

Indian Intermediary Liability Regime

Compliance with the Manila Principles on Intermediary Liability

BY

Divij Joshi

EDITED BY

Elonnai Hickok, Swaraj Barooah

The Centre for Internet and Society, India

This research is funded by Facebook India.

Designed by **Saumyaa Naidu**



Shared under
Creative Commons Attribution 4.0 International license

Contents

Introduction	1
Assessment of Indian Intermediary Liability Law	1
Principle I	1
Recommendations	6
Principle II	7
Recommendations	11
Principle III	13
Recommendations	17
Principle IV	19
Recommendations	20
Principle V	22
Recommendations	25
Principle VI	26
Recommendations	30
Conclusion	32

Introduction

This report assesses the compliance of the Indian intermediary liability framework with the Manila Principles on Intermediary Liability, and recommends substantive legislative changes to bring the legal framework in line with the Manila Principles. The report is an examination of Indian laws based upon the background paper to the Manila Principles as the explanatory text on which these recommendations have been based, and not an assessment of the principles themselves. To do this, the report considers the Indian regime in the context of each of the principles defined in the Manila Principles. As such, the explanatory text to the Manila Principles recognizes that diverse national and political scenario may require different intermediary liability legal regimes, however, this paper relies only on the best practices prescribed under the Manila Principles.

Assessment of Indian Intermediary Liability Law

Principle I



Intermediaries
should be Shielded by
Law
from
Liability for
Third-Party Content

- a. Any rules governing intermediary liability must be provided by laws, which must be **precise, clear, and accessible**.
- b. Intermediaries should be immune from liability for third-party content in circumstances where they have not been involved in **modifying** that content.
- c. Intermediaries must not be held liable for failing to restrict **lawful** content.
- d. Intermediaries must never be made strictly liable for **hosting unlawful third-party content**, nor should they ever be required to **monitor content proactively** as part of an intermediary liability regime.

Recommendations

IT Act

- The framework under the IT Act would need to be amended to clarify that no direct liability for unlawful third party content shall accrue to an intermediary who does not modify the content.
- The liability should be limited to a reasonable penalty for the failure to take down content upon notification through a court order, or for failure to forward a notice of unlawful content between a complainant and the opposite party.

Copyright Act

- The scope of intermediary liability for primary infringement and secondary infringement should be clarified.
- Intermediaries should be defined under the Copyright Act, as defined in the IT Act.
- A provision may be introduced under Section 51(a)(2) to limit the liability of intermediaries who do not modify the content to a notice-and-notice requirement.
- If the IT Act and the Copyright Act incorporate similar notice-and-notice regimes, the amended Copyright Act may specifically provide that the responsibilities for intermediaries shall be governed by the provisions of Section 79 of the IT Act.

- A clear statutory framework could restrain the judiciary from resorting to extra-legislative means for content restriction.

Principle I: Intermediaries should be shielded by law from liability for third-party content

(a) Any rules governing intermediary liability must be provided by laws, which must be precise, clear, and accessible.

The statutory regime governing intermediary liability for third party content in India is to be found primarily, but not exclusively, in Section 79 of the Information Technology Act, 2000 (“**IT Act**”), the Information Technology (Intermediaries Guidelines) Rules, 2011 (“**Intermediary Guidelines Rules**”) as well as the Indian Copyright Act, 1957, (“**Copyright Act**”) and the Copyright Rules, 2013 (“**Copyright Rules**”). Separately, Section 69A of the IT Act, and the Rules under Section 69A, provide for a procedure for the government to take down third party content, failure for which makes the intermediary liable to a penalty. Section 69A and the associated rules are discussed in more detail below under Principle II.

Apart from the above, there is a parallel set of obligations for network service providers, which has its genesis under the Indian Telegraph Act, 1885 (“**Telegraph Act**”). The Telegraph Act empowers the central government to mandate and issue licenses for operating of telegraph services (which includes providing internet access). Such a license is not required in the case of online platforms or similar services, or any intermediary which does not provide internet access. The licenses under which network providers operate, namely the Internet Service Providers License and the Unified License, (“**Telecom Licenses**”) also govern intermediary liability for hosting third party content.¹ The Telecom Licenses, *inter alia*, also allow the government to issue directions for content restriction.²

The precise relationship between the different intermediary liability rules is unclear. While Section 79 provides for an umbrella safe harbour provision from civil and criminal legal liability, the license conditions are contractual and breach of the same could entail the termination or revocation of the ISP’s license by the Department of Telecommunications.³ Further, the relationship between liability for copyright infringement and the liability under the IT Act is also unclear. The Delhi High Court in the case of *Myspace vs Super Cassettes*,⁴ held that the safe harbour provisions are applicable to intermediaries in the case of copyright infringement, however, the court decision still leaves the applicable standards for intermediary liability under copyright law unclear, as will be discussed subsequently. Further, the IT Rules under Section 79 also contain provisions that are not directly related to conditions for safe harbour, and include provisions for cyber security reporting, which obligations are not appropriate within the scope of the IT Rules.

In 2015, the constitutionality of Section 79 and the IT Rules (among other provisions of the IT Act) were challenged before the Supreme Court of India in *Shreya Singhal v Union of India*. Section 79 as originally framed contained a ‘notice and takedown’ procedure, where

1 License Agreement for Unified License, available at http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf.

2 Clause 7.12, Chapter X, Unified License.

3 Clause 10, Chapter I, Unified License.

4 *Myspace Inc. v. Super Cassettes*, DELHI HIGH COURT, available at <https://indiankanoon.org/doc/12972852/>.

upon its own knowledge or upon receiving actual knowledge from any affected person, the intermediary would be held primarily liable for failure to take down a broad range of content, including any content which was ‘harmful’, ‘harassing’, ‘disparaging’ or ‘objectionable’. The Supreme Court held that the IT Rules as originally framed were likely to lead to a chilling effect on speech by intermediaries, and read down the provision by reading ‘actual knowledge’ of an intermediary to mean notice by a judicial or governmental order *specifically requiring the intermediary* to disable such content. Further, the restrictions ordered by courts must be within constitutional thresholds. As per the language of the judgement, not only must there be an order on the alleged illegality of the impugned content, but the order must also direct the intermediary to remove access to such content.⁵ Subsequently, the Supreme Court has issued directions to intermediaries to disable specific content, as in the case of *Kamlesh Vaswani v Union of India*, where websites operating child pornography were sought to be restricted.⁶

The regime under the Copyright Act is also difficult to navigate. While the Copyright Act does not define intermediaries, intermediaries may be held liable for secondary infringement under Section 51(a)(ii), which imposes liability upon any person ‘for permitting, for profit, a place to be used to communicate infringing works to the public’, unless they were not aware or had ‘no reasonable ground’ for believing that the works were infringing. In *Myspace v Super Cassettes*, the Delhi High Court interpreted the requirement of awareness to mean ‘actual knowledge’, of specific infringing works, not necessarily by way of a court order. However, the standard of notice required for the obligation to kick in is unclear.⁷

Section 52(1)(b) and 52(1)(c) of the Copyright Act provide for a specific safe harbour in the case of intermediary liability in the case of ‘transient or incidental’ copies of infringing works, however, such ‘transient or incidental’ works are not defined, leaving it open to differing interpretations, given the varied nature of possible intermediaries. Further, the standard for the intermediary for having ‘reasonable grounds’ under Section 52(1)(c) for believing that specified content is infringing is not defined, and may conflict with the proviso to the provision, which allows the intermediary the right to not disable access to content unless it is satisfied of its illegality. Section 52(1)(b) and (c) violate this principle by predicating safe harbour from liability upon complying with takedown notices. In addition, there is an overlap in the scope of the IT Rules and the Copyright Act, and it is unclear as to how the two regimes can be harmonized. Specifically, Rule 3(d) of the Intermediary Guidelines Rules requires intermediaries to respond to copyright infringement requests under the framework established under Section 79.

Beyond the statutory scheme, courts also regularly exercise their inherent powers in order to implead and issue directions to intermediaries to take down content, most conspicuously in the cases of copyright or trademark infringement. This has become a common practice, with intermediaries normally bearing the costs of content removal and facing the risk of contempt of court’s orders for failure to comply.⁸ These costs include operational costs of monitoring and policing the content flagged by the court, which may often be vaguely worded, as well

5 Shreya Singhal and Ors. v Union of India and Ors., Writ Petition(Criminal) No.167 OF 2012, available at http://supremecourtindia.nic.in/FileServer/2015-03-24_1427183283.pdf. “Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material.”

6 Kamlesh Vaswani v Union of India, Supreme Court of India, Order No. 813-7/25/2011-DS (Vol. V) dated March 31, 2015.

7 Myspace Inc. v. Super Cassettes, DELHI HIGH COURT, available at <https://indiankanoon.org/doc/12972852/>.

8 Ananth Padmanabhan, *Can Judges Order ISPs to Block Websites for Copyright Infringement?*, Centre for Internet and Society, available at <https://cis-india.org/a2k/blogs/john-doe-orders-isp-blocking-websites-copyright-1>.

as legal fees and other costs. These costs can add up and potentially be significant – as was pleaded by ISPs in the context of content restriction orders issued by UK Courts.⁹ The scope of the court’s power in this situation is unclear, and as such conflicts with the requirement that laws must be clear and accessible which is found under this principle.

Further, the Indian Supreme Court has held search engines, liable, as intermediaries, for hosting advertisements and keywords relating to pre-natal sex determination, in the case of *Sabu Mathew George v Union of India and Ors.*,¹⁰ where a writ petition was filed *inter alia* against search engine operators including Google, Yahoo and Microsoft, to hold them liable for displaying advertisements or searches in violation of the Prenatal Sex Determination Act, and the Court imposed obligations to monitor the complaints and respond to complaints relating to the Act upon the search engines. Such court-ordered actions for content restriction are outside of any explicit statutory authority, even though similar outcomes may be achieved through existing legislation (for example, blocking under Section 69 of the IT Act). Further, implicating intermediaries in such schemes makes them liable for its compliance, as failure to do so could be punished as contempt of court. The lack of statutory backing for such actions places them in violation of this principle.

(b) Intermediaries should be immune from liability for third-party content in circumstances where they have not been involved in modifying that content.

Section 79 of the IT Act grants intermediaries immunity for third party content, provided that they meet at least one of the below conditions (and subject to the notice and takedown procedure described above):

- a. *the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or*
- b. *the intermediary does not-*
 - (i) *initiate the transmission,*
 - (ii) *select the receiver of the transmission, and*
 - (iii) *select or modify the information contained in the transmission*
- c. *the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf for intermediary safe harbour.*

The provision clearly exempts all ‘mere conduit’ ISP’s from liability for information transiently passing through their networks. However, intermediaries may be held responsible if they ‘select or modify’ the information contained in the transmission, which is a vague and undefined requirement. Moreover, the immunity is subject to compliance with government guidelines (presently embodied in the IT Rules). The Supreme Court, in *Shreya Singhal*, has also clarified that Section 79 is an exemption provision, and therefore, the compliance with the conditions must be strictly complied with for availing safe harbour. This conflicts with the requirement that intermediaries as a rule should not be held liable for third party content unless they play a role in the modification of the impugned content, and should only be held liable to the extent of their modification.

9 *Cartier v bSkyb*, UK High Court, Chancery Division, available at <http://www.bailii.org/ew/cases/EWHC/Ch/2003/3354.html#para239>.

10 *Sabu Mathew George vs Union Of India And Ors.*, Writ Petition (Civil) No. 341 Of 2008, Supreme Court of India, (Order dt. December 17, 2017), available at <https://indiankanoon.org/doc/192654466/>.

(c) Intermediaries must not be held liable for failing to restrict lawful content.

This principle requires that intermediaries must not be penalized for hosting and not restricting content when the content itself is not illegal. Therefore, a prerequisite to intermediary liability must be that the content sought to be restricted is illegal, as determined by law. This principle is important in the context of emerging models of intermediary governance for aggregators such as search engines, for example in the case of the Court of Justice of the EU requiring Google to de-link lawful content in the interests of an individual's right to be forgotten.¹¹

As explained above, the IT Act and Intermediaries Guidelines Rules specified that intermediaries would be liable for restricting a range of content including that which was 'objectionable' or 'disparaging', although such content may not be considered illegal under Indian law. However, this has been read down by the Supreme Court, in *Shreya Singhal*, to only include content that has been determined unlawful through a legal process, in line with constitutional standards. Despite this, under the Intermediaries Guidelines Rules, intermediaries must still include terms of service which proscribe certain legal and/or illegal content. Thus despite the Judgment, intermediaries may pro-actively or on request remove content as per their Terms of Service - even if this content is otherwise legal.

The Supreme Court of India has also directed search engines to 'auto block' certain keyword searches and advertisements appearing on search engines, which could potentially violate the Prenatal Sex Determination Act, without making a specific determination as to the legality of the content being blocked.¹² In a similar case, the Supreme Court came up with a comprehensive framework for the intermediaries to respond to videos of sexual assault.¹³ This court-created framework requires the government to frame key regulations for search engines, such as, *inter alia*, a list of impermissible search terms, setting up a mechanism for reviewing requests related to such videos and establishing a committee to identify and block 'rogue sites'. Such an agency has been established by the Government of India, which directs search engines, from time to time, to restrict content based on the Supreme Court's guidelines.¹⁴ Certain aspects of the court's directions were aimed at specific intermediaries, such as Whatsapp, which was ordered to improve its complaints reporting mechanism. The creation of a separate judicial regime under which content takedown occurs takes away from the requirement of a clear legal basis and standard practice for content restriction, and also potentially exposes intermediaries to liability for contempt of court orders.

(d) Intermediaries must never be made strictly liable for hosting unlawful third-party content, nor should they ever be required to monitor content proactively as part of an intermediary liability regime.

The general statutory scheme for intermediary liability in India excludes strict liability for third party content, as explained above, provided the conditions under Section 79 are fulfilled.

11 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12, Court of Justice of the European Union, *available at* http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=152065&occ=first&dir=&cid=667631.

12 Sabu Mathew George vs Union Of India And Ors., Writ Petition (Civil) No. 341 Of 2008, SUPREME COURT OF INDIA, (Order dt. December 17, 2017), *available at* <https://indiankanoon.org/doc/192654466/>.

13 In re Prajwala, SMW (CrL) No(s).3/2015, Supreme Court of India, [supremecourt/2015/6818/6818_2015_Order_23-Oct-2017.pdf](http://supremecourtfindia.nic.in/supremecourt/2015/6818/6818_2015_Order_23-Oct-2017.pdf).

14 Sabu Mathew George vs Union Of India And Ors., Writ Petition (Civil) No. 341 Of 2008, Supreme Court of India, (Order dt. September 5, 2017), *available at* http://supremecourtfindia.nic.in/supremecourt/2008/21458/21458_2008_Order_05-Sep-2017.pdf

Recommendations

The intermediary liability regime in India imposes direct liability upon intermediaries for third party content in cases where the due diligence requirements have not been satisfied, or where the 'actual knowledge' standard has not been satisfied. To comply with this principle, the framework under the IT Act would need to be amended to clarify that no direct liability for unlawful third party content shall accrue to an intermediary who does not modify the content. The scope of modification should also be clarified. Any liability should be limited to a reasonable penalty for the failure to take down content upon notification through a court order, or for failure to forward a notice of unlawful content between a complainant and the opposite party, i.e. incorporate a notice-and-notice requirement (as described below). For example, Chilean law incorporates such a standard for 'actual knowledge', and only imposes liability upon an intermediary where it has knowingly failed to comply with a court order which specifies content to be restricted.¹⁵

The Copyright Act must also be amended to clarify the scope of intermediary liability for primary infringement and secondary infringement. Intermediaries should be defined under the Copyright Act as defined in the IT Act. A proviso may be introduced under Section 51(a) (2) to limit the liability of intermediaries who do not modify the content to a notice-and-notice requirement as described above. If the IT Act and the Copyright Act incorporate similar notice-and-notice regimes, the amended Copyright Act may specifically provide that the responsibilities for intermediaries shall be governed by the provisions of Section 79 of the IT Act. This would also remove the confusion stemming from the Delhi High Court's interpretation of the relationship between the Copyright Act and Section 79 safe harbour in *Myspace v Super Cassettes*. A notice and notice regime of this nature, for civil copyright disputes has been established in Canada, under the 2012 Copyright Modernisation Act.¹⁶

Two problems need to be addressed by the judiciary. The first is that of creating judicial regimes for intermediary liability, which is not statutorily permissible, using a Court's inherent powers. The second is of enjoining ISP's through John Doe orders to assist in content restriction in cases of copyright infringement without a clear finding of liability. The creation of a statutory framework whereby the boundary conditions for the exercise of content restriction powers under law are defined, would lead to a reduction in such arbitrary measures being taken for blocking content by the judiciary instead of under statutory law.

15 Claudio Ruiz Gallardo and J. Carlos Lara Gálvez, 'Liability of Internet Service Providers (ISPs) and the exercise of freedom of expression in Latin America', available at http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/02-Liability_Internet_Service_Providers_exercise_freedom_expression_Latin_America_Ruiz_Gallardo_Lara_Galvez.pdf.

16 Copyright Modernisation Act, 2012, (Canada), available at http://laws-lois.justice.gc.ca/eng/annualstatutes/2012_20/FullText.html.

Principle II

Content
*must not be required
to be*
Restricted
without an order by a

**Judicial
Authority**



- a. Intermediaries must not be required to restrict content unless an order has been issued by an independent and impartial **judicial authority** that has determined that the material at issue is **unlawful**.
- b. Orders for the restriction of content must:
 - Provide a determination that the content is unlawful in the **jurisdiction**.
 - Indicate the **Internet identifier** and **description** of the unlawful content.
 - Provide **evidence** sufficient to document the legal basis of the order.
 - Where applicable, indicate the **time period** for which the content should be restricted.
- c. Any liability imposed on an intermediary must be **proportionate** and **directly correlated** to the intermediary's wrongful behavior in failing to appropriately comply with the content restriction order.
- d. Intermediaries must not be liable for **non-compliance** with any order that does not comply with this principle.

Recommendations

- An expedited judicial process to address unlawful online content may be imported into the Indian framework. Concern of overburdened judicial systems and processes would have to be considered and addressed.
- Section 79(1), providing for safe harbour, should be de-linked from the obligation to take down content upon issuance of a court order under Section 79(3)(b).
- The IT Act may be amended to incorporate the requirement under *Shreya Singhal*, that an intermediary shall only be liable to take down content upon notification of the specific content by way of a court order directly addressed to it, and only for the period of time for which the illegality of the content persists. Failure to act upon such a notification may be addressed by a proportionate penalty.
- Section 69A, which empowers the government to issue content restriction requests without following basic norms of due process, would have to be deleted or amended to require a judicial order for blocking of content.
- The law should explicitly clarify the scope of Section 79 and its application to the Copyright Act.
- The requirement under Copyright Rules, that an intermediary must temporarily disable allegedly infringing content for 21 days, without judicial notice for the same, would need to be deleted.
- The regime for content restriction (currently found under Section 69A of the IT Act and the Blocking Rules) may be harmonized with the amended regime under the IT Act, providing for a judicial review of restriction requests.
- Criminal sanctions on intermediaries for non-compliance with government orders under the Blocking Rules would need to be repealed as being disproportionate and creating a chilling effect on the freedom of expression.

Principle II: Content must not be required to be restricted without an order by a judicial authority

(a) Intermediaries must not be required to restrict content unless an order has been issued by an independent and impartial judicial authority that has determined that the material at issue is unlawful.

At the outset, it is important to note that the intermediary liability and content restriction regimes are synchronous under the IT Act. Section 79 operates as a content restriction mechanism by linking safe harbour from liability to the requirement to respond to takedown notices.

Section 79 of the IT Act does not specify the threshold for an intermediary having ‘actual knowledge’ that the information which is in their control is being used for unlawful means. Moreover, Rule 3 of the IT Rules states that the intermediary must not only act upon ‘obtaining knowledge by itself’ or ‘being brought to actual knowledge by any affected person in writing’. Therefore, as originally framed, the provisions clearly do not require the intermediary to act only upon notice by a court, but upon any ‘affected person’ providing the intermediary with information, which presumably requires the intermediary to parse the information to determine its legality. However, after the Supreme Court decision in *Shreya Singhal*, the prevailing standard requires a content takedown notice to be issued by a court or a government order, for liability under Section 79 to incur. However, this standard does not apply to government blocking orders issued under Section 69A, described below.

Though the Manila principles recommend that an order comes from a judicial authority, they recognize and attempt to address the need to balance the right to freedom of expression, the needs of intermediaries, and the need to expeditiously respond to illegal content by recommending an expedited process for certain requests. As noted in the background paper to the Manila Principles, the requirement of judicial review/due process must strike a balance between overly burdening intermediaries and allowing unlawful content to remain online. It is necessary to respond to legitimate concerns regarding speech or content which may be clearly illegal and potentially harmful, which could include, for example, incitement to violence. The concerns of intermediary liability and potential censorship must therefore take into account the requirement to expeditiously remove such content. An expedited process attempts to balance the concerns of the targets of illegal content with the necessity to have judicial determination of content takedown. However, under the prevailing standard set by the Supreme Court of India in *Shreya Singhal*, no expeditious process or remedy has been contemplated.

The Delhi High Court, in the case of *Myspace v Super Cassettes*, has also held that the safe harbour exemption under Section 79 of the IT Act would apply for intermediaries to protect them from claims of copyright infringement as well. However, the court also ruled that, in the case of copyright infringement notices, the actual knowledge requirement would be fulfilled by a notice to the intermediary from the rights holder, containing the specifics of the content alleged to have been infringed.¹⁷

A similar ‘notice-and-takedown’ regime exists for ‘mere conduit’ intermediaries under the Copyright Act read with the Copyright Rules. Section 52 of the Copyright Act provides for exemptions from infringement. Section 52 states that the following would not constitute infringement of copyright –

“(b) the transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public;

¹⁷ Myspace Inc. v. Super Cassettes, Delhi High Court, available at <https://indiankanoon.org/doc/12972852/>.

(c) transient or incidental storage of a work or performance for the purpose of providing electronic links, access or integration, where such links, access or integration has not been expressly prohibited by the right holder, unless the person responsible is aware or has reasonable grounds for believing that such storage is of an infringing copy:

Provided that if the person responsible for the storage of the copy has received a written complaint from the owner of copyright in the work, complaining that such transient or incidental storage is an infringement, such person responsible for the storage shall refrain from facilitating such access for a period of twenty-one days or till he receives an order from the competent court refraining from facilitating access and in case no such order is received before the expiry of such period of twenty-one days, he may continue to provide the facility of such access.”

Section 75 of the Copyright Rules specifies the particulars of the notice contemplated under Section 52 as well as the procedure to be followed by the intermediary after receiving such a notice. The Copyright Act safe harbour is only available to certain classes of intermediaries, namely, to ‘mere conduit’ intermediaries who provide network access and those, such as search engines, which provide hyperlinks or incidental storage, unlike the general safe harbour under Section 79 of the IT Act for intermediaries not modifying or selecting the content. While the procedure attempts to provide safeguards by requiring a judicial order as a prerequisite to the permanent blocking or removal of certain infringing content, it requires the intermediaries to block the content merely upon notice by the affected person for a period of 21 days, wherein intermediary would be required to assess the legality of the content themselves. Thus, the requirement found in Indian law to remove content without judicial determination of the same is a violation of this principle.

Besides takedown orders which can be issued by judicial authorities, the IT Act also contains provisions by which various government departments can issue content blocking requests to intermediaries, under Section 69A read with the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (“**Blocking Rules**”). The constitutionality of such blocking orders was upheld by the Supreme Court in the case of *Shreya Singhal v Union of India*,¹⁸ where the court noted that the IT Act and the Blocking Rules contained adequate safeguards to protect against its misuse. The Blocking Rules allow any government department to issue a request for removal of content by an intermediary, the request is examined by an executive committee, through a quasi-judicial administrative process, which allows for a personal hearing of the intermediary of third party to take place as well. However, the procedure (and practice) of issuing takedown requests under the Blocking Rules has been criticised for lacking proper safeguards, including the lack of judicial review and basic due process requirements for hearing the intermediary¹⁹

Finally, as noted above, the Telecom Licenses required for network service providers allow for the government to order content restriction by such ISPs, without judicial determination, which is also contrary to this principle.

(b) Orders for the restriction of content must:

1. Provide a determination that the content is unlawful in the jurisdiction.
2. Indicate the Internet identifier and description of the unlawful content.
3. Provide evidence sufficient to document the legal basis of the order.
4. Where applicable, indicate the time period for which the content should be restricted.

¹⁸ *Shreya Singhal and Ors. v Union of India and Ors.*, Writ Petition(Criminal) No.167 OF 2012, available at http://supremecourtindia.nic.in/FileServer/2015-03-24_1427183283.pdf.

¹⁹ Geetha Hariharan, *Is India's website-blocking law constitutional? – I. Law & Procedure*, Centre for Internet and Society, available at <https://cis-india.org/internet-governance/blog/is-india2019s-website-blocking-law-constitutional-2013-i-law-procedure>

There are no statutory or judicial guidelines that judicial orders for content restriction must follow. The only requirement, as specified by the Supreme Court in *Shreya Singhal v Union of India*,²⁰ is that the content determined unlawful by a court of law must be deemed to fall under one of the heads under which reasonable restrictions on the freedom of speech can be placed, namely, in the case of *'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.'*²¹

Under the Blocking Rules, orders are issued by a quasi-judicial committee, are not required to be made public and are issued only to the person or intermediary hosting the content.²² The committee is empowered to determine the legality of the content under Section 69A of the IT Act. There is no requirement for the order to only recognize specific identifiers or descriptions of the content deemed to be unlawful, and the only requirement for evidence/proof of illegality is a sample of the content alleged to be unlawful under Section 69A.²³ There is also no requirement for the committee to specify a time period within which such content may be restored. Rule 8 also allows intermediaries to respond to the allegations regarding the impugned content, however, this is not mandatory in cases where the intermediary cannot be identified through the 'reasonable efforts' of the committee.

The Telecom Licenses merely specify that content restriction requests must refer to 'specific instances', but do not provide further guidelines for these requests.

The intermediary liability regime under Section 79, as interpreted by the Supreme Court in *Shreya Singhal*, requires the judicial order for removal of content to be directed specifically at the intermediary. However, under the Copyright Act read with the Copyright Rules, no such specificity is required, and the rights owner or exclusive licensee may approach the intermediary with an order of a court only determining whether a specific copy is infringing or not.²⁴ There is also no clear standard followed by the judiciary in cases where ISP's are required under John Doe orders to restrict content, although the Bombay High Court has attempted to bring more specificity into the practice of identifying infringing content, as discussed below.

(c) Any liability imposed on an intermediary must be proportionate and directly correlated to the intermediary's wrongful behavior in failing to appropriately comply with the content restriction order.

This principle requires that in cases where conditional safe harbour is provided to intermediaries, they should not be found liable for the primary action in cases where the safe harbour conditions have not been complied with. For example, the failure to abide by a court order for content restriction should result in liability for contempt of court and not the primary liability for the content itself. Legal provisions and judicial precedent in India do not meet the standards laid out in this principle.

Section 69A of the IT Act establishes a criminal penalty upon intermediaries for non-compliance of the blocking orders issued by the government. In such a case of inaction, the intermediary may be liable for imprisonment for up to 7 years or a fine, which is not specified. The penalty imposed under Section 69A, is criminal in nature, and has been highlighted as disproportionate.²⁵

20 *Shreya Singhal and Ors. v Union of India and Ors., Writ Petition(Criminal) No.167 OF 2012, available at http://supremecourtindia.nic.in/FileServer/2015-03-24_1427183283.pdf.*

21 Article 19(2), Constitution of India, 1950.

22 Rule 8, Blocking Rules.

23 Rule 5, Blocking Rules.

24 Section 52 of the Copyright Act, read with Rule 75 of the Copyright Rules.

25 <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf>

However, where an intermediary is found to be liable under Section 79 for lack of safe harbour, or for civil liability under the Copyright Act, there is no threshold for liability - such intermediaries may be held primarily liable for the content, which may entail civil or criminal penalties. For example, in the landmark case of *Avnish Bajaj v State*, before the enactment of the safe harbour under Section 79, the Court found the proprietor of a website criminally liable for content hosted on its marketplace.²⁶

(d) Intermediaries must not be liable for non-compliance with any order that does not comply with this principle.

As noted above, there may be circumstances where an intermediary may be held liable for non-compliance of an order which is not a judicially determined order and does not fulfill the safeguards required under this principle.

Recommendations

There are several models which may be followed to draw a balance between protecting intermediaries from undue liability and ensuring expeditious removal of content. The administrative quasi-judicial committee constituted under the Blocking Rules attempts to provide such a model, however, it lacks important safeguards - in particular, there is no provision for judicial review of allegedly illegal content. Another model, incorporating an expedited judicial review, has been put in place in Chile.²⁷ An expedited judicial process to address unlawful online content may be imported into the Indian framework as well, though there is the existing concern of overburdened judicial systems and processes that would have to be considered and addressed.

Further, the Manila Principles require that immunity of the intermediary from primary liability for the content itself must not be conditional upon compliance with such an order. The liability for failure to comply with a court direction must be proportional to the action of the intermediary, which may be penalised under general laws of contempt of a court order, or alternatively for failure to comply with Section 79. Therefore, it is proposed that Section 79(1), providing for safe harbour, be de-linked from the obligation to take down content upon issuance of a court order under Section 79(3)(b). Under Canada's notice-and-notice framework, the liability of intermediaries is limited to a financial penalty for failure to forward a notice of infringement to an identified third party content provider. This limits the potential liability of an intermediary and shields intermediaries from direct liability for actions of third parties.

To comply with the principle that content should not be required to be taken down without a judicial order (whether under an expedited process or otherwise), the Information Technology Act may be amended to incorporate the requirement under *Shreya Singhal*, that an intermediary shall only be liable to take down content upon notification of the specific content by way of a court order directly addressed to it, and only for the period of time for which the illegality of the content persists. Failure to act upon such a notification may be addressed by a proportionate penalty. This requirement will also foster transparency, as judicial orders are, by default, public.

26 *Avnish Bajaj v State*, Delhi High Court, 116 (2005) DLT 427, available at <https://indiankanoon.org/doc/309722/>. In this case, the website hosted an online marketplace, where a third party put up an advertisement for a pornographic clip of a minor. The Court held that the actions of the MD of the website, in failing to take action against the illegal clip (such as by putting up filtering mechanisms) was sufficient to attract the provisions of the Indian Penal Code, and sentenced him to imprisonment.

27 'Chile's Notice - And Takedown System For Copyright Protection: An Alternative Approach', Centre for Democracy and Technology (2012), available at <https://cdt.org/files/pdfs/Chile-notice-takedown.pdf>.

To bring Indian law in compliance with this principle, Section 69A, which empowers the government to issue content restriction requests without following basic norms of due process, would have to be deleted or amended to require a judicial order for blocking of content.

Where takedowns in cases of copyright infringement are concerned, the Delhi High Court's interpretation in *Myspace v Super Cassettes*, of the actual knowledge requirement under Section 79 is flawed.²⁸ The interpretational differences in Section 79 may be resolved if Section 79 is amended, as suggested above, and the law explicitly clarifies the scope of Section 79 and its application to the Copyright Act. Further, the requirement under the Copyright Rules, that an intermediary must temporarily disable allegedly infringing content for 21 days, without judicial notice for the same, would need to be deleted. The regime for content restriction (currently found under Section 69A of the IT Act and the Blocking Rules) may be harmonized with the amended regime under the IT Act, providing for a judicial review of restriction requests.

Finally, criminal sanctions on intermediaries for non-compliance with government orders under the Blocking Rules would need to be repealed as being disproportionate and creating a chilling effect on the freedom of expression.

28 *Myspace Inc. v. Super Cassettes*, Delhi High Court, available at <https://indiankanoon.org/doc/12972852/>.

Principle III



Requests
for
Restriction
of Content
must be

Clear,
Unambiguous,
and
**Follow Due
Process**

- a. Intermediaries must not be required to substantively evaluate the **legality of third-party content**.
- b. A **content restriction request** pertaining to unlawful content must, at a minimum, contain the following:
 - The **legal basis** for the assertion that the content is unlawful.
 - The **Internet identifier** and **description** of the allegedly unlawful content.
 - The consideration provided to **limitations, exceptions, and defences** available to the user content provider.
 - **Contact details** of the issuing party or their agent, unless this is prohibited by law.
 - **Evidence** sufficient to document legal standing to issue the request.
 - A **declaration of good faith** that the information provided is accurate.
- c. Content restriction requests pertaining to an intermediary's **content restriction policies** must, at the minimum, contain the following:
 - The **reasons** why the content at issue is in breach of the intermediary's content restriction policies.
 - The **Internet identifier** and **description** of the alleged violation of the content restriction policies.
 - **Contact details** of the issuing party or their agent, unless this is prohibited by law.
 - A **declaration of good faith** that the information provided is accurate.
- d. Intermediaries who host content may be required by law to **respond** to content restriction requests pertaining to unlawful content by either forwarding lawful and compliant requests to the user content provider, or by notifying the complainant of the reason it is not possible to do so ('notice and notice'). Intermediaries should not be required to ensure they have the capacity to identify users.
- e. When forwarding the request, the intermediary must provide a clear and accessible explanation of the **user content provider's rights**, including in all cases where the intermediary is compelled by law to restrict the content a description of any available counter-notice or appeal mechanisms.
- f. If intermediaries restrict content hosted by them on the basis of a content restriction request, they must comply with Principle VI on **transparency and accountability** below.
- g. **Abusive or bad faith** content restriction requests should be penalized.

Recommendations

- A notice-and-notice framework for hosting intermediaries may be adopted in India.
- Section 79 should be amended to include a provision for conditional liability on a 'notice and notice' basis, except for 'mere conduit' or caching intermediaries who are not responsible for modification of any content.
- A clause may be inserted to Section 79, providing that an intermediary (not being a mere conduit intermediary) upon receipt of a notice shall forward such notice to the third party content provider, and shall retain the records of available information on the third party content provider for a specific period upon receipt of the notice, for the purpose of identifying such third party.
- The liability of the intermediary for failing to comply with the forwarding requirement should not be equated with primary liability, and may be fixed under the scheme itself, as an appropriate monetary penalty or damages to the affected person.
- The costs for forwarding the notice by the intermediary to the alleged third party content provider should be borne by the person sending the notice, by way of an appropriate fees to be paid along with the notice, which may be prescribed by the government.
- There must be appropriate penalties for takedown notifications which are issued in bad faith or if they constitute an abuse of process.

Principle III: Requests for restrictions of content must be clear, be unambiguous, and follow due process

(a) Intermediaries must not be required to substantively evaluate the legality of third-party content.

A core concern of the Manila Principles is that intermediaries should not effectively determine the legality of content and attempt to restrict it upon its own evaluation. Laws which require intermediaries to judge the legality of content restriction requests, such as the obligation upon search engines in the EU to de-index certain links under the Right to Be Forgotten, place the intermediaries in the position where they must substantively assess important rights, including privacy and freedom of expression, which are determinations which must be made by the judiciary.

In India, the notice-and-takedown regime under the Copyright Act and the Copyright Rules requires the intermediary to assess whether the flagged material is infringing and to take down content upon its own satisfaction that such content is infringing for a period of at least 21 days, or until it receives judicial notice that the content is not illegal.²⁹ Further, as noted above, the Supreme Court in *Sabu Mathew George*, has in the past ordered search engines to install 'auto-blocks' for filtering content related to pre-natal sex determination, without sufficient precision as to what should be captured within the filter.³⁰ Thus, intermediary liability law in India does, in certain circumstances, place intermediaries in a position where they must evaluate the legality of content and take appropriate action.

29 Rule 75, Copyright Rules.

30 *Sabu Mathew George vs Union Of India And Ors.*, Writ Petition (Civil) No. 341 Of 2008, SUPREME COURT OF INDIA, (Order dt. December 17, 2017), available at <https://indiankanoon.org/doc/192654466/>.

(b) A content restriction request pertaining to unlawful content must, at a minimum, contain the following:

1. The legal basis for the assertion that the content is unlawful.
2. The Internet identifier and description of the allegedly unlawful content.
3. The consideration provided to limitations, exceptions, and defences available to the user content provider.
4. Contact details of the issuing party or their agent, unless this is prohibited by law.
5. Evidence sufficient to document legal standing to issue the request.
6. A declaration of good faith that the information provided is accurate.

The only legislative requirement in India, which captures the contents of the notice by an affected person under a notice and takedown regime, is contained in the Copyright Rules. As per Rule 75 read with Section 51 of the Copyright Act, the owner of a copyrighted work may have such work restricted by a mere conduit intermediary, following a notice and takedown procedure. Rule 75 requires that such a notice must, at a minimum, contain the following:

- “(a) the description of the work with adequate information to identify the work;*
- (b) details establishing that the complainant is the owner or exclusive licensee of copyright in the work;*
- (c) details establishing that the copy of the work which is the subject matter of transient or incidental storage is an infringing copy of the work owned by the complainant and that the allegedly infringing act is not covered under Section 52 or any other act that is permitted under the Act;*
- (d) details of the location where transient or incidental storage of the work is taking place;*
- (e) details of the person, if known, who is responsible for uploading the work infringing the copyright of the complainant; and*
- (f) undertaking that the complainant shall file an infringement suit in the competent court against the person responsible for uploading the infringing copy and produce the orders of the competent court having jurisdiction, within a period of twenty-one days from the date of receipt of the notice.”*

As per these conditions, the claimant of the copyright in the work is not required to specifically identify the URL of the infringing work, nor are they required to assess any possible limitations, exceptions or defences which the third party content provider may take, or provide any assurance that the notice has been sent in good faith. However, there is an important safeguard in that the owner must provide the intermediary a copy of an order of a court against the third party provider of the content, within a period of 21 days from sending the notice.

There is little judicial guidance on the contents of a notice for removal in the case of an intermediary which is not a mere conduit and which is governed under Section 79 of the IT Act. While the Delhi High Court, in *Myspace v Super Cassettes*, has allowed for a notice and takedown system for copyright infringement other than by mere conduits, there is no requirement in the judgement for such a notice to comply with this principle, save for the fact that the specific infringing URL must be provided to the intermediary.³¹

Further, where content restriction is sought through blocking injunctions and John Doe orders, practice has varied across courts and from case to case – in several instances,

31 *Myspace Inc. v. Super Cassettes*, Delhi High Court, available at <https://indiankanoon.org/doc/12972852/>.

courts have merely accepted the petitioners' submissions and issued orders to ISPs to block entire websites, without even prima facie determination of whether the website contains any actionable material.³² However, some courts have attempted to draw guidelines to be followed in such cases, for example, the Bombay High Court in *Balaji Motion Pictures v BSNL* required that the plaintiffs submit specific infringing URLs which have been verified by third parties.³³ However, such guidelines were restricted to specific cases and have not seen wide adoption.

(c) Content restriction requests pertaining to an intermediary's content restriction policies must, at the minimum, contain the following:

1. The reasons why the content at issue is in breach of the intermediary's content restriction policies.
2. The Internet identifier and description of the alleged violation of the content restriction policies.
3. Contact details of the issuing party or their agent, unless this is prohibited by law.
4. A declaration of good faith that the information provided is accurate.

Ruled 3(2) of the Intermediary Guidelines provides that the content restriction policies of an intermediary must, at a minimum, provide that a user may not:

"...host, display, upload, modify, publish, transmit, update or share any information that

a) belongs to another person and to which the user does not have any right to;

b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;

c) harm minors in any way;

d) infringes any patent, trademark, copyright or other proprietary rights; (e) violates any law for the time being in force;

e) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

f) impersonate another person;

h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

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

There are no legal provisions for the form of a notice to be provided in the case of a claimed infraction of the terms and conditions of the content restriction policies of an intermediary, including infractions pertaining to content specified in the IT Rules.

32 Divij Joshi, 'Madras High Court Issues 'Ashok Kumar' Order to Block the Internet Archive + 2649 Websites', available at <https://spicyip.com/2017/08/madras-high-court-issues-ashok-kumar-order-to-block-the-internet-archive-2649-websites.html>.

33 *Balaji Motion Pictures v BSNL*, Bombay High Court, (July 4, 2016), available at <https://spicyip.com/wp-content/uploads/2016/07/Great-Grand-Masti-2.pdf>

(d) Intermediaries who host content may be required by law to respond to content restriction requests pertaining to unlawful content by either forwarding lawful and compliant requests to the user content provider, or by notifying the complainant of the reason it is not possible to do so ('notice and notice'). Intermediaries should not be required to ensure they have the capacity to identify users.

(e) When forwarding the request, the intermediary must provide a clear and accessible explanation of the user content provider's rights, including in all cases where the intermediary is compelled by law to restrict the content a description of any available counter-notice or appeal mechanisms.

Principles (d) and (e) above, advocate for the responsibility and liability of intermediaries in the case of content restriction to be limited to being a facilitator forwarding notices between the disputing parties.

As described above, Indian laws either contemplate a notice-and-takedown regime upon receiving information of allegedly unlawful content directly from users, or by way of a court order directed at the intermediary. Accordingly, no obligation of forwarding notices between the disputing parties is found in the Indian context. Further, there is no requirement for the third party content provider or author of the original content to be given any notice about such a takedown of their content by the intermediary.

(f) If intermediaries restrict content hosted by them on the basis of a content restriction request, they must comply with Principle VI on transparency and accountability below.

There are no transparency requirements for intermediaries regarding content restrictions. This is discussed in detail in Principle VI, below.

(g) Abusive or bad faith content restriction requests should be penalized.

There is no legal provision under the intermediary liability regime to penalise content restriction requests which are illegitimate and sent in bad faith. As such, there is little legal disincentive against abusive requests being sent to the intermediaries.

Recommendations

India's statutory scheme for safe harbour currently prescribe notice-and-takedown regimes where intermediaries must evaluate the legality of third-party content. This has been sought to be read down by the Supreme Court of India in *Shreya Singhal v Union of India*, as explained above. However, much confusion prevails over the response expected of intermediaries in instances of copyright infringement. In particular, the Court's reading down of conditional safe harbour, through its interpretation of the 'actual knowledge' requirement, does not strike a balance between the rights of a party affected by allegedly unlawful content, and the rights of the intermediary or general public who may access such information.

The Manila Principles endorse a 'notice and notice' requirement for hosting intermediaries who receive knowledge of allegedly unlawful content from a third party. Under this regime, the intermediary's safe harbour for third party content is conditional upon forwarding the notice of the content to the third party content provider in order to allow the affected party to directly resolve the dispute with the third party. Where such third party cannot be

found, or it is not possible to directly initiate action against the third party content provider, the affected party may obtain a judicial order against an intermediary for takedown. The conditional liability under such a scheme should be limited to hosting intermediaries or intermediaries responsible for modification of content (such as search engines, in certain cases). Such a scheme has been implemented under the Canadian Copyright Modernization Act.³⁴ The Canadian Copyright Modernisation Act envisages a notice-and-notice framework in the context of copyright infringement. The law specifies that the notice must be narrowly tailored and point out the specific infringing content, in a form compliant with statutory requirements. A similar framework may be adopted in India.

Substantive amendments to the statutory scheme for conditional liability would have to be implemented to change the present position of conditional safe harbour in India. In particular, it is recommended that Section 79 be amended to include a provision for conditional liability on a 'notice and notice' basis, except for 'mere conduit' or caching intermediaries who are not responsible for modification of any content.

A clause may be inserted to Section 79, which should provide that an intermediary (not being a mere conduit intermediary) upon receipt of a notice (complying with the conditions set out above in sub-principle III(b)) shall forward such notice to the third party content provider, and shall retain the records of available information on the third party content provider for a specific period upon receipt of the notice, for the purpose of identifying such third party. The liability of the intermediary for failing to comply with the forwarding requirement should not be equated with primary liability, and may be fixed under the scheme itself, as an appropriate monetary penalty or damages to the affected person. Further, the costs for forwarding the notice by the intermediary to the alleged third party content provider should be borne by the person sending the notice, by way of an appropriate fees to be paid along with the notice, which may be prescribed by the government. The fees would also act as an adequate deterrent against bad faith notices. In addition, there must be appropriate penalties for takedown notifications which are issued in bad faith or if they constitute an abuse of process. The US DMCA contains a provision for bad faith or abusive takedown notices to be penalized, although its efficacy in the larger frame of the law may be found wanting.³⁵

34 Canada's Approach to Intermediary Liability for Copyright Infringement: the Notice and Notice Procedure, Berkeley Technology Law Journal, (May 2014), available at <http://btlj.org/2014/03/canadas-approach-to-intermediary-liability-for-copyright-infringement-the-notice-and-notice-procedure/>.

35 <http://cyberlaw.stanford.edu/blog/2017/01/dmca-counter-notice-does-it-work-correct-erroneous-takedowns>

Principle IV

Laws
and
Content Restriction
Orders and Practices
must comply
with the tests of
Necessity and
Proportionality

- a. Any restriction of content should be limited to the **specific content** at issue.
- b. When restricting content, the **least restrictive technical means** must be adopted.
- c. If content is restricted because it is unlawful in a particular geographical region, and if the intermediary offers a geographically variegated service, then the **geographical scope** of the content restriction must be so limited.
- d. If content is restricted owing to its unlawfulness for a limited duration, the restriction must not last beyond this **duration**, and the restriction order must be reviewed periodically to ensure it remains valid.

Recommendations

- The requirements for a legally valid order for taking down content must be specified under the IT Act, as recommended above, incorporating the requirements of specificity.
- The Intermediary Guidelines may be amended to include that the intermediary must adopt the least technical means for restricting content, and should not restrict content beyond the geographical or temporal scope of the application of the takedown order.
- Where technical means like DRM or TPMs have been adopted in order to filter or prevent copyright infringement, the law should adequately protect fair uses of the protected content without incurring liability for circumvention of such TPMs. The Indian position on the same would have to be clarified by amendments to the Copyright Act.
- The Copyright Rules (specifically Section 75) may be amended to include such requirements in cases of content restrictions orders or requests in cases of online infringement of copyright.

Principle IV: Laws and content restriction orders and practices must comply with the tests of necessity and proportionality

(a) Any restriction of content should be limited to the specific content at issue.

There is no statutory requirement under Indian law for takedown requests to be narrowly tailored to only the specific content at issue. However, in the case of intermediary liability for copyright infringement, the Delhi High Court has read in a requirement that the intermediary must be provided with the URLs of the specific infringing content for a takedown notice to be valid.³⁶ Further, in the context of judicially ordered takedown through John Doe orders, courts have, in specific instances, required plaintiffs to provide specific details of the content sought to be restricted, and to have the same verified by a third party.

36 Myspace Inc. v. Super Cassettes, Delhi High Court, available at <https://indiankanoon.org/doc/12972852/>.

(b) When restricting content, the least restrictive technical means must be adopted.

There is no statutory requirement to use the least restrictive technical means for content restriction through legal mechanisms. There is, in fact, a trend in the judiciary to require intermediaries to broadly filter content using auto-blocking features, which may be disproportionately restrictive.³⁷ Similarly, in the case of issuing blocking injunctions to intermediaries impleaded in copyright or trademark infringement disputes, courts have often ordered the blocking of entire websites as compared to specific infringing URL's.³⁸ Further, in the context of copyright claims, the use of Technological Protection Measures or Digital Rights Management technologies are frequently utilized to prevent unauthorized access of copyrighted content. However, these technical measures tend to be overbroad and fail to incorporate legal safeguards against content restriction, such as requirements to enable fair use of copyrighted content, which is a right under Section 52 of the Copyright Act. An intermediary liability regime which places the burden upon intermediaries to expeditiously identify and remove content engenders the use of such broad technical measures.

(c) If content is restricted because it is unlawful in a particular geographical region, and if the intermediary offers a geographically variegated service, then the geographical scope of the content restriction must be so limited.

Indian law does not make any specific provision for the geographical scope of any content restriction orders by a court or any government authority. The extra-territorial reach of blocking orders on the internet has not been examined in an Indian Court.

(d) If content is restricted owing to its unlawfulness for a limited duration, the restriction must not last beyond this duration, and the restriction order must be reviewed periodically to ensure it remains valid.

There is no provision for a mandatory periodic review of a restriction which may be time-sensitive. As such, courts or government authorities are not required to tailor content restriction requests to an appropriate time-frame for content which is unlawful only for a limited duration.

Recommendations

The requirements of specificity of content required to be restricted, adopting the least restrictive technical means for restriction, and ensuring geographical and temporal limitations on the restriction may all be built into the statutory scheme by appropriate amendments to the IT Act and Rules and the Copyright Act and Rules. The requirements for a legally valid order for taking down content must be specified under the IT Act, as recommended above, incorporating the requirements of specificity. Chilean law incorporates some of these elements, including specificity of content and identification of the relevant rights holder, etc. The European Council has also recommended provisions that states may adopt to incorporate the above safeguards in content restriction notices.³⁹

37 Sabu Mathew George vs Union Of India And Ors., Writ Petition (Civil) No. 341 Of 2008, Supreme Court of India, (Order dt. December 17, 2017), available at <https://indiankanoon.org/doc/192654466/>.

38 Madras High Court Issues 'Ashok Kumar' Order to Block the Internet Archive + 2649 Websites, SPICYIP, (August, 2017), available at <https://spicyip.com/2017/08/madras-high-court-issues-ashok-kumar-order-to-block-the-internet-archive-2649-websites.html>.

39 Council of Europe, 'Recommendation on freedom of expression and information with regard to Internet filters,' (March 26, 2008), available at <https://wcd.coe.int/ViewDoc.jsp?id=1266285&Site=CM>.

In order to implement the principles of geographical and temporal limitation of content restriction by intermediaries, upon receipt of lawful orders or requests, the Intermediary Guidelines may be amended to include that the intermediary must adopt the least technical means for restricting content, and should not restrict content beyond the geographical or temporal scope of the application of the takedown order. Further, where technical means like DRM or TPMs have been adopted in order to filter or prevent copyright infringement, the law should adequately protect fair uses of the protected content without incurring liability for circumvention of such TPMs. The Indian position on the same would have to be clarified by amendments to the Copyright Act.⁴⁰

Similarly, the Copyright Rules (specifically Section 75) may be amended to include such requirements in cases of content restrictions orders or requests in cases of online infringement of copyright.

40 T. Krishnakumar and K. Saha, 'India's new copyright law: the good, the bad and the DRM', *Journal of Intellectual Property Law and Practice*, (2012), available at <https://jiplp.blogspot.in/2012/12/indias-new-copyright-law-good-bad-and.html>.

Principle V

Laws
and
Content Restriction
Policies and Practices
must respect

Due Process



- a. Before any content is restricted on the basis of an order or a request, the intermediary and the user content provider must be provided an effective **right to be heard** except in exceptional circumstances, in which case a post facto review of the order and its implementation must take place as soon as practicable.
- b. Any law regulating intermediaries must provide both user content providers and intermediaries the **right of appeal** against content restriction orders.
- c. Intermediaries should provide user content providers with **mechanisms to review decisions** to restrict content in violation of the intermediary's content restriction policies;
- d. In case a user content provider wins an appeal under (b) or review under (c) against the restriction of content, intermediaries should **reinstate the content**.
- e. An intermediary should not disclose **personally identifiable information about a user** without an order by a judicial authority. An intermediary liability regime must not require an intermediary to disclose any personally identifiable user information without an order by a judicial authority.
- f. When drafting and enforcing their content restriction policies, intermediaries should respect **human rights**. Likewise, governments have an obligation to ensure that intermediaries' content restriction policies respect human rights.

Recommendations

- Section 79 may be amended to require that, in any case where a content restriction is sought against an intermediary, the intermediary shall be made a necessary party to the proceedings.
- Intermediary Guidelines Rules must be amended to (1) delete the mandate for intermediaries to restrict and monitor certain content as per their terms of use; and (2) incorporate a due process requirement when dealing with content restriction requests based on the breach of terms of use.
- Rule 3(2) of the Intermediary Guidelines would need to be deleted, as intermediaries must not be compelled to include terms of service which restrict lawful content.
- The Rules must be amended to require intermediaries to follow transparent and fair practices in the enforcement of their terms of service.
- The obligations for data sharing upon government order imposed upon intermediaries under various Acts (and licenses) must be deleted, including under Rule 3(7) of the Intermediary Guidelines Rules.
- India should take the lead in developing a legal framework incorporating due process and transparency requirements between intermediaries and their users.

Principle V: Laws and content restriction policies and practices must respect due process

(a) Before any content is restricted on the basis of an order or a request, the intermediary and the user content provider must be provided an effective right to be heard except in exceptional circumstances, in which case a post facto review of the order and its implementation must take place as soon as practicable.

There is no clear guidance on whether intermediaries are required to be party to all litigations where directions for content restriction may be ordered against an intermediary under Section 79 of the IT Act.

Further, there is no provision for a right to a hearing prior to a content restriction request or order against an intermediary under the Blocking Rules. Where a content restriction order is issued by a government department under the Blocking Rules, as per Rule 8, the appropriate government must take all 'reasonable steps' to notify *either* the intermediary *or* the content provider in respect of the impugned content, and direct them to submit their clarifications as well as appear in a personal hearing before the committee constituted to review such requests for restriction. However, as per Rule 9, in emergency situations (which are not defined), such a hearing or submission from the relevant intermediary or content provider may be disposed off prior to the content restriction, and may be held up to 48 hours after the issuance of the the content takedown request.

Intermediaries themselves have significant leeway to restrict content in breach of their terms of use, under Rule 3(5) of the Intermediary Guidelines Rules, which allows intermediaries to "*immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove noncompliant information.*" There are no due process requirements mandated of intermediaries when exercising their right to remove content based upon the breach of their terms of service, apart from a salutary requirement that users be informed that the breach of terms of services entitles the intermediary to terminate its services.

The Manila Principles acknowledge that certain circumstances may require that takedown notices must be complied with, without delay, and do not attempt to list out such extenuating circumstances. However, Indian law does not provide for a judicial hearing for the intermediary in any scenario, and therefore is in violation of this principle.

(b) Any law regulating intermediaries must provide both user content providers and intermediaries the right of appeal against content restriction orders.

There is no right to appeal under the substantive provisions for content restriction against intermediaries or user content providers under Indian law.

(c) Intermediaries should provide user content providers with mechanisms to review decisions to restrict content in violation of the intermediary's content restriction policies;

(d) In case a user content provider wins an appeal under (b) or review under (c) against the restriction of content, intermediaries should reinstate the content.

While some intermediaries, such as TATA Communications and Vodafone, which operate under Indian laws, provide for grievance redressal mechanisms to counter wrongful restriction of users' content by an intermediary, there is no specific obligation for the

intermediary to provide mechanisms for users to challenge any decision taken by an intermediary against user content. However, the Intermediary Guidelines require intermediaries to appoint a grievance officer, who is required to take action on complaints sent by the 'victims' of allegedly unlawful content. However, some legal remedies may be available under contract law, for breach of contract in cases of violation of the terms of service or terms of use between the intermediary and the user.⁴¹ Such remedies have not been used in India, however, there is some jurisprudence regarding the binding nature of such contractual terms in other jurisdictions like the US and Canada.⁴²

(e) An intermediary should not disclose personally identifiable information about a user without an order by a judicial authority. An intermediary liability regime must not require an intermediary to disclose any personally identifiable user information without an order by a judicial authority.

India has a notoriously lax data protection regime, and India's surveillance regime places significant burdens upon intermediaries to monitor content on their networks.⁴³ Further, provisions under the IT Act and relevant rules, as well as under UAS Licenses allow the government to access records held by intermediaries.

Apart from this, the intermediaries are obliged to disclose information upon obtaining a 'lawful order' as per the Intermediaries Guidelines Rules. Rule 3(7) states that –

"...When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance."

The Rules do not clarify what constitutes a lawful order for the purpose of this obligation. However, the obligations under the Monitoring Rules for intermediaries to share personal information without a judicial order for the same is in violation of this principle, as violation of any of the provisions for sharing personal information would entail civil or criminal liability upon the intermediary.

(f) When drafting and enforcing their content restriction policies, intermediaries should respect human rights. Likewise, governments have an obligation to ensure that intermediaries' content restriction policies respect human rights.

There is no legal obligation upon intermediaries incorporate due process or any elements of procedural fairness into their content restriction enforcement policies. As such, intermediaries operating out of India vary in their use of methods and policies for content restriction. The Ranking Digital Rights India report highlights some examples of content

41 For an assessment of a sample of Indian intermediaries content restriction policies, see the Ranking Digital Rights in India report, Centre for Internet and Society, available at <https://cis-india.org/internet-governance/blog/ranking-digital-rights-in-india>.

42 Indranath Gupta, 'Are websites adequately communicating terms & conditions link in a browse-wrap agreement?', 3 European Journal of Law and Technology, 2, (2012), available at <http://ejlt.org/article/view/47>.

43 Centre for Internet and Society, 'State of Cyber Security and Surveillance in India', available at <https://cis-india.org/internet-governance/blog/state-of-cyber-security-and-surveillance-in-india.pdf>.

restriction policies of certain Indian intermediaries.⁴⁴ As per this data, Indian intermediaries largely do not adequately address human rights concerns of freedom of expression or privacy in their terms and conditions.

Recommendations

To be compliant with the principles outlined above, the following changes would need to happen in the Indian regime:

- Section 79 may be amended to require that, in any case where a content restriction is sought against an intermediary, the intermediary shall be made a necessary party to the proceedings.
- The Intermediary Guidelines Rules must be significantly amended in order to (1) delete the mandate for intermediaries to restrict and monitor certain content as per their terms of use; and (2) incorporate a due process requirement when dealing with content restriction requests based on the breach of terms of use.
- Rule 3(2) of the Intermediary Guidelines would need to be deleted, as intermediaries must not be compelled to include terms of service which restrict lawful content.
- Rule 3(5), which grants intermediaries the right to terminate its services to an end user on any violation of its terms of use, is also against this principle. The Rules must be amended to require intermediaries to follow transparent and fair practices in the enforcement of their terms of service. This would include an obligation to provide a fair hearing pursuant to a take down process for terms of service infringement, and provide an appellate mechanism for the resolution of grievances arising from this process. This procedure may be institutionalized under the Grievance Redressal Officer required to be appointed by intermediaries under Rule 11.
- In respect of intermediaries' obligation to share information with government agencies without a judicial order, it would require substantial amendments to the existing data protection and surveillance framework in India. With respect to intermediary liability, the obligations for data sharing upon government order imposed upon intermediaries under various Acts (and licenses) must be deleted, including under Rule 3(7) of the Intermediary Guidelines Rules. Substantive protections would likely have to be instituted through a comprehensive data protection regulation, which is currently being proposed by the Central Government.

Few regimes internationally have incorporated sufficient due process into their content restriction and intermediary liability framework. India should take the lead in developing a legal framework incorporating due process and transparency requirements between intermediaries and their users.

⁴⁴ Ranking Digital Rights in India report, Centre for Internet and Society, available at <https://cis-india.org/internet-governance/blog/ranking-digital-rights-in-india>.

Principle VI

Transparency
and
Accountability
must be built into
Laws
and
Content
Restriction Policies
and Practices

- a. Governments must publish all legislation, policy, decisions and other forms of regulation relevant to intermediary liability online in a **timely** fashion and in **accessible** formats.
- b. Governments must not use **extra-judicial measures** to restrict content. This includes collateral pressures to force changes in terms of service, to promote or enforce so-called “voluntary” practices and to secure agreements in restraint of trade or in restraint of public dissemination of content.
- c. Intermediaries should publish their content restriction policies online, in **clear language** and **accessible formats**, and keep them updated as they evolve, and notify users of changes when applicable.
- d. Governments must publish **transparency reports** that provide specific information about all content orders and requests issued by them to intermediaries.
- e. Intermediaries should publish **transparency reports** that provide specific information about all content restrictions taken by the intermediary, including actions taken on government requests, court orders, private complainant requests, and enforcement of content restriction policies.
- f. Where content has been restricted on a product or service of the intermediary that allows it to display a notice when an attempt to access that content is made, the intermediary must display a **clear notice** that explains what content has been restricted and the reason for doing so.
- g. Governments, intermediaries and civil society should work together to develop and maintain independent, transparent, and impartial oversight mechanisms to ensure the **accountability** of the content restriction policies and practices.
- h. Intermediary liability frameworks and legislation should require regular, systematic review of rules and guidelines to ensure that they are up to date, effective, and not overly burdensome. Such **periodic review** should incorporate mechanisms for collection of evidence about their implementation and impact, and also make provision for an independent review of their costs, demonstrable benefits and impact on human rights.

Recommendations

- The General Clauses Act, 1897 and the Right to Information Act, 2005, must be amended to ensure the timely and wide publication of all laws and rules.
- Provisions under Section 69A and other provisions, such as those under the Telecom Licenses must be made publicly available.
- The IT Act may be amended to include a provision for the systematic review of the Act as well as Rules and Regulations published under the Act.

- The requirement that intermediaries mandatorily include certain content restriction practices in their terms of service under Rule 3(2) of the Intermediary Guidelines Rules, must be deleted.
- In order to introduce transparency and accountability requirements, Rule 3(5), which ex facie allows intermediaries to restrict content or terminate services for breach of terms of service without following any due process requirements, should be deleted.
- Rule 3(1) may be amended to read that the rules and regulations, privacy policy and user agreement, published by the intermediary, must be in clear and accessible formats and be prominently displayed and be promptly notified to every user who accesses the intermediary's services, including any changes made to such rules and regulations, privacy policy or user agreement.
- A rule may be introduced to require intermediaries to give clear notice to any affected person attempting to access restricted content as to the law or provision of the terms of service under which the content was restricted, and the mechanisms available to such affected person to challenge such a decision.
- A specific obligation to publish aggregated information on content restriction requests may be included by inserting a Rule in the Intermediary Guidelines.
- The Rules may also be amended to ensure that sensitive or personal data is not revealed in the transparency report.
- Rule 16 of the Blocking Rules, Rules 23 and 25(4) of the Monitoring and Interception Rules would need to be amended to allow intermediaries to publish data on government content restriction or monitoring requests.
- An obligation to systematically review intermediary liability law is desirable.

Principle VI: Transparency and accountability must be built into laws and content restriction policies and practices

(a) Governments must publish all legislation, policy, decisions and other forms of regulation relevant to intermediary liability online in a timely fashion and in accessible formats.

In general, legislative enactments (Acts and Rules) are published in the Gazette of India, a weekly, official government digest, along with any rule, regulation, order, bye-law or notifications which may be required to be published in the Gazette of India. As per a decision of the Ministry of Law and Justice, all Gazette notifications are to be published only in electronic format. However, laws are often published in an ad-hoc manner and are not updated or are incomplete.⁴⁵

Consequently, accessibility to laws and rules published online suffers. There is no standard format for accessing various central or state laws. Moreover, the online publication of the laws are plagued with problems including illegibility or non machine-readability, making even those laws published online difficult to properly access. The lack of online access and machine readability also violates the government's duty to provide access to laws to persons with visual impairments who rely on the use of specific technologies for access to laws.

⁴⁵ Gaurav Vivek Bhatnagar, Centre Directed to Upload All Laws and Amendments on Official Website, THE WIRE, (May 29, 2016) available at <https://thewire.in/39335/centre-directed-to-upload-all-laws-and-amendments-on-official-website/>.

The decisions of the Government body under Section 69A and the Blocking Rules are not made public.

(b) Governments must not use extra-judicial measures to restrict content. This includes collateral pressures to force changes in terms of service, to promote or enforce so-called “voluntary” practices and to secure agreements in restraint of trade or in restraint of public dissemination of content.

The due diligence guidelines under Section 79 of the IT Act and notified under the Intermediary Guidelines Rules require the intermediaries to mandatorily issue terms of service which prohibit a wide and vague range of content. While the prescription that such content must be disabled upon actual knowledge of the same by the intermediary has been struck down by the Supreme Court in *Shreya Singhal*, the intermediaries are still expected to be in compliance with and enforce their own terms of service. Moreover, as discussed above, intermediaries have carte blanche to remove content or even terminate services for infraction of their terms of services.

(c) Intermediaries should publish their content restriction policies online, in clear language and accessible formats, and keep them updated as they evolve, and notify users of changes when applicable.

There is no legal obligation upon intermediaries in India to publish their content restriction policies, apart from the terms and conditions required to be published under the Intermediary Guidelines Rules.

(d) Governments must publish transparency reports that provide specific information about all content orders and requests issued by them to intermediaries.

The Indian Government does not publish transparency reports of content restriction or similar requests issued to intermediaries. While some data on content restriction has been made available through information requests made under the Right to Information Act, 2005,⁴⁶ Indian laws on content restriction through government orders (under the Blocking Rules) as well as laws on monitoring and requests for data from intermediaries (under the Monitoring Rules or the Reasonable Security Practices Rules) require intermediaries to maintain confidentiality regarding all such requests made by the government. These confidentiality requirements are vague, therefore, intermediaries are often hesitant about what sort of information may or may not fall under this legal censure. However, certain intermediaries do publish transparency reports, including Facebook⁴⁷ and Google,⁴⁸ usually as aggregate information about content restriction and user data requests from the government, without providing the specifics of the same.

(e) Intermediaries should publish transparency reports that provide specific information about all content restrictions taken by the intermediary,

46 Reply to RTI Application on Blocking of website and Rule 419A of Indian Telegraph Rules, 1951, Centre for Internet and Society (2013), available at <https://cis-india.org/internet-governance/resources/reply-to-rti-application-on-blocking-of-website-and-rule-419a-of-indian-telegraph-rules-1951>; RTI responses provide copies of Internet shutdown orders, Software Freedom Law Centre (2017), available at <https://www.legallyindia.com/views/entry/rti-responses-provide-copies-of-internet-shutdown-orders>.

47 Facebook Global Transparency Report, available at <https://transparency.facebook.com/>

48 Google Transparency Report, available at https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:IN

including actions taken on government requests, court orders, private complainant requests, and enforcement of content restriction policies.

There is no legal obligation upon intermediaries to publish transparency reports regarding actions taken in response to content restriction requests by governments or private complainants. In fact, as noted above, requests made by government authorities for content restriction or for access to data are required to be kept confidential by the intermediaries.

(f) Where content has been restricted on a product or service of the intermediary that allows it to display a notice when an attempt to access that content is made, the intermediary must display a clear notice that explains what content has been restricted and the reason for doing so.

In specific cases regarding court issued blocking orders to intermediaries for trademark or copyright offences committed by unknown third parties, the Bombay High Court has directed that the intermediaries (defendants in that dispute) must display a special default error page noting the specific offence under which the website has been ordered to be blocked, along with the details of the suit and the relief granted by the Court.⁴⁹ However, this requirement was restricted to the specific dispute and does not reflect a legal principle. Apart from this, there is no legal requirement for intermediaries to display a notice with details of the reason for content restriction under Indian law.

Under certain laws, including the Blocking Rules in India, content restriction requests must follow broad and vague confidentiality requirements, which prohibit publication of any details on the content restriction orders. A recently standardized HTTP protocol, HTTP Code 451 also attempts to introduce a technical standard whereby websites can identify when a website is unavailable due to a legal obligation to restrict content.⁵⁰ However, its actual usage among Indian intermediaries is not known.

(g) Governments, intermediaries and civil society should work together to develop and maintain independent, transparent, and impartial oversight mechanisms to ensure the accountability of the content restriction policies and practices.

There are few avenues for civil society, intermediaries and the government to work together in the development of oversight mechanisms. There is no industry best-practices framework particular to Indian intermediaries which has been adopted.

(h) Intermediary liability frameworks and legislation should require regular, systematic review of rules and guidelines to ensure that they are up to date, effective, and not overly burdensome. Such periodic review should incorporate mechanisms for collection of evidence about their implementation and impact, and also make provision for an independent review of their costs, demonstrable benefits and impact on human rights.

There has been no review of intermediary liability law in India. The IT Act was enacted in 2000 and substantive amendments were made in 2008. Subsequently, various rules, including the Intermediary Guidelines, have been enacted in a piecemeal manner. No general obligation to review legislation exists under Indian law.

49 Eros International Media Limited & Anr. vs Bharat Sanchar Nigam Limited Ors., Suit No. 751 Of 2016, (Order dt. August 12, 2016) available at <https://spicyip.com/wp-content/uploads/2016/08/TCL-order-in-Dishoom-12th-August-2016.pdf>.

50 'An HTTP Status Code to Report Legal Obstacles', Internet Engineering Task Force, available at <https://datatracker.ietf.org/doc/rfc7725/>.

Recommendations

While there are specific responsibilities upon the government to proactively publish laws, under the General Clauses Act, 1897 as well as the Right to Information Act, 2005, there are glaring lapses in the implementation of the mandate to make laws easily accessible to the general public. These laws may be suitably amended to ensure the timely and wide publication of all laws and rules.

Even though this report has recommended the deletion of provisions under Section 69A and other provisions, such as those under the Telecom Licenses, which allow government restriction of content without a judicial order, at the very least, such decisions must be made publicly available except for in exceptional circumstances as provided for by law. In addition, the IT Act may be amended to include a provision for the systematic review of the Act as well as Rules and Regulations published under the Act. This may take the form of a 'sunset clause' which would provide that the laws (including Rules) shall lapse unless specifically extended by way of legislative action.

The Intermediary Guidelines Rules must be comprehensively amended, as suggested above, in order for Indian laws to comply with these principles. In regard to Principle VI(b), the requirement that intermediaries mandatorily include certain content restriction practices in their terms of service (Under Rule 3(2)), must be deleted.

In order to introduce transparency and accountability requirements, the Intermediary Guidelines would have to be substantially amended. It is suggested that Rule 3(5) be deleted, which *ex facie* allows intermediaries to restrict content or terminate services for breach of terms of service without following any due process requirements. Further, Rule 3(1) may be amended to read as follows:

*"The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person. **Such rules and regulations, privacy policy and user agreement, must be published in a clear and accessible formats and be prominently displayed and be promptly notified to every user who accesses the intermediary's services, including any changes made to such rules and regulations, privacy policy or user agreement.**"*

Further, a rule may be introduced to require intermediaries to give clear notice to any affected person attempting to access restricted content as to the law or provision of the terms of service under which the content was restricted, and the mechanisms available to such affected person to challenge such a decision.

A specific obligation to publish aggregated information on content restriction requests may be included by inserting a Rule in the Intermediary Guidelines. This Rule may read as follows:

*"Rule 3(12) – **Transparency Report** –*

Every intermediary shall, on a bi-annual basis, publish a consolidated report of information on content restriction requests or orders received by it by way of (a) government orders, (b) orders of a competent judicial authority and (c) requests by a private party.

Unless specifically prevented by law or under such order, and without prejudice to the generality of Clause (1) above, this report must contain (a) the details of the content restriction request; (b) the action taken pursuant to the request and (c) an explanation as to why such an action was taken.

Where the intermediary is prohibited by law from publishing any of the information under Clause (2) above, it shall specify the applicable legal provision (or, in case of a judicial order, such order) prohibiting the same."

While the above clause presumes a strong data-protection framework forthcoming in India, the Rules may also be suitably amended to ensure that sensitive or personal data is not revealed in the transparency report, for example, by requiring anonymization of the data published.

While reporting and transparency requirements may allow intermediaries to publish information in respect of breach of their own terms of service, information relating to government requests for content restriction would require an amendment of various other laws prohibiting such disclosures. In particular, Rule 16 of the Blocking Rules, Rules 23 and 25(4) of the Monitoring and Interception Rules would need to be amended to allow intermediaries to publish data on government content restriction or monitoring requests.

An obligation to systematically review intermediary liability law is certainly desirable, particularly given the new issues thrown in by advancements in technology. There may be a clause which mandates the Act to be laid before parliament for review after the lapse of a period of time. Alternately, a 'sunset' clause may be introduced under the IT Act, which would provide for the Act to lapse upon a specific date unless it is reviewed and re-enacted.

Conclusion

Information Technology Act and Rules Amendments

- **Section 79** must be amended to address imposition of direct liability for failure to comply with certain conditions
- The regime for content restriction must be de-linked from the regime for intermediary liability
- Clear Procedures should be Defined
- Clear notice should be provided
- Principles of due process should be incorporated: **Rule 3(5)** of the Intermediaries Guidelines Rules must be repealed
- Restriction of content should be limited to content that has already been defined in law as illegal
- **Section 69A** of the Act, along with the Blocking Rules, must be repealed
- Criminal sanctions for the non-compliance with requirements under the IT Act must be repealed
- **Rule 16** of the Blocking Rules, **Rules 23** and **25(4)** of the Monitoring and Interception Rules are needed to be amended to remove restrictions on transparency of content restriction and information sharing requests
- **Rule 3(7)** of the Intermediaries Guidelines Rules must be repealed
- Mandatory periodic review of the IT Act and rules may be introduced

Copyright Act and Rules Amendments

- Provide for safe harbour for intermediaries under **Section 51(a)(ii)**
- The liability regimes under **Section 79** of the IT Act and **Section 51(a)(ii)** of the Copyright Act may be harmonized
- **Section 52(b)** and **(c)** of the Copyright Act as well as **Rule 75** of the Copyright Rules may be amended to require judicially determined orders for content restriction

The intermediary liability framework in India consists of a patchwork of statutes, rules and judicial orders, with significant lapses and interpretational issues. This report has indicated that the Indian intermediary liability framework is out of sync with the Manila Principles for Intermediary Liability, in several respects. The missteps with the Principles are attributable to the legal context and political requirements of the law, but also often simply unclear drafting and lack of foresight.

Throughout the paper, recommendations have been suggested to the legal framework for intermediary liability, which may bring the scheme of the law in compliance with the Manila Principles. These are summarized below:

1. Amendments to the Information Technology Act and Rules:

- **Section 79** must be comprehensively amended. The amendments must address the aspect of imposing direct liability for failure to comply with certain conditions. Similarly, the Intermediaries Guidelines Rules must be amended to provide for a notice-and-notice obligation for intermediaries. The Section should specify that any liability arising from failure to comply with this should be proportionate to the action.
- **The regime for content restriction must be de-linked from the regime for intermediary liability.** Section 79 should be amended to provide for a regime where intermediaries must respond to judicially reviewed orders for content restriction. The orders must be narrowly tailored to respond to the specific content at issue, including specifying, where possible, the temporal and geographical limitation of such restriction. Further, the orders must be passed after providing a right to hear the intermediary and the affected persons, except for in exceptional circumstances, including child pornography or incitement to violence.
- **Clear Procedures should be Defined:** The Intermediaries Guidelines Rules should be amended to provide for the procedure to be followed by intermediaries while complying with judicial orders, private requests or terms of service violations regarding content restriction. Such requirements should ensure that content restriction requests are not expansively implemented. The Guidelines should also require intermediaries to follow a bi-annual reporting mechanism to make public, at the minimum, aggregate numbers of requests for content restriction. The role of the Grievance Redressal Officer must be expanded to include a requirement to provide, wherever possible, a hearing to an affected person whose content is sought to be restricted for terms of service violations, with requirements to provide information on the grounds for restriction as well as appellate mechanisms for review.
- **Clear notice should be provided:** . Further, a rule may be introduced to require intermediaries to give clear notice to any affected person attempting to access restricted content as to the law or provision of the terms of service under which the content was restricted, and the mechanisms available to such affected person to challenge such a decision.
- **Principles of due process should be incorporated: Rule 3(5) of the Intermediaries Guidelines Rules must be repealed,** as it allows for the termination of a user's services without due process requirements being followed.
- **Restriction of content should be limited to content that has already been defined in law as illegal:** Further, Rule 3(2) must be amended to remove requirements for intermediaries to include and enforce terms of service under which certain legal content must be restricted.
- **Section 69A of the Act, along with the Blocking Rules, must be repealed.** The procedure for restriction of content should be clearly outlined as a part of Section 79 of the IT Act, which may include, *inter alia*, expedited judicial review.
- **Criminal sanctions for the non-compliance with requirements under the IT Act must be repealed.**
- **Rule 16 of the Blocking Rules, Rules 23 and 25(4) of the Monitoring and Interception Rules** would need to be amended to remove restrictions on transparency of content restriction and information sharing requests.
- **Rule 3(7) of the Intermediaries Guidelines Rules,** obliging intermediaries to share information upon administrative order, **must be repealed.**
- A provision for mandatory periodic review of the IT Act and rules, or, alternatively, a **'sunset' clause** may be introduced into the IT Act in order to mandate periodic review of the legislation and rules.

2. Amendments to the Copyright Act and Rules:

- **The Copyright Act must be amended** to include the definition of intermediaries, as defined under the IT Act, and **provide for safe harbour for intermediaries under Section 51(a)(ii).**
- **The liability regimes under Section 79 of the IT Act and Section 51(a)(ii) of the Copyright Act may be harmonized** by making specific reference that safe harbour for intermediaries under Section 79 shall be available to intermediaries under the Copyright Act.
- **Section 52(b) and (c) of the Copyright Act as well as Rule 75 of the Copyright Rules may be amended to require** judicially determined orders for content restriction. This may also be done through a reference to the amended IT Act as suggested above.

