Response to the Draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018

30 January 2019

B6-1, First Floor, DDA Commercial Complex, Safdarjung Enclave, New Delhi, 110029
contact@esyacentre.org | www.esyacentre.org

Response to the Draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018

We at the Esya Centre, greatly appreciate the opportunity given to us by the Ministry of Electronics and Information Technology (MeitY) to respond to the draft 'Information Technology [Intermediary Guidelines (Amendment) Rules], 2018' ("**Draft Rules**"), which seek to replace the rules notified in 2011. We appreciate that MeitY has undertaken to reform and clarify issues on Internet governance through these rules.

However, after a thorough analysis of these rules, we believe a more holistic understanding of evolving technologies, and global trends in Internet governance may be instructive for MeitY to take this discussion forward. As such, we have approached this analysis from a broad, techno-legal perspective, highlighting the major thematic areas under each proposed rule, rooting our arguments in broader discourses on internet governance and the attendant rights and obligations of stakeholders.

Therefore, **Part I** of this response will provide a brief snapshot of some of the proposed Rules, and how they can be revised to comply with prior legislative jurisprudence, and best practices. **Part II** will delve into a more detailed discussion on the broader principles of regulatory governance. We hope that these thematic discussions will prove instructive in a larger discourse about the growing Internet ecosystem in India.

Part I

Comments on the Draft Rules

Draft Rules	Text of the Draft Rule	Comments
1	**Short Title and Commencement** – (1) These rules may be called the Information Technology Intermediaries Guidelines (Amendment) Rules, 2018. (2) They shall come into force on the date of their publication in the Official Gazette.	Although the Draft Rules intuitively fall under section 79 of the Information Technology Act, 2000 (IT Act), this is not currently specified. It may be useful to clearly state the principal provision under the IT Act to avoid future challenges on this basis.
2(k)	"Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;	An intermediary, as defined in the IT Act includes a vast array of service providers, ranging from internet service providers to cyber cafés. Given the various types of intermediaries involved and the evolving nature and functions of different classes of intermediaries, it is important that regulations applicable to them are graduated and differentiated.
3(2) and 3(8)	**Rule 3(2)**: Rules and regulations, privacy policy and user agreement to be published by the intermediary to not allow for certain information. **Rule 3(8)**: (8) The intermediary upon receiving actual knowledge in the form of a court order, or on being notified by the appropriate Government or its agency under	From a plain reading of the provisions, there appears to be an inconsistency between the list of objectionable and unlawful information mentioned under Rule 3(2), and unlawful acts mentioned under Rule 3(8). It may be helpful to either provide clarity on the distinction maintained for what is unlawful under the two provisions, or to harmonize the two. This will also help in better compliance of the provisions by intermediaries and users.

	section 79(3)(b) of Act shall remove or disable access to that unlawful acts relatable to Article 19(2) of the Constitution of India such as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner, as far as possible immediately, but in no case later than twenty-four hours in accordance with sub-rule (6) of Rule 3. Further the intermediary shall preserve such information and associated records for at least ninety days one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by government agencies who are lawfully authorised.	
3(4)	The intermediary shall inform its users at least once every month, that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.	The requirement to inform users "at least once every month" is a welcome step towards appraising users of the content take down and termination of access policies. This can be supplemented by providing useful context to users about the nuances of a company's privacy policy, rules and regulations, and user agreements. One way of doing this is to provide details to users every time there is a change in the user agreements, or privacy policy, or the laws, in a clear and succinct manner, giving users greater autonomy over their choices on the internet.

3(5)	When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorised.	This Rule could have significant implications on the users' right to freedom of expression, and potentially requires intermediaries to intervene and break encryption on secure communication platforms. It also does not lay down qualifications for the use of these powers by the State, violating the users' right to privacy, which was held to be Constitutionally protected in the *Puttaswamy* judgment[1]. There are problems with the construction of the provision as well. When unqualified access to all data is being requested by the State, the language of the provision should be restrictive, rather than illustrative. This is evidenced by the phrase "*...and matters connected with or incidental thereto*". Therefore, a creative rather than restrictive reading would allow unfettered access of data to the State, without having to define narrowly the reach of this Rule.
3(7)	The intermediary who has more than fifty lakh users in India or is in the list of intermediaries specifically notified by the government of India shall: (i) be a company incorporated under the Companies Act, 1956 or the Companies Act, 2013; (ii) have a permanent registered office in India with physical address; and (iii) Appoint in India, a nodal person of contact and	The rule applies to intermediaries with 50 lakh users, a number that represents 1.43% of India's Internet user base. There is no clear justification as to how this number was arrived at, and whether it signifies active users, subscribers, etc[2]. Further, the aim of requiring certain intermediaries to be incorporated under the Companies Act, 2013, and to have a permanent physical office in India is unclear. If it is for law enforcement to have a point of contact for

[1] *K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1.
[2] Nikhil Pahwa, Medianama, 22 January, 2019, "A serious and open threat to Internet in India", available at https://www.medianama.com/2019/01/223-a-serious-and-imminent-threat-to-the-open-internet-in-india/.

	alternate senior designated functionary, for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders/requisitions made in accordance with provisions of law or rules.	communication or issuing directions, it could be accomplished by Rule 3(7)(iii). The proposed requirements in Rule 3(7)(i) and 3(7)(ii) would place entry barriers on smaller intermediaries, whether based in India or outside, who may not have the financial means to set up a physical company in India. There must also be clarity over the intent behind having a dedicated nodal person of contact, provided for in Rule 3(7)(iii). If the intent is to accrue liability to one person designated in India, that may still be difficult to implement. For example, there could be problems with extradition (as has been seen in previous instances of people fleeing the country to escape prosecution[3]), and it could also potentially sour relationships with intermediaries and foreign governments[4], who could have better served as mutual aides.
3(8) and 3(5)	*Provided above*	While Rule 3(8) specifies that court or governmental orders can require intermediaries to remove or disable access to content only if the content relates to the restrictions provided for in Article 19(2) of the Constitution (per *Shreya Singhal*[5]), Rule 3(5), which is much wider in scope and has potentially greater implications for free speech, does not contain any such restrictions. Further, the "information or assistance" requested from intermediaries in Rule 3(5) is wide enough to also potentially cover blocking or disabling access to content, and does not contain Article 19(2) restrictions, nor does it

[3] The New Indian Express, 31 July, 2018, "Vijay Mallya Extradition case: India has weak extradition treaties", available at http://www.newindianexpress.com/nation/2018/jul/31/vijay-mallya-extradition-case-india-has-weak-extradition-treaties-1851272.html.
[4] The Telegraph, 18 December, 2004, "US slips in word for web loss", available at https://www.telegraphindia.com/india/us-slips-in-word-for-web-boss/cid/690202.
[5] *Shreya Singhal v Union of India*, AIR 2015 SC 1523.

		provide for judicial oversight. It can therefore potentially be used to circumvent the restrictions placed in Rule 3(8).
3(9)	The Intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content.	This Rule applies to all intermediaries, homogenously, without taking into account their size, function etc. This means that even intermediaries like cyber cafes, and regional news websites, amongst others, would also need to deploy these mechanisms; who may not have the resources to comply with this requirement, and hence may need to shut down. Further, this rule effectively delegates censorship and content moderation to intermediaries, who are motivated by profit and not user rights. It also does not define what "unlawful information or content" is, and intermediaries are likely to err on the side of over-enforcement to absolve themselves of liability. It does not provide for a judicial determination of unlawful content, or for any appeal or redressal mechanism. It also does not account for the limitations of automated tools and machine learning technology, and would significantly impair users' right to freedom of expression.

Part II

Broad Principles of Internet Governance

Cyberspace is a complex ecosystem that has evolved to encompass the breadth of human activity within its fold, from commercial considerations, interpersonal matters, to issues of governance. However, along with a rise in prosperity the expansion of cyberspace has also birthed newer forms of malevolence. Resultantly, institutions are moving to regulate and monitor activity on cyberspace more closely, to insulate society from the broader harms presented by it, and to also ensure that the broader principles of democratic governance and constitutionality are observed when passing laws to regulate it. To this end, we analysed the Draft Rules, and gave specific comments in the previous Part (I), and in this Part (II), chart a principle-based underpinning to the governance processes will help evolve a more durable framework for Internet governance, and policy discussions. Thus, in the following section, we have delineated some of these principles, and highlighted how the Draft Rules may be harmonised with them.

However, before commencing a discussion on the Draft Rules, it must be noted that in this response, we largely understand intermediaries to mean 'Internet intermediaries', referring to a wide, diverse and rapidly evolving range of service providers that facilitate interactions on the Internet between natural and legal persons[6].

Principle 1 - Blurring distinctions between the 'State' and 'private parties': The State must ensure that the unfettered power to seek information, and actively monitor content online is qualified both for the State and the intermediaries

There is an increasing blurring of distinction between the State/Government, and private parties in the form of intermediaries, in the regulation of online content, given the data analytic capabilities of big intermediaries. In this regard, Draft Rules 3(5) and 3(9) demonstrate a shift of responsibility of Internet governance and monitoring, seemingly from the State to the intermediaries. Further, these Draft Rules grant both the State, and the intermediaries the unfettered power to seek out any information they want, which may lead to instances of automated or conscious profiling, and discrimination. The Draft Rules particularly fail to lay down qualifications for the use of this power by the State, leading to a violation of a person's right to privacy, a right now espoused and enshrined in judicial consciousness through the *Puttaswamy*[7] judgement, which established that privacy forms the constitutional core of human dignity and autonomy[8]. A key part of this right has been conceptualised to include not only the control of personal information, but also the right to inaccessibility, and the right to subjectively desired inaccessibility[9]. Therefore, in light of the *Puttaswamy* judgement, the legality of provisions

[6] For this understanding, we have referred to the Council of Europe's "Roles and Responsibilities of Internet Intermediaries", available at https://rm.coe.int/leaflet-internet-intermediaries-en/168089e572.
[7] *K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1.
[8] Bhandar and Sane, Socio Legal Review, Vol 14, "Protecting Citizens from the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018", pp. 147.
[9] C Hunt, (2011) 37:1 Queen's LJ, "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort", pp. 173.

allowing for active policing by the State, and the imposed obligations on intermediaries to do the same, is suspect. Looking to international treatments, the Council of Europe also recommends that State authorities should not directly or indirectly impose a general obligation on intermediaries to monitor content which they merely give access to, or which they transmit or store, be it by automated means or not, and also impose proportionate sanctions for failure to comply, to avoid restriction of lawful content, and a resultant chilling effect on the right to freedom of expression[10].

This issue of asymmetry of agency between citizens vis-a-vis the State and powerful intermediaries gains special importance in the absence of a comprehensive legislation on surveillance and privacy, the expansive mandate given to State authorities and law enforcement agencies operating through myriad laws and executive orders, and the express lack of judicial oversight in India.

Principle 2 - Upholding User rights: The State must ensure that any legislation or rules thereunder pertaining to cyberspace does not curtail user rights

a. *The Problems with Intermediary Oversight*[11]

We understand why MEITY is considering placing greater responsibility on intermediaries to regulate behaviour on their own platforms. Cyberspace may be too vast for State agencies, in their current form and capacities, to manage alone. This is a trend that is being followed globally. Illustratively, the United States (US) enacted two statutes in 2018 – the Allow States and Victims to Fight Online Sex Trafficking Act and the Stop Enabling Sex Traffickers Act (FOSTA-SESTA). FOSTA-SESTA was passed with the goal of mitigating sex trafficking online. These laws impose a limitation on the safe harbour provision in the US Telecommunications Act, 1996. Section 230 of the Communications Decency Act, which falls under the broader US Telecommunications Act holds that Internet intermediaries, like social media websites and internet service providers, cannot be held accountable for user-generated content posted on their platforms. FOSTA-SESTA carves out an exception to this protective rule, stating that Internet intermediaries would be held responsible if advertisements soliciting sex showed up on their websites.

The initial dearth of regulation on Internet intermediaries, coupled with the dotcom crash in the early 2000s, compelled these entities to develop business models that centred on the monetisation of user data. The data is collected largely through user engagement on the platform, and then sold to third parties who largely use it for advertisement purposes. Thus, the prime commercial motivation for intermediaries is to encourage the generation of as much user data as possible.

---

[10] Council of Europe, "Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries", pp. 1.3.5 -1.3.6

[11] As enunciated by one of the authors of this response in Meghna Bal, "Regulating Online Intermediaries: We Need to Start Focussing on User Rights," *Firstpost*, December 17, 2018, https://www.firstpost.com/tech/news-analysis/regulating-online-intermediaries-we-need-to-start-focusing-on-user-rights-5745201.html.

As the vulnerability of these datasets has become increasingly apparent, regulators have started issuing data protection norms to govern how they are collected and processed. These regulations directly curtail the ability of intermediaries to gather user data. The extent of the effect these regulations have on the value of an intermediary may be evinced by the enactment of the General Data Protection Rules (GDPR) in Europe and the subsequent drop in the market capitalisation of one Internet intermediary by USD 123 billion,[12] even though there are reports stating that the GDPR did not hold back the digital marketing tide[13]. Therefore, in times of great legislative changes, the impact on the market, and on the ability of intermediaries to cope with these changes will have to be considered by any prudent State. This may also be the reason why intermediaries are also driven to resist any legislative action that would oblige them to regulate user behaviour on their websites or hinder their ability to collect user information.

In the context of increased intermediary liability obligations, intermediaries may overzealously enforce legislative and policy mandates to avoid further regulation, sometimes to the detriment of user rights. These may include the constitutionally protected and internationally recognised rights[14] of users to freedom of expression, privacy, religious freedom, public participation, information, and assembly. Illustratively, FOSTA-SESTA's enactment prompted one prominent social media platform to amend its community guidelines to prohibit sexual solicitation of any kind. These guidelines go as far as forbidding implicit sexual solicitation through either suggestive comments or images. Justifiably, activists are concerned that these guidelines may lead to an inordinate level of censorship of speech online. It is therefore necessary for regulatory policies concerning intermediaries to be framed around principles of creating strong digital ecosystems of accountability, like encouraging more transparency in reporting on operations, to protect against potential harms.

b. Interplay with Shreya Singhal

The Draft Rules have significant implications for free speech, and run directly counter to the Supreme Court's directions in the *Shreya Singhal* case. The case dealt in part with the safe harbour provision available to intermediaries under the IT Act, which provides that intermediaries would lose their safe harbour protection under section 79 of the IT Act and be liable for content posted on their platforms, if they failed to act upon having actual knowledge of illegal content. In this respect, the Supreme Court read "actual knowledge" to mean a notice to Internet intermediaries in the form of a court order.[15] This meant that the courts, and not the intermediary, would have to subjectively determine what would constitute illegal content. However, the Draft Rules, through Rule 3(9), now effectively outsource the determination of what constitutes lawful speech

[12] Romain Dillet, "Facebook Officially Loses $123 Billion in Value," *Tech Crunch*, July 2018, https://techcrunch.com/2018/07/26/facebook-officially-loses-123-billion-in-value/.
[13] MediaPost, "GDPR did not hold back the digital marketing tide", available at https://www.mediapost.com/publications/article/331209/.
[14] United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, p.3; available at https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf
[15] *Shreya Singhal v Union of India*, AIR 2015 SC 1523, para 117.

to private companies, which is something that neither they, nor the State should do, without judicial oversight.

In this context, it is also important to note that the State can only restrict speech on the grounds specified in Article 19(2), and in a manner that is necessary and proportional to meet those grounds. In *Shreya Singhal,* the Supreme Court specified that "unlawful acts" in Section 79(3)(b) of the IT Act would have to conform to Article 19(2) restrictions.[16] Rule 3(9), which requires Internet intermediaries to proactively monitor their platforms for unlawful content, does not reflect this restriction.

c. The chilling effect on free speech

One of the primary issues with draft Rule 3(9), is the requirement to proactively identify and remove access to "unlawful information or content". This is problematic for a number of reasons. First, the rules do not define what would constitutes as "unlawful" information or content, leaving intermediaries with no guidelines to assess the standards they should use. This is compounded by the fact that it is often difficult to assess whether controversial content is constitutionally protected. For example, although various legislations broadly detail the types of expression that would attract criminal liability, accurately assessing whether a particular picture or statement, for example, intends to "outrage the religious feelings" or "insult the religious beliefs" of a class of persons[17] is not something private parties are equipped to do.

Therefore, in order to absolve themselves of liability, intermediaries are likely to over-censor content and err on the side of over-enforcement, and take down even legal but controversial content. This is something that has occurred before in the context of Internet intermediaries,[18] and would significantly chill free speech and reduce the quality of discourse around uncomfortable, but often necessary and important issues. Given the volume of data published online and the resources that Internet intermediaries would require to monitor all this data, this measure could vastly reduce the volume of information that is even available online, with a severe impact on the extent and diversity of online communication.

d. Ineffective redressal mechanisms

Globally, Internet intermediaries have been criticised for not being transparent about their processes, and for the lack of effective redressal mechanisms for appealing content takedowns[19]. Even if content is later reinstated, content removal and account suspensions during public protest or debate could significantly harm users' political rights, and impair discourse.

e. Larger social context

---

[16] *Shreya Singhal v Union of India*, AIR 2015 SC 1523, para 117.
[17] Section 295A, Indian Penal Code, 1860.
[18] Rishabh Dhara, Centre for Internet and Society, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet,* available at https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf
[19] United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, p.13; available at https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf

We appreciate that the Draft Rules are an attempt to reduce misinformation on online platforms. In this regard, it is also useful to remember that the provisions on safe harbour were meant to serve as an incentive for more responsible regulation of the Internet. However, we question whether there is any discernible benefit in the Draft Rules seeking to change this incentive based regulatory framework, by actively encouraging intermediaries to censure and surveil all content on the Internet. We argue that it may be essential to also assess whether increasing intermediary liability is the best, or even an effective way to address what are essentially human, social issues. Doing so would make sure that the regulations framed do not just serve to reactively address specific symptoms (which may change form and require further regulation), but serve to regulate the cause of such information online. The first step in this assessment would be to undertake in-depth and evidence-based research (based on previous instances of unrest) to ascertain the role that Internet intermediaries play in spreading misinformation, and the extent to which any censorship or content takedown methods were effective in achieving their aims.[20] Research suggests a correlation between online hate speech and anti-immigrant crime in Germany, but it is unclear whether the existing anti-immigrant sentiment drove online hate speech, rather than the converse.[21] Some Internet intermediaries have commissioned related studies,[22] and the State would be well placed to commission independent studies as well. In any case, an effective response to misinformation online would require the different stakeholders to proactively work together to develop and publicise ways to, for example, verify the truth of claims found on online platforms.

Principle 3 - Ensuring Transparency and Accountability: The State must ensure that legislation or rules thereunder pertaining to cyberspace upholds globally accepted principles of transparency and accountability for all relevant stakeholders

The value of transparency (both from intermediaries and the State) in safeguarding user rights and promoting accountability cannot be overstated. For the meaningful and effective exercise of free speech and information rights on digital media platforms, users must have a clear understanding of what kind of content they can and cannot post, and the reasons for and number of takedowns and account suspensions.

a. Intermediary Transparency

It is in the interest of all stakeholders for intermediary platforms to be transparent with policy-makers and users about the limits and abilities of technologies they deploy, with the help of specific case studies, to effectively demonstrate the extent of human intervention and judgment required in assessing controversial content online[23] (especially as it relates to issues of

[20] Anja Kovacs, *5 Ways in which the Indian Government can improve its responses to hate speech online,* available at https://internetdemocracy.in/2012/09/5-ways-to-improve-responses-to-hate/

[21] Karsten Müller and Carlo Schwarz, *Fanning the Flames of Hate: Social Media and Hate Crime,* available at https://dx.doi.org/10.2139/ssrn.3082972.

[22] Facebook Research, *Announcing the Whatsapp Social Science and Misinformation request for proposals*, available at https://research.fb.com/announcing-the-whatsapp-social-science-and-misinformation-request-for-proposals/.

[23] Anna Windemuth, Rachel Brown, Yuan Tian and Imogen Sealy, *Wikimedia panelists tackle the future of intermediary liability*, available at https://wikimediafoundation.org/2018/08/02/intermediary-liability-future-panel/.

misinformation and "fake news", where much of the content is highly localised and context-based), and the difficult choices they can be required to make.

Secondly, encouraging transparency by Internet intermediaries with respect to the volume and details of content takedowns (both pursuant to State requests and company terms of use), and the decision-making process relating to handling relevant content, would go a long way in providing clarity to users and policy-makers on the metrics used for content regulation on platforms,[24] and in promoting consistency and accountability. It would also contribute to the creation of a "case law" of sorts, which would enable stakeholders to understand how intermediaries interpret and implement their standards.[25] Since companies currently can face legal risks relating to transparency on this front, it might be useful to consider granting intermediaries a transparency safe-harbour, which would encourage them to provide more information and being transparent, without fearing legal liability; and also provide a basis for informed engagement between Internet intermediaries, policy-makers, civil society and users.[26]

b. State Transparency

Given the magnitude of user rights at stake and their importance in preserving our democratic institutions, it would be beneficial for the State to not think of regulation as a way of imposing liability on intermediaries, but to explore ways to enable the public to make meaningful choices about how to engage with online platforms.[27] Users can only make informed decisions on how best to engage on intermediary platforms if the relationship between the State and intermediaries is meaningfully transparent.[28]

The Draft Rules, and the IT Act in general, currently do not provide for this kind of transparency. For example, State agencies are not required to provide details regarding the volume and types of content sought to be taken down, methods of inter-operability between various ministries and departments, actions sought (for example, blocking, partial or full takedown of content), etc. Further, Internet intermediaries may sometimes also be restricted from making such information public as part of their transparency reports or otherwise.

---

[24] United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*; available at https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf.

[25] United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, p.19; available at https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf.

[26] Tiffany Li, Information Society Project, Yale Law School, *Beyond Intermediary Liability: The Future of Information Platforms*, available at https://law.yale.edu/system/files/area/center/isp/documents/beyond_intermediary_liability_-_workshop_report.pdf.

[27] United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*; available at https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf.

[28] United Nations Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,* pp.16, available at https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf.

Introducing a requirement to provide information regarding the interaction of the State with Internet intermediaries would go a long way in promoting accountability on both sides.

Principle 4 - Following Regulatory Best Practices: The State must ensure that globally accepted regulatory best practices are followed, to achieve optimal outcomes for internet governance

It is imperative for the State to frame stable and responsive regulations, taking into account evolving questions of the operation of technology, sharing and access, and the impact on the market. This is crucial in understanding the intersectionality of Internet governance, user rights, and interests of the State, and it will be meaningful to create a charter of regulatory principles, which can then find their place in any policy, or law that the State creates – both for public interest, and for creating a culture of accountability, as mentioned in the previous section. To do so effectively, the State must identify the specific issues it wants to regulate, provide cogent rationale for interventions, and the potential impact on people and businesses. Without a framework of predictable, responsive governance in India, there is a high probability of "global innovation arbitrage", with innovators, businesses, and eventually the market shifting to regulatory regimes that are more hospitable to entrepreneurial activity[29].

a. Moving towards non-deterministic governance

Global best practices reveal several ways in which technological regulations can be made responsive and reflexive. One such example is the use of regulatory sandboxes, which can provide innovators the space to evolve new technologies without the burden of complying with regulations, and allowing the regulator to, in turn, be responsive, and use evidence and outcome-based research to inform further regulation. This approach necessitates more collaborative law making with other associated regulatory and State agencies to craft harmonised laws, optimise regulatory capacity, and make laws forward looking. This will aid in identifying big technological and appropriate governance trends for the future, and their impacts on markets and people on markers such as productivity, demography, and ethnography. This is substantiated by research, which states that for emerging science and technology issues, a non-deterministic approach to governance works much better in accommodating the various uncertainties about the future[30]. It has also been noted that technologically neutral regulations can often be sub-optimal because of the problem of prediction, that is, laws may not be able to adequately regulate new technologies, unless such new technologies become known, or else, we risk referencing older technologies. Therefore, a combination of technology neutrality and specificity, may better serve policy goals by improving legal tailoring, reducing legal uncertainty, increasing statutory longevity, and promoting treating like technologies alike[31].

b. Encouraging self-governance and principle-based regulations

---

[29] Adam Thierer, The Technology Liberation Front, August 22, 2016, "Global Innovation Arbitrage: Driverless Cars Edition", available at https://techliberation.com/2016/08/22/global-innovation-arbitrage-driverless-cars-edition/.
[30] Kuhlmann, S., Research Policy, "The tentative governance of emerging science and technology—A conceptual introduction", pp. 2, available at https://doi.org/10.1016/j.respol.2019.01.006.
[31] Greenberg, Minnesota Law Review, 100:1495, "Rethinking Technology Neutrality", pp. 1498-1500, available at http://www.minnesotalawreview.org/wp-content/uploads/2016/04/Greenberg_ONLINEPDF.pdf.

This means that the State must also encourage the development of self-governance standards, and voluntary codes of conduct to pursue newer and evolving perspectives on looking at newer challenges. This must be aided by regulations that are simple, certain, and accompanied by safeguards, and Constitutional values and principles. Further, older regulations that do not meet these regulatory standards should be periodically reviewed for their adequacy[32]. For instance, in the EU, regulations have been prescribed to have sunset provisions with periodic review of old and obsolete laws[33].

Principle 5 - There must be graduated and differentiated regulations for different classes of intermediaries

We urge that regulations on intermediaries be graduated, and differentiated for different classes of intermediaries, considering their heterogeneity, with differences in size, function, and convergence of services. Regulations that attempt to attach liability to this vast group as a homogenous class, run into the dangers of crafting a disproportionate liability framework, with no distinctions being made on the basis of the roles of intermediaries as publishers, mass-media, gate-keepers who control access to information etc.; making the law rigid, and unresponsive to future technological changes.

This has also been recommended in Europe, where Member States have been told to consider this heterogeneity to prevent possible discriminatory effects[34]. They also recommend that apart from applying a graduated and differentiated approach, States must also determine appropriate levels of protection, as well as duties and responsibilities according to the particular role of the intermediary[35].

Principal 6 - Promoting good governance: There must be a shift from a culture of 'liability' to one of 'responsibility' for approaching questions of intermediary liability

There is significant global discourse on reviving the moral approaches to intermediary liability, with legal theory increasingly shifting from a framework of 'liability' to one of enhanced 'responsibilities' for Internet intermediaries[36]. This is primarily under the assumption that the role of intermediaries is largely increasing in scope, and the potential for elevating the wider informational environment and users' interactions is unprecedented. Therefore, increased public accountability and transparency may work far better in ushering good governance.

Further, several emerging economies such as Brazil are introducing civil liability exemptions for Internet access providers and other Internet providers. For hosting providers in particular, there are civil liabilities, except in cases of copyright infringement. In Europe, the European

[32] American Legislative Exchange Council, "Six Principles for Communication and Technology", available at https://www.alec.org/model-policy/six-principles-for-communications-and-technology/.
[33] European Parliament, EPRS, June 2018, "Review Clauses in EU Legislation", pp. 10, available at http://www.europarl.europa.eu/RegData/etudes/STUD/2018/621821/EPRS_STU(2018)621821_EN.pdf.
[34] Council of Europe, "Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries", pp. 1.1.5.
[35] Council of Europe, "Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media", pp. 7.
[36] G.F.Frosio, Ijlt Vol 13, "Internet Intermediary Liability: WILMap, Theory and Trends", pp. 25.

Commission, along with all major online hosting providers including Facebook, Twitter, YouTube and Microsoft, decided upon a code of conduct, including a series of commitments to combat the spread of illegal hate speech online in Europe[37]. In Argentina, in the *Rodriguez M. Belen v. Google*[38] case, the Supreme Court held that intermediaries such as Google did not have any active monitoring obligation that could be linked to liability. We argue that while content moderation may help both intermediaries and law enforcement to filter unlawful and harmful content more efficaciously, it can be done in a more transparent and collaborative manner in the absence of any strict liability framework, and with joint development of mutually beneficial codes of conduct and standards.

Principle 7 - Upholding legal certainty of encryption: There must be legal certainty of preserving encryption for upholding the right of privacy for users

In the absence of certainty in the State's strategy and direction, evidenced from the lack of a coherent national encryption policy, having provisions such as the draft Rule 5, makes it uncertain and suspicious for users whether encryption would be broken to enable access for the State, or if encryption can be retained in the process at all, and how. We urge that the Draft Rules accord legal certainty to secure and preserve encryption, without any arbitrary qualifications.

Principle 8 - Mandating due process and judicial review: There must be due process and judicial review for orders to assist authorities in accessing information or content on the Internet

It is instructive to note that several countries across the world have ensured that robust and due processes are maintained with respect to provisions regarding obligations on providers to assist authorities. For instance, in the UK, section 253 of the Investigatory Powers Act 2016, states that the Secretary of State may give a telecommunications service provider a 'technical capability notice'. Such a notice may impose on the provider any applicable obligations specified, and require them to take all steps specified in order to comply with those obligations. This however requires the fulfilment of three requirements - (i) the Secretary of State must believe that the provider in question has the *capability to assist*; (ii) the Secretary of State must consider that the conduct required by the notice is *proportionate* to what is sought to be achieved by that conduct; and (iii) the notice must be *approved by a Judicial Commissioner*, who while deciding whether or not to approve the notice, must consider whether the notice is *necessary and proportionate*.

In Europe, Convention 108 on data protection specifically recommends that any demand or request by State authorities addressed to internet intermediaries to access, collect or intercept personal data of their users, including for criminal justice purposes, or any other measure which interferes with the right to privacy, should be *prescribed by law*, *pursue legitimate aims*, and be used

[37] European Commission, Press Release, May 31, 2016, "European Commission and IT Companies announce Code of Conduct on illegal online hate speech", available at http://europa.eu/rapid/press-release_IP-16-1937_en.htm.
[38] WILMAP, M. Belen Rodriguez c/Google y Otro s/ daños y perjuicios, Corte Suprema [Supreme Court], Civil, R.522.XLIX, available at https://wilmap.law.stanford.edu/entries/m-belen-rodriguez-cgoogle-y-otro-s-danos-y-perjuicios.

only when it is *necessary and proportionate* in a democratic society[39]. There are clear standards, which state that securing the restriction of illegal content by States with intermediaries must always be along the principles of *legality, necessity and proportionality*. States are urged to consider the fact that automated means, which may be used to identify illegal content, *currently have a limited ability to assess context*[40].

It is not abundantly clear from Draft Rule 5, if such tests of judicial approval (even when the order is lawfully made by a State agency), or necessity and proportionality are strictly to be applied, since powers of decision-making rest solely with the State agency. Further, it is unclear as to what a lawful order is; with the term neither being defined in the principal Act, or the attendant Rules. This is reminiscent of Rule 3(7) of the Information Technology (Intermediaries Guidelines) Rules, 2011, wherein there was considerable confusion over the term "lawful order", being interchangeably used with the term "request in writing", which implied that a 'lawful order' could simply be a written letter or notice from authorized State agencies, which did not bear adequate force of law, or due process. As such, the process is inordinately simplified, and the lawful order in effect simply becomes a notification/executive order of the State.

In the interest of transparency and protection against abuse of power, it may also be beneficial for the State to make available to the public in a regular manner, comprehensive information on the number, nature and legal basis of content restrictions or disclosures of personal data that they have applied in a certain period, through requests addressed to intermediaries under this proposed rule. Therefore, we urge that due process requirements and effective remedies should be facilitated vis-à-vis both the State, and intermediaries for the entirety of the Draft Rules.

Principle 9 - Harmonising legislations: There must be clear intent for mandating onerous obligations on intermediaries, with attempts to harmonise legislations that specify different requirements for foreign companies carrying out business in India

With respect to foreign intermediaries that are operating in India, it is important to note that the Companies Act, 2013 does not impose the obligation of a foreign company to necessarily have a physical presence in India to conduct business. The Companies (Registration Offices and Fees) Rules, 2014 state explicitly that foreign companies carrying out business in India through an electronic mode may have their main servers located either in India, or abroad. A physical presence in India has till now, mostly been mandated for banks, but that has been with an express intent to counter money laundering concerns, and *benami* transactions[41], along with offering significant protections like that of deposit insurance.

This is also evidenced world-wide, where regulators impose such obligations primarily on cross-border financial intermediaries like banks, pension funds and mutual funds, for considerations of

[39] Council of Europe, European Treaty Series No 108, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", available at https://rm.coe.int/1680078b37.
[40] Council of Europe, "Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries", pp. 1.3.8.
[41] Reserve Bank of India, Extracts from FATF-IX Report, Annexure, Annexure II, available at https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=281.

investor protection, and efficient capital markets. The OECD guidance on regulating commerce intermediaries also notes that while the requirement for residency or physical presence may be reasonable for conventional commerce, it is questionable in the context of B2C[42] electronic commerce, because such a requirement could result in businesses either restricting their trade or inadvertently failing to comply[43]. Therefore, in the case of draft Rule 3(7), it is not clear as to what the larger goals sought to be achieved are, by mandating a physical presence, and how this provision will be harmonised with other extant legislations like the Companies Act.

Principle 10 - Understanding the economic impact of provisions: There must be reliance on data about the economic impact of removal of safe harbour provisions in India, to draft more responsive legislations

It has been documented that having less onerous, or at least differentiated compliance requirements would assist in helping start-ups, and increase the expected profit for successful start-up intermediaries by 5% in India[44]. Further, the economic impact of weakening safe harbour provisions for Internet intermediaries can be significant. For example, the impact of that on the US economy has been estimated to be elimination over 425,000 jobs, and a decrease of the US GDP by $44 billion annually[45]. No such study has been conducted in the context of India, and it would be instructive to have unambiguous data on the impact of these Draft Rules on the ecosystem, before notifying them.

Principle 11 - Resisting proactive monitoring of information and content through automated tools: There must be insistence on taking measured steps to regulate online information and content, to prevent against widespread censorship; and expensive requirements for smaller businesses.

Draft Rule (9) states that intermediaries, as a matter of obligation, have to "proactively" identify and remove, or disable access to unlawful information or content. The rule is similar in many ways to Article 13 of the proposed Directive for Copyright in the Digital Single Market Directive in the EU[46], which requires platforms to proactively work with rights holders to stop users uploading copyrighted content. This was criticised, for obligating these platforms to scan all data being uploaded to sites like YouTube and Facebook, with the possibility of this being used for widespread censorship, and also creating a huge burden for small platforms, both in terms of resources, and liability. As such, a number of the Internet's original architects and pioneers and their successors, including Wikipedia's founder, and the World Wide Web's inventor, expressed

---

[42] B2C means 'business to consumer', *please see* https://www.investopedia.com/terms/b/btoc.asp.
[43] OECD, "Facilitating Collection of Consumption Taxes on Business to Consumer Cross-Border E-Commerce Transactions", pp. 9, available at http://www.oecd.org/tax/consumption/34422641.pdf.
[44] Oxera, February 2015, "The economic impact of safe harbours on Internet intermediary start-ups", pp. 2, available at https://www.oxera.com/wp-content/uploads/2018/07/The-economic-impact-of-safe-harbours-on-Internet-intermediary-start-ups.pdf.pdf.
[45] Nera Economic Consulting, June 5, 2017, "Economic Value of Internet Intermediaries and the Role of Liability Protections", pp. 2, available at https://cdn1.internetassociation.org/wp-content/uploads/2017/06/Economic-Value-of-Internet-Intermediaries-the-Role-of-Liability-Protections.pdf.
[46] European Commission, COM(2016) 593 final, 2016/0280(COD), "Directive of the European Parliament and of the Council on Copyright in the Digital Single Market", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0593.

their dissent by stating that the proposed rule was an "*unprecedented step towards the transformation of the Internet from an open platform for sharing and innovation, into a tool for the automated surveillance and control of its users*"[47]. They further said that the cost of adopting necessary automatic filtering technologies would be expensive and burdensome, and yet those technologies have still not developed to a point where their reliability could be guaranteed.

Thus, we urge a re-think on the draft rule, because by obligating platforms to proactively scan information and content, the Rule not only impacts the business models of several small platforms, that would now have to invest in technologies to enable them to comply with this Rule, but also embed an automated infrastructure for monitoring and censorship deep into the networks of an intermediary will run contrary to the essential values on which the internet today functions for the users – freedom, and safety.

a. Understanding Algorithmic oversight and its discontents

Intermediaries are relying increasingly on algorithms to oversee the quotidian administration of their platforms. These algorithmic oversight mechanisms rely on the continual gathering and dissecting of vast amounts of current data to trigger automatic responses.[48] Algorithmic oversight systems present palpable advantages for regulating behaviour and ensuring desirable behavioural outcomes. However, there are some key issues with algorithmic oversight that make it an imperfect mechanism for the large-scale regulation and monitoring of human activity online.

i. *Algorithms are not immune to making errors* - Algorithms generally find it hard to interpret the contextual meanings of words.[49] The meaning of content is relative to the specific context it is placed in. A particular word may have several meanings, depending on the setting or even the language it has been spoken or written in. Therefore, algorithms may erroneously dub a statement as nefarious, because they might not be able to interpret its context correctly. For instance, an algorithm used by Twitter to weed out 'hate speech' has been known to wrongfully remove harmless statements because it could not identify the context in which these statements were made.[50]

ii. *Lack of Transparency and Accountability* - Due to the opacity of these systems, it is difficult to ascertain the extent of the damage or harm they cause.[51] Further, algorithmic opacity also

[47] The letter is available at https://www.eff.org/files/2018/06/13/article13letter.pdf.
[48] Karen Yeung, "Algorithmic Regulation:A Critical Interrogation," *Regulation & Governance* 12 (2018): 505–23, https://doi.org/10.1111/rego.12158.
[49] Nicholas Thompson, "Instagram Unleashes an AI System to Blast Away Nasty Comments," *Wired*, June 29, 2017, https://www.wired.com/story/instagram-launches-ai-system-to-blast-nasty-comments/.
[50] Ibid
[51] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015) as cited by Karen Yeung in "Algorithmic Regulation:A Critical Interrogation," *Regulation & Governance* 12 (2018): 505–23, https://doi.org/10.1111/rego.12158.

makes it difficult to trace the point of system error such as which faulty dataset led the algorithm to make its final determination.[52]

iii. *There are inherent biases in the datasets used to train algorithms* - For instance, researchers have found a high rate of racial and gender bias in publicly available text embedding - a common source of data used to train machine-learning algorithms.[53]

iv. *No due process for individuals to challenge algorithmic decisions* - Algorithms geared towards taking down offensive or unlawful content generally do so automatically, by granting the user little or no opportunity to contest the take-down. Even when there is an opportunity to do so, the system may be loaded in favour of one party against the other. For instance, Google launched a Content ID program to allow rights-holders to make claims of copyright infringement on YouTube videos. Under the Content ID program copyright owners upload their videos to Google's repository. Algorithms proceed to scan the content and create a unique fingerprint of its elements. Thereafter, the algorithms search YouTube for any content that may match that fingerprint. Copyright owners may also make manual searches. Once a claim is filed, copyright owners may either have the allegedly offending video taken down, or monetise it through YouTube. As is evident, unfortunately, the system places the entire burden of proof solely on the alleged infringer, even in cases when it is blatant that no infringement has been made.[54] Further, disputes are a lengthy process and if the claimant insists that the work is infringed, the system weights their claim over the alleged infringer.[55]

Therefore, having a "person in the middle" is often presented as a solution for the issues with the automated decision-making proffered by algorithms. The premise here is that the algorithm will present its findings to a human being who will then make the final determination. Scholars note two reasons that such a strategy is ineffective for tackling the problems of algorithmic decision-making and oversight[56] --

- Making an individual a part of the procedure of determination fails to meet the "requirements of due process", namely "a fair hearing" and an impartial trial.
- People are susceptible to "automation bias" and have a tendency to yield to the data generated by computational calculations and analysis.

---

[52] Karen Yeung, "Algorithmic Regulation:A Critical Interrogation," *Regulation & Governance* 12 (2018): 505–23, https://doi.org/10.1111/rego.12158.
[53] Nathaniel Swinger et al., "What Are the Biases in My Word Embedding?" (Arxiv, December 27, 2019), https://arxiv.org/pdf/1812.08769.pdf.
[54] Paul Tassi, "The Injustice Of The YouTube Content ID Crackdown Reveals Google's Dark Side," *Forbes*, December 19, 2013, https://www.forbes.com/sites/insertcoin/2013/12/19/the-injustice-of-the-youtube-content-id-crackdown-reveals-googles-dark-side/.
[55] Ibid
[56] Karen Yeung, *Regulation & Governance* 12 (2018): 505–23, "Algorithmic Regulation: A Critical Interrogation", available at https://doi.org/10.1111/rego.12158.

In this context, it is our recommendation that if any legislation places the onus on intermediaries to regulate activity on their platforms, such legislation must ensure that the methods used by the intermediaries at the very least, adhere to the Santa Clara Principles, which set out a minimum threshold for accountability and transparency in online content removal.[57]

[57] The Santa Clara Principles are summarized as follows:

i. Companies must publicly share the number of posts and accounts that were "removed or temporarily suspended" for violating their community standards or "content guidelines.

ii. Appropriate notice must be provided to users whose accounts are temporarily or permanently suspended or posts are taken down.

iii. Users must get a realistic chance to appeal the take down of their account or post. Further, if a human is put in charge of making the final determination on an appeal, such an individual should be an independent authority that is not part of the company whose platform the content was removed from. For more detail please see, "The Santa Clara Principles on Transparency and Accountability in Content Moderation" (New America, 2018), available at https://newamericadotorg.s3.amazonaws.com/documents/Santa_Clara_Principles.pdf.

This document has been prepared by the Fellows at the Esya Centre; and Ms. Meghna Bal, a lawyer, and technology policy researcher based in New Delhi.

For any further contact, please get in touch with us at:

Esya Centre
B6-1 First Floor, DDA Commercial Complex
Safdarjung Enclave
New Delhi - 110029
+91-11-41834471
www.esyacentre.org