a message.

  This method has serious adverse effects on the security of online communications. Hashing is not equivalent to encryption, and retaining hashes of private, confidential messages opens them up to scrutiny by messaging service providers or bad actors capable of breaching the infrastructure of the service providers. This is possible through what is known as a 'dictionary attack' — computers today are capable of calculating trillions of hashes per second, this capability can be used to find hashes of combinations of commonly used words and phrases, which can be compared with the hashes that messaging service providers retain to guess the contents of many messages from their hash.

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".

[75] This terminology was used by a participant in a discussion on the IL Rules 2021 organised by the Center for Democracy and Technology (CDT). The discussion was held on 3 March 2021 under the Chatham House Rule.

[76] Deeksha Bhardwaj, 'Hash constant: Govt's solution to tracing originator of viral messages', *Hindustan Times*, 2 March 2021, <https://www.hindustantimes.com/india-news/hash-constant-govt-s-solution-to-tracing-originator-of-viral-messages-101614667706841.html>.

It creates new avenues for mass surveillance, profiling and censorship by allowing for the identification of everyone who shared a particular message or preventing messages corresponding to a particular hash from being delivered.

This method is also easily circumvented. Since the service provider only sees the hash of a message and not its contents, it has no way of verifying that the end-user device is sending it the correct hash.

- **Attaching originator information to messages**: A submission to the Madras High Court, suggested a method to achieve 'traceability': attaching identifying information about the originator to each message.[77] This can either be made visible to each recipient of the message, or be encrypted in a way that allows only the messaging service provider to see the originator information. While this method can be implemented in a way as to not strictly violate the confidentiality of messages, attaching additional metadata to online communications and allowing third parties such as the message recipients or the service provider (depending on the variant chosen) to view originator information will seriously weaken communication privacy. This method also may not satisfy the requirements of the rule as it can only trace a single relative originator and not the absolute originator.

This rule may also discourage the adoption of strong end-to-end encryption mechanisms entirely.

Additionally, all of these technical proposals pose certain practical limitations:

- **Poor identification**: Online messaging services rely on weak identification mechanisms to identify their users. This can be a phone number, email address, or other device identifier, all of which can be forged, stolen, or registered anonymously.[78]

- **Poor attribution**: A message's true author may not correspond to the first originator. Individuals often paste or share content from elsewhere.[79] Experts have also suggested that a traceability mandate may spawn commercial services located offshore to aid the spread of messages while being shielded from liability.[80]

- **Geographic spillover of effects**: The rule also states that if an originator is located outside of India, the first recipient inside India must be tagged as the first

---

[77] Aditi Agrawal and Nikhil Pahwa, 'IIT Madras's Kamakoti tells MediaNama how WhatsApp traceability is possible without undermining end-to-end encryption', *Medianama*, 8 August 2019, <https://www.medianama.com/2019/08/223-kamakoti-medianama-whatsapp-traceability-interview/>.
[78] Antony Clement Rubin & Anr. v. Union of India, WP No. 20744 & 20214 of 2019, Madras High Court, Submission of Intervenor, <https://www.medianama.com/wp-content/uploads/Typed-Set-Volume-II-filed-by-Intervenor-.pdf> ('Antony Clement Rubin Case, Submission of Intervenor').
[79] Aditi Agarwal, 'Exclusive: WhatsApp's response to Dr Kamakoti's submission', *Medianama*, 21 August 2019, <https://www.medianama.com/2019/08/223-exclusive-whatsapps-response-kamakotis-submission/> (Mediamana, Whatsapp's Response').
[80] Antony Clement Rubin Case, Submission of Intervenor

originator. To implement this, service providers would need to guess an individual's location which, if misidentified, could make them susceptible to lawsuits.[81]

Irrespective of the technical implementation chosen, allowing for the tracing of online communications is a violation of the fundamental right to privacy. Applying the framework by Bhandari, et al[82] that condenses the Supreme Court's judgments on the right to privacy, we examine the suitability and necessity of this rule with respect to the purpose it aims to serve, and balancing of the right and the need to interfere thereinto.

- **Legality**: As already noted, nothing in sections 69A and 79 envisions a state power to infringe upon privacy in the rules notified under these provisions. Even the IT Act as a whole does not empower the Government to mandate technical changes to platforms.

- **Necessity and Suitability:** Traceability is only necessary when a message goes viral i.e. it has been forwarded too many times for existing metadata-based investigations to be viable. In this case it ignores distributors, and aims to prosecute creators. Considering the ease with which all traceability proposals can be circumvented by motivated individuals, how poorly they identify the actual creators of content, and the limited scenarios in which it may be potentially useful, serious doubt is cast on the suitability.

- **Balancing**: Compromising privacy[83] (and consequently freedom of expression and freedom of assembly) of many in an attempt to catch a few bad individuals who can circumvent the technical measures enacted to catch them. Efforts from global experts to apply the principles of necessity and proportionality identified as a clear principle that governments "should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes."[84] Traceability runs squarely opposite to this proposition.

Under the IT Act, the Government does not have the legal power to mandate traceability. Additionally, the rule is unconstitutional: it moves companies from privacy-respecting

---

[81] Antony Clement Rubin Case, Submission of Intervenor; Medianama, Whatsapp's Response.
[82] Vrinda Bhandari and Karan Lahiri, 'The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World', 3(2) U OxHRH J 15 (2020). <http://ohrh.law.ox.ac.uk/wordpress/wp-content/uploads/2020/05/U-of-OxHRH-J-The-Surveillance-State-Privacy-and-Criminal-Investigation-1.pdf>.
[83] Nadika N., IT Rules 2021 Recommendations.
[84] The Principles: Necessary and Proportionate on the Application of Human Rights to Communication Surveillance (2014), ,https://necessaryandproportionate.org/principles/>.

technologies, goes contrary to data minimisation principles,[85] and undermines privacy for all while being easily circumventable by motivated actors.[86]

Rule 4(3): Promotional and licensed content

Rule 4(3) is applicable to SSMIs who, on behalf of another person, provides any service with respect to any information:

- either for direct financial benefit to increase either the visibility of the information, or to target the receiver of the information, or
- to which the SSMI holds a copyright or any sort of exclusive licenses.

In essence, the first prong of Rule 4(3) regulates advertisements, including targeted advertisements, while the second prong regulates content on the SSMI's platform to which it holds a license. Under this rule, these SSMIs are obligated to clearly identify such information, either as being advertised, marketed or sponsored, or any other identification as may be applicable.

Rule 4(4): Technology-based measures for content filtering

As per Rule 4(4), SSMIs are expected to 'endeavour' to "*deploy technology-based measures, including automated tools or other mechanisms*" to proactively detect information depicting rape, child sexual abuse material (CSAM), or content that is duplicate to information removed earlier by a takedown notice issued under Rule 3(1)(d). Additionally, the SSMI would be obligated to display a notice to the users who attempt to access such disabled content. The rule contains three *provisos* outlining additional safeguards in the deployment of such technology-based measures, which we have discussed in more detail in the subsequent subsections.

It is interesting to note that a proto version of this rule existed in the 2018 draft amendments, which had been intended to be applied to all intermediaries. Additionally, the nature of the obligation had been mandatory, as opposed to the current best-efforts version, and the scope of the content that ought to be filtered was also extended to all 'unlawful' materials. In light of this, it is perhaps an improvement that the current version of the rules curtail the scope significantly to content that is either: a) CSAM or material depicting sexual violence, or b) duplicate to content disabled pursued to a legal takedown order under Rule 3(1)(d).

---

[85] *See also* Katitza Rodriguez, 'Why Indian Courts Should Reject Traceability Obligations', *Electronic Frontier Foundation*, 2 June 2021, <https://www.eff.org/deeplinks/2021/06/why-indian-courts-should-reject-traceability-obligations; https://exmachina.substack.com/p/traceability-is-antithetical-to-liberty>.

[86] See also Vasudev Devadasan, 'Intermediary Guidelines and the Digital Public Sphere: Tracing First Originators', *IndConLawPhil*, 10 April 2021, <https://indconlawphil.wordpress.com/2021/04/10/intermediary-guidelines-and-the-digital-public-sphere-tracing-first-originators/>.

CSAM and material depicting sexual violence

There seems to be some consensus that certain forms of automated technologies like fingerprinting and hash-matching may be able to successfully detect and remove CSAM.[87] This may be because of the existence of a large amount of corpora with which these tools can be trained.[88] This logic can also be extended to the policing of content depicting sexual violence, since scholars have opined that certain forms of technology-based measures can be utilized to filter out content "*that is predetermined to be unlawful.*"[89]

On the other hand, we must emphasize that any endeavour to filter, monitor and block such content should not be completely delegated to private entities like SSMIs, nor should such operations be continued without due oversight. Content recognition technologies, like the measures envisaged under this provision, have been used historically to detect and report CSAM, including by the NCMEC, an US-based organization working on these causes. However, as studies show, the endeavour to deploy technology-based measures must be done in consonance with relevant law enforcement authorities, and organizations working to eradicate child exploitation.[90]

Finally, in 2011, the Special Rapporteur to the Human Rights Council, UN General Assembly, had noted that while utilization of blocking and filtering technology for detection of CSAM may be justifiable, the law making provisions for the same must be precise, and there should be sufficient safeguards, including oversight from an independent and impartial regulatory body.[91]

Safeguards and oversight

The aforementioned three *provisos* to the rule further delineate safeguards that the SSMI would be expected to adopt, and includes: a) ensuring that the measures adopted are proportionate to the interests of free speech and privacy of the users, b) implementation of proper human oversight, including a periodic review of such automated tools, and c) ensuring that such review looks into the accuracy and fairness of such tools, the propensity of bias and discrimination in these tools, and the impact on their privacy and security. However we do note that the first *proviso* to the rule, regarding ensuring that the tools operate proportionately to user safeguards, is couched in broad terms. As an

---

[87] Spandana Singh, 'Everything in Moderation An Analysis of How Internet Platforms Are Using Artificial Intelligence to Moderate User Generated Content', *New America*, 15 July 2019, https://www.newamerica.org/oti/reports/everything-moderation-analysis-how-internet-platforms-are-using-artificial-intelligence-moderate-user-generated-content/the-limitations-of-automated-tools-in-content-moderation> (New America, Content Moderation'); Cambridge Consultants, 'Use of AI in Online Content Moderation', *Ofcom UK* (2019), <https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf>.

[88] New America, Content Moderation.

[89] Hannah Bloch-Wehba, 'Automation in Moderation', 53 CORNELL INT'L L. J. 42 (2021), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3521619>.

[90] *See* Melissa Strobel and Stacy Jeleniewski, 'Global Research Project: A Global Landscape of Hotlines Combating Child Sexual Abuse Material on the Internet and an Assessment of Shared Challenges', *National Centre for Missing and Exploited Children* (2015), <https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/grp.pdf>.

[91] Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue', Doc. A/HRC/17/27, 16 May 2011, <https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>.

operational safeguard therefore, it might not amount to a functional test or benchmark for automated tools. Additionally, we note that these *provisos* do not make any provision for an aggrieved user to challenge removals via technology-based measures[92]. While the third *proviso* makes a reference to the need for assessing the accuracy of the tools deployed by the concerned SSMIs, this does not directly translate into a need for the SSMI to actually rectify erroneous removals real-time.

Recommendation

1. While the utilization of technology-based measures for the blocking and removal of CSAM and material depicting sexual violence can be a justifiable aim, the task must not be completely delegated to the SSMIs. Instead, the obligation in question should also be to ensure continuous, robust collaboration and knowledge-sharing between the technology industry and organizations working with child rights.

2. The *provisos* must be broken down further to achievable and clear goals in terms of ensuring user rights vis-a-vis the use of automated tools. This may include giving users a right to challenge erroneous removals by use of these tools, asking SSMIs to clearly document the technical nature of the tools being used, and the potential violation of rights that may arise out of the same. Additionally, while the mandated periodic review is a welcome step, we emphasise that the results of these review processes must be made public, to ensure better understanding of these technology-based measures.

Rule 4(7): Voluntary verification of accounts

This sub-rule mandates significant social media intermediaries to offer users a way to verify their accounts (using "appropriate" mechanisms, including the active Indian mobile number of such a user). The Rules do not specify any mechanism to determine the appropriate method for intermediaries to verify the users and concerns have been raised that this may dilute the voluntary nature of identification.

Such an obligation on the social media intermediaries has also been proposed under the Personal Data Protection Bill. The Bill prescribes that every social media intermediary which is recognised as a 'significant data fiduciary under the PDP Bill has an obligation to ensure that users are able to voluntarily identify their account.[93] Provisions regarding social media intermediaries and their verification are not within the ambit of a personal data protection bill, or under the intermediary guidelines.

---

[92] *See* Irene Khan, Clement Nyaletsossi Voule and Joseph Cannataci, 'Letter: Mandates of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; The Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association and the Special Rapporteur on the Right to Privacy', Doc. OL IND 8/2021, 11 June 2021, <https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26385>.
[93] PDP Bill, Section 28(2).

The rule obligates social media intermediaries to collect more data than is required, thus violating the principle of data minimisation.[94]

Recommendation

Delete 4(7).

Rule 4(8): Accountability practices

Rule 4(8) obligates SSMIs to ensure accountability to users, prior to removing their content, either under Rule 3(1)(b), or of the SSMI's own accord. Rules 4(8)(a) and (b) state before removing an user's content on the aforementioned grounds, the SSMI would be required to provide the user with a) a notification explaining the action being taken and the reasons for taking such action, b) an '*adequate and reasonable*' opportunity to dispute the action and request for the reinstatement of the content. Further, Rule 4(8) requires the SSMI to ensure that their Resident Grievance Officer maintains due oversight over any disputes raised by the user.

Both the requirements for providing the user with a notice and an opportunity to appeal a content removal action, are in-line with international best practices of content moderation, including the Santa Clara Principles on Transparency and Accountability and in Content Moderation,[95] which were adopted in 2018 and endorsed by more than seventy human rights groups.[96] In light of this, it is commendable that the IT Rules formalize this requirement within the law. We further note that the Santa Clara Principles underwent a period of industry-wide and public consultation in 2020, with an aim to understand and update the principles in light of the changing nature of content moderation landscape. Similar sunset clauses should exist within the current law as well, to ensure that the obligations does not become outdated, or unduly onerous on the SSMIs.

Rule 6: 'other intermediary'

The rule allows the Government, through notification, to mandate any intermediary to follow the conditions set out in Rule 4 (i.e. for SSMIs) even if they do not meet the criteria for SSMIs. The government shall base such decisions on whether the intermediary's service "create[s] a material risk of harm to the sovereignty and integrity of India, security of the State, friendly relations with foreign States or public order." [97]

There are several concerns with this rule. *First*, this will allow the Government to mandate intermediaries to follow onerous obligations listed out for SSMIs even if the intermediary in question is not a social media intermediary. As noted earlier, the definition of intermediary under the IT Act is broad and includes internet service providers, network

[94] Tanaya Rajwade and Gurshabad Grover, 'India's Privacy Bill Will Alter How it Regulates Social Media Platforms, Not all of it Good', *The Wire*, 17 February 2020, <https://thewire.in/tech/indias-privacy-bill-regulates-social-media-platforms>.

[95] Santa Clara Principles.

[96] Santa Clara Principles, Open Letter.

[97] IL Rules 2021, Rule 6.

backbones, etc.: it would be technically impossible for these intermediaries to comply with the obligations in Rule 4.

Second, the grounds under which the Government may use its power are excessive and broad. Such powers could be a case of excessive delegation to the executive, possibly having an arbitrary impact on intermediaries in India, who may be called to comply with onerous requirements at the government's will. This concentration of power in the hands of the government should be viewed in conjunction with the fact that the power can be abused to target intermediaries which do not have a large user-base, but may be focused on dissenting speech. The government can thus arbitrarily increase their operational costs.

Recommendation

Delete Rule 6.

Rule 8: Administration of Part III

Rule 8 states that the provisions relating to publishers of OCC and news would be administered by the I&B Ministry. It is a matter of customary practice[98] that one Ministry or Department administers an Act, which implies only a particular Ministry or Department may notify rules using the provisions of a particular Act[99], under which the concerned Ministry or Department may issue orders or directions. Therefore, this creates an administrative incongruity, since the I&B Ministry is administering part III of the rules, while part II of the rules is being administered by MeitY.

As we have argued earlier, regulation of 'Digital Media' is not within the scope of the MeitY (as it had conceded that 'Digital media' is the subject matter of the I&B Ministry). Further, the I&B Ministry, for reasons mentioned above, cannot regulate the subject within the current framework of the rules. Accordingly, the administration of the provisions regarding 'digital media' falls beyond the ambit of either of the Ministries mentioned within the rules.

Recommendation

Part III should be deleted *in toto*.

---

[98] *See* Business Rules; It is a matter of customary practice unless it is expressly mentioned. *See for example*, entry 9 of Department of Revenue (Ministry of Finance) i.e 'Administration of the Narcotic Drugs and Psychotropic Substances Act, 1985'. While entry 54 of Department of Internal Security (Ministry of Home Affairs) i.e 'All matters relating to Narcotics Control Bureau set up under the provisions of Section 4(3) of the Narcotic Drugs and Psychotropic Substances Act, 1985' has been explicitly handed over to Department of Internal Security, Ministry of Home Affairs.

[99] Business Rules.