CGG Working paper: Tackling the dissemination and redistribution of NCII[1]

1. Introduction

The dissemination and redistribution of non-consensual intimate images ("**NCII**") is a problem that has plagued platforms, courts, and lawmakers in recent years. NCII content may be shared on a variety of websites and online platforms, but the difficulty of restricting its spread is heightened on independent 'rogue' websites that are unresponsive to user complaints. Such unresponsiveness has prompted affected users to approach courts with lists of URLs where their NCII is located, seeking the blocking of these web-pages.[2] However, even when courts direct internet service providers ("**ISPs**") to block these URLs, the unlawful content often re-surfaces at different locations on the internet, compelling users to continually approach courts with updated lists of URLs.

Thus, the current regulatory approach has two deficiencies. First, it requires affected users to obtain a court order to remove or block content from websites which ignore their complaints, which may involve substantial expenditure and time. Second, the problem of *redistribution* of NCII at different locations persists even after URLs are blocked by a court. This working paper analyses these two issues and proposes a multi-stakeholder solution to NCII using a hash database maintained by an independent organisation or body ("**Independent Body**"). The proposed solution would allow affected users to have NCII content blocked by simply submitting URLs to a portal provided by the Independent Body. This is a far more convenient option for removal than going to court. Our solution also addresses the problem of redistribution on rogue websites by having the Independent Body crawl networks or clusters identified to host NCII and detecting 'known' NCII for eventual removal. We also list several safeguards that would prevent the inadvertent removal of lawful content.

2. Definition of NCII

Regulatory responses to NCII must begin with a stable definition of the proscribed content. For the purposes of the present working paper brief, we rely on the text of Section 66E of the Information Technology Act, 2000 ("**IT Act**") when describing and referring to NCII.[3]

Section 66E criminalises the intentional capture, publishing, or transmission of an image of a person's private area under circumstances violating their privacy and without their consent. 'Private area' is explained as naked or undergarment clad genitals, the pubic region, buttocks or breasts; 'publishes' means making publicly available in physical or electronic form; and 'circumstances violating privacy' means situations where individuals have a reasonable expectation that they can disrobe in private or that any part of their private areas would not be visible to the public (irrespective of whether at a private or public location).[4]

[1] Authored by Vasudev Devadasan, Aishwarya Giridhar, Shashank Mohan, Sachin Dhawan, and Jhalak M. Kakkar. For feedback or comments, please write to us at <ccg@nludelhi.ac.in>. We thank the National Law University Delhi for its support, without which this working paper would not have been possible.

[2] *See X v Union of India* WP (Cri) 1082 of 2020 (High Court of Delhi, 20 April 2021).

[3] We do not rely on Rule 3(2)(b) of the Intermediary Guidelines 2021 for several reasons. Firstly, it establishes a private complaint mechanism and does not render the content described therein per se unlawful. Secondly, Rule 3(2)(b) does not refer to content captured 'without consent' or 'in violation of privacy', essential to the definition of NCII. Thirdly, as a result, the rule may be used to remove content that may be mere nudity or lawful content that violates traditional mores. Finally, Rule 3(2)(b) is *prima facie* in contradiction with *Shreya Singhal v Union of India* 2015 (5) SCC 1.

[4] Information Technology Act, 2000 s. 66E (Explanation).

3. Distinguishing between varied intermediaries

Any regulatory approach to content governance online must recognise the heterogeneity in intermediary functionality and types of unlawful content. The proposed regulatory response involves four distinct types of intermediaries, and this section briefly explains the functionality they offer and how they may be best leveraged to ensure removal and restrict the redistribution of NCII.

The four types of intermediaries referenced in our proposed response are: (1) ISPs; (2) websites hosting third-party content; (3) social media platforms; and (4) search engines. Each of these intermediaries performs different functions:

- **ISPs**: connect their subscribers to the internet by supplying telecommunications facilities and equipment such as modems and last-mile connectivity.[5] ISPs do not ordinarily filter or examine the data that is transmitted on their networks,[6] nor can they interfere with the content by altering or removing the content they transmit. Thus, it is impractical to require ISPs to monitor and detect unlawful content. However, since they control their subscribers' access to the internet, they can block certain locations (URLs) on the internet if directed by a government or court order. This effectively prevents any of the ISPs' subscribers from accessing the URL. This may be particularly useful when websites refuse to remove unlawful content.

- **Websites hosting third-party content:** While some websites host their own content (eg, a news website), other websites allow third parties (eg, ordinary users) to upload content on their website. The latter type of website is an "intermediary" as it is hosting third-party content.[7] Websites may host thousands of pieces of third-party content, and may not always be aware that they are hosting NCII. However, a user may complain directly to a website (identifying NCII content). Because websites *host* the third-party content, unlike ISPs, they have the ability to *remove* any unlawful content at source. Removal at source is preferable to blocking by ISPs, as it ensures the deletion of the content for every user on the internet, irrespective of which ISP they use or which country they attempt to access the content from.[8]

- **Social media platforms**: are similar to websites hosting third-party content but may be distinguished by their size and efforts to curate the content their users see (and don't see). The Intermediary Guidelines recognises that social media platforms with more than five million subscribers in India (termed 'significant social media companies' or "**SSMIs**") are subject to heightened obligations *vis-à-vis* unlawful content.[9] Like websites (but unlike ISPs and search engines), SSMIs have control over third-party content on their platforms and can remove content at source if necessary. Further, SSMIs proactively detect unlawful content (including NCII) voluntarily because it is in their commercial interests to keep their platforms free of such

[5] Jaani Riordan, 'A Taxonomy of Internet Intermediaries' in Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) 38.

[6] ibid.

[7] Information Technology Act, 2000 s. 2(1)(w) defines an intermediary with reference to a piece of content as a person "*who on behalf of another person receives, stores or transmits*" that content or provides any service with respect to that content.

[8] Riordan J, 'Blocking Injunctions' in Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) 462.

[9] Intermediary Guidelines 2021, r. 2(1)(w), 2(1)(v), 4; Ministry of Electronics and Information Technology, Notification S.O. 942(E) dated 25 February 2021.

content.

- **Search engines:** do not themselves store and transmit content but allow users to locate and visit content. Search engines 'crawl' web-pages across the internet, extracting key-words and metadata to identify the type of content on these pages. Search engines then 'index' the extracted data to make it accessible for future use.[10] When a user submits a query, the search engine matches the query against pages in its index that likely have content useful to the user's query and displays them. Because search engines do not themselves host the content (such as NCII) on these pages, they cannot take down or remove unlawful content on websites. For the same reason, search engines cannot proactively detect unlawful content like SSMIs. However, they can 'de-index' (remove from the search engine's index) specific URLs. Once a webpage is de-indexed, traffic to the page can be expected to decline, as new users who do not know the page's exact URL are unlikely to find the page given the billions of webpages on the internet.[11]

The varied functionality of these intermediaries illustrates why mandating a single, uniform, approach to 'remove' NCII content for all the above intermediaries would be ineffective. Rather, a coherent regulatory approach should leverage the varied functionality of these intermediaries by requiring them to take steps to curb NCII where their functionality enables them to have maximum impact.[12]

4. Current regulatory deficiencies

The current regulatory regime suffers from two key deficiencies. First, in the case of websites that are unresponsive to user complaints about NCII, users have to approach courts to block web-pages hosting their NCII. Second, even after a series of URLs are blocked, the same NCII may resurface at different locations on the internet in the future, forcing users to re-approach courts with a new set of URLs.

(a) Difficulty in blocking 'rogue' websites

The dissemination of NCII may occur either on social media platforms, or on individual websites hosting third-party content. A user can complain directly to the relevant intermediary for removal of such content. An intermediary acting in a *bona-fide* manner would examine the complaint, determine whether it violates their terms of service, and if it does, would remove it in response to the user's complaint. Given that NCII is proscribed in a host of jurisdictions including India,[13] it is reasonable to expect a *bona-fide* intermediary's terms of service to prohibit their users from uploading or sharing NCII content. Thus, there is a high likelihood that such content will be removed voluntarily by an intermediary acting in a *bona-fide* manner.

However, intermediaries hosting NCII may also be unresponsive to such complaints for a variety of reasons such as: (i) lack of Grievance Officers, (ii) lack of content moderation capacity, (iii) belief that the risk of prosecution is remote, (iv) lack of concern over losing safe harbour, and (v) financial incentives such as advertising revenue derived from hosting NCII content.

[10] Riordan, 'A Taxonomy of Internet Intermediaries' (n 6) 44.

[11] Jaani Riordan, 'De-Indexing and Freezing Orders' in Jaani Riordan, *The Liability of Internet Intermediaries* (Oxford University Press 2016) 537.

[12] For example, network intermediaries such as ISPs that do not host or interfere with content are poorly placed to respond to user complaints for content removal, while application lawyer intermediaries such as websites and social media platforms are better placed to respond to such complaints. Further, there are several hundred ISPs operating in India, making it impractical to require users to complain to each one for each piece of content. However, if directed by a court or government order, ISPs can block content even when websites are unresponsive. Thus, different types of intermediaries offer users and lawmakers different resources to restrict the spread of NCII.

[13] Neris N, Ruiz JP and Valente MG, 'Fighting the Dissemination of Non-Consensual Intimate Images': (Internet Lab 2018) <http://www.internetlab.org.br/wp-content/uploads/2018/11/Fighting_the_Dissemination_of_Non.pdf>.

In such situations the current regulatory regime offers users very few options. Affected users may complain to search engines seeking the de-indexing of the relevant web-pages. But this still leaves the web-pages themselves unaffected. Consequently many users choose to apply for a court order directing ISPs to block the web-pages of the unresponsive sites, thus ensuring that the content is blocked irrespective of the websites' unresponsiveness to the user-complaint. Users are also entitled to initiate civil and criminal legal actions against such a website on the basis that it has lost safe harbour. Nonetheless such recourse to the courts is time consuming and expensive.

This is the first regulatory deficiency our proposal seeks to address.

(b) Problem of redistribution

Even where a court directs ISPs to block URLs at which NCII is located, it is possible that the same NCII content is re-uploaded at a different location on the internet. The content may be re-uploaded at a different location on the same website, or on a different website. For example, a court may direct an ISP to block 'www.abc.com/video1', but the originator may later re-upload the video at 'www.abc.com/video1a' or www.xyz.com/video1', circumventing the court order and perpetuating the spread of NCII content. In such situations, the user must once again approach the court, and request the court to block these new URLs at which the NCII content has been re-uploaded.

At this second juncture, the content has already been determined to be illegal and has been blocked by a court, but the user is compelled to approach the court a second or third time merely to secure a court order for identical content at different URLs. This represents a second regulatory deficiency, as users are compelled to continually approach courts to ensure their illegal content stays offline.

5. Incomplete or imperfect solutions

Several solutions have been proposed to address the issue of redistribution such as de-indexing by search engines and proactive monitoring for specific kinds of content by intermediaries. In our opinion, these approaches are flawed or incomplete.

De-indexing of content: As discussed above, where intermediaries are unresponsive to user complaints against NCII on their networks, users can complain to search engines and request the URLs associated with their NCII be de-indexed. While web-traffic to de-indexed websites can be expected to decline, this is an incomplete remedy as individuals who already possess the URL at which the NCII is located can continue to access and disseminate the NCII.[14] This remedy may be particularly ineffective where a key vector for dissemination is user-to-user sharing on messaging apps or groups dedicated to circulating proscribed content. Also, the problem of re-uploading remains. In addition to voluntary de-indexing, our proposal suggests that ISP blocking (facilitated through the Independent Body) should also be employed to more effectively restrict NCII.

Blocking entire websites: While 'rogue' websites discussed above may predominantly host explicit content, search engine de-indexing and ISP blocking should strictly be limited to URLs and not extend to blocking of entire websites. Blocking an entire website raises serious issues of proportionality as it presumes that *all content* on the website is illegal. Even in copyright contexts, Indian courts have been wary of blocking entire websites, laying down high thresholds that examine various factors such as whether the primary function of the website is to commit or facilitate

[14] Because search engines do not host the content, they can only remove the concerned web-pages from their index but cannot remove the actual content on websites or block access to such websites.

infringement.[15] Thus, merely because the NCII is located on a website that predominantly or exclusively hosts explicit content should not be a reason to block or de-index the website in its entirety. Until a detailed proportionality analysis along the lines established by Indian courts in copyright contexts has been conducted, blocking and de-indexing should be limited to specific URLs. Our proposal is strictly limited to individual URLs and does not contemplate the blocking of entire websites.

Proactive monitoring for NCII content: In 2021, a Single Judge of the Delhi High Court attempted to address the problem of re-uploading of known NCII by stipulating that *all* intermediaries must engage in the proactive monitoring and removal of NCII that the Court had previously determined to be illegal.[16] Such mandatory monitoring obligations create significant free speech and privacy risks as intermediaries must monitor *all* users to identify those uploading unlawful content.[17] Such automated filtering has also been demonstrated to disproportionately restrict lawful expression by individuals from racial and linguistic minorities.[18] Imposing a monitoring requirement on all intermediaries could lead to more content removal, but not necessarily *better* content removal, resulting in the removal of lawful speech. Therefore, curbing the redistribution of NCII requires a more nuanced approach.

6. Our Proposed solutions

We propose a *regulatory* solution; our recommendations are specifically directed at the problem of removal of NCII from unresponsive websites and the redistribution of known NCII at new locations on the internet. It is acknowledged that the exact technical implementation may require inputs from technologists and engineers. Also, our solution does not address the dissemination of NCII content over private communications between users on platforms that use end-to-end encryption.

The regulatory approach we suggest requires substantial multi-stakeholder commitment that will likely take time to formalise. It envisages bodies and structures that do not currently exist and will have to be developed pursuant to multi-stakeholder consultations. Nevertheless, our proposed model can coexist with and does not contradict the existing legislative and judicial remedies, since individuals can approach courts and platforms for the removal of NCII content.

In brief, we call for the creation of an independent organisation or body (the Independent Body) that can: (i) maintain a hash database of known NCII content; (ii) liaise with the government to directly block unresponsive web pages; (iii) adopt a multi-stakeholder approach to reporting and moderating NCII with vetted partner platforms, along the lines of existing efforts to curb CSAM; and (iv) assist victims by providing resources and proactively crawling for known NCII.

Short term possibilities

In the immediate future, we recommend that all major platforms, including search engines, adopt

[15] Other factors include: (1) whether the registration details of the website may be traced; (2) whether there has been inaction on behalf of the website; (3) whether the owner or operator of the website displays a disregard for copyright; (4) whether the website has been blocked in other jurisdictions; (5) whether the website contains instructions on how to circumvent blocking measures; (6) the volume of traffic on the website; (7) the availability of less onerous measures; and (8) the efficacy and dissuasiveness of measures which the ISP will have to adopt. See *Dept. of Electronics and Information Technology v Star India Pvt Ltd* FAO (OS) 57 of 2015 (High Court of Delhi, 29 July 2016); *UTV Software Communications Ltd v 1337x* CS (Comm) 724 of 2017 (High Court of Delhi, 10 April 2019).

[16] *X v Union of India* WP (Cri) 1082 of 2020 (High Court of Delhi, 20 April 2021) [90].

[17] Daphne Keller, 'Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling' (2020) 69 GRUR International 616.

[18] Duarte N, Llanso E and Loup A (2017) rep <https://cdt.org/wp-content/uploads/2017/11/Mixed-Messages-Paper.pdf> accessed November 17, 2022.

a token or digital identifier based approach to allow for the quick removal of previously removed or de-indexed content. Complainants can be assigned a unique token upon the initial takedown of NCII content. Subsequently, if the complainant were to detect their NCII at a new URL, they could submit the new URL with the token. Upon receipt, the search engine or platform would only need to check whether the URL contains the same content as content that had previously been taken down linked to that token. This would likely involve minimal human intervention and oversight and serve as a valuable pre-cursor to an independently managed hash database (discussed below).

Adoption of the token approach by search engines will help curb the prevalence of NCII even on independent 'rogue' websites, as traffic to such de-indexed URLs can be expected to decline.[19]

Long term multi-stakeholder recommendations

Our recommendations seek to reduce the burden on victims of NCII by: (a) reducing the time, cost, and effort users have to expend by going to court to remove or block access to NCII; (b) not requiring victims to re-approach courts for the blocking of redistributed NCII; and (c) providing administrative, legal, and social support to victims. The Independent Body and vetted partner platforms would also work together to improve the reporting and removal of NCII, drawing from current efforts by platforms and organisations maintaining a hash database to address CSAM.

First, we suggest a centralised complaint mechanism run by the Independent Body that can liaise with the Department of Telecommunications ("**DoT**") and the Ministry of Electronics and Information Technology ("**MeitY**") to ensure the rapid blocking of URLs hosting NCII.

Second, we suggest expanding on the hash-based technological model pioneered by Meta to tackle the removal of NCII (www.stopncii.org). We suggest a multi-stakeholder approach amongst platforms, civil society, the judiciary, and the government. Such a system would rely on the use of a hash database for NCII content, which would be maintained by the Independent Body. The rest of this section describes how these processes will work in tandem to curb the dissemination and redistribution of NCII content.

Use of a hash database and adding NCII content to it: We recommend setting up a hash database maintained by the Independent Body that victims can directly submit NCII content complaints to. Additionally, vetted technology platforms can also contribute NCII complaints to this database. A procedure to ensure that the hashes of NCII content blocked pursuant to a court order are also submitted to the Independent Body for vetting and inclusion in the database can be developed over time.

The use of a hash database coupled with a multi-stakeholder group has already been adopted with some success to combat CSAM, and it can potentially be adopted to tackle NCII.[20] This is similar to how CSAM is provided to the database maintained by the Internet Watch Foundation ("**IWF**").[21]

[19] Riordan, 'De-Indexing and Freezing Orders' (n 12) 537.

[20] David Thiel and Lisa Einstein, 'Online Consent Moderation' (Stanford Internet Observatory, 18 December 2020) <https://cyber.fsi.stanford.edu/io/news/ncii-legislation-limitations> accessed 20 October 2022.

[21] This is similar to how CSAM is provided to the database maintained by IWF, and would reduce the likelihood of non-NCII content being submitted to the database and ease the burden of vetting each piece of content for the IB, as we discuss below. See 'Hash List "Could Be Game-Changer" in the Global Fight against Child Sexual Abuse Images Online | IWF' <https://www.iwf.org.uk/news-media/news/hash-list-could-be-game-changer-in-the-global-fight-against-child-sexual-abuse-images-online/> accessed 18 November 2022.

Simply put, hashing generates and assigns a unique hash value (ie, a secure digital fingerprint) to an instance of NCII. For example, if a user complains about a piece of NCII, the content is verified as NCII and hashing technology scans the properties of the content and assigns it a specific hash value (eg, '*123456*'). The hash value is thus a numeric representation of the NCII content and is unique to each piece of content. This hash value is then added to a database of known NCII content. Subsequently, content that is suspected of being NCII can be hashed; if the hash-value generated from the suspected content matches the hash-value of known NCII in the database, the two pieces of content are identical as they have identical properties. It can thus be deduced that the second suspected content is also NCII. Individuals in possession of the hash-value cannot reverse engineer the content, thus a hash-database poses a lower security risk than storing the actual unlawful content.

Such a model would require the vetted technology platforms and Independent Body to identify, store, and transmit NCII content, which could open them up to liability under the IT Act. Legal exemptions or special permissions would therefore have to be provided to the vetted technology platforms as well as the Independent Body, to enable them to identify and transmit NCII content for specific purposes related to the removal of NCII.

On receiving submissions or complaints, multiple experts within the Independent Body would vet each piece of content to ensure that it is NCII - as per Section 66E of the IT Act - before it is hashed and included in the database. We recommend that a model similar to what is currently followed for CSAM is adopted,[22] and that every hash is independently verified to contain NCII by multiple human reviewers strictly on the basis of documented criteria. The Independent Body would also have to incorporate stringent safeguards and data security protocols to protect the privacy of the individuals involved.

There may be circumstances where content submitted to the Independent Body has substantial free speech or public interest value, requiring a balance to be struck between public interest, speech, and privacy considerations. For example, the NCII may depict a public figure engaged in wrongdoing, who then submits the content to the Independent Body for removal. In such cases, where public interest, free speech, and privacy considerations need to be balanced, the Independent Body should not be required to add content to the database given that judicial proceedings would be the more appropriate process.

Functions of the Independent Body: As noted above, the Independent Body would be responsible for maintaining the hash database of NCII content, and vetting submitted content before inclusion into the database.

Since each hash on the database maintained by the Independent Body would have been vetted by multiple experts to confirm that it pertains to NCII, the Independent Body could also work with the DoT to direct ISPs to block access to specific web pages containing NCII. This would be particularly effective where 'rogue' websites do not remove NCII content pursuant to user complaints. By creating a centralised complaint form and liaising with the DoT to block webpages, the Independent Body would drastically reduce the burden on victims, since they would not have to obtain a court order for blocking each instance of NCII, particularly where the same content has been re-uploaded on multiple unresponsive websites over a period of time.

To further reduce the burden on victims, the Independent Body could also be given a mandate to

[22] 'How Image Hashing Technology Helps NCMEC - Google Safety Center' <https://safety.google/stories/hash-matching-to-help-ncmec/> accessed 18 November 2022; 'Hash List "Could Be Game-Changer" in the Global Fight against Child Sexual Abuse Images Online | IWF' <https://www.iwf.org.uk/news-media/news/hash-list-could-be-game-changer-in-the-global-fight-against-child-sexual-abuse-images-online/> accessed 18 November 2022.

search for, or use a web crawler to proactively detect copies of previously hashed NCII. It can also work with NCII victims towards identifying repeat instances of NCII. For example, in the context of CSAM, the IWF employs a proactive web-crawler that crawls the web in a targeted manner to locate CSAM content (by matching it against an existing hash database).[23] Deployed in a targeted manner against networks or clusters of websites identified to regularly host NCII pursuant to a risk assessment, such efforts would reduce the risk of redistribution at no effort or cost to victims. As noted previously, the Independent Body would need to be provided with a statutory exemption allowing it to look for, identify, transmit, and store NCII content to perform its functions given the illegality of NCII content under Section 66E of the IT Act.

To provide additional support to individuals, the Independent Body could work with organisations that would provide social, legal, and administrative support to victims of NCII. It would also be able to coordinate with intermediaries, law enforcement, and regulatory agencies in investigating and facilitating the removal of NCII online.

Structure and independence of the Independent Body: The Independent Body would have to be independent of both intermediary and governmental influence. This is to ensure the accuracy and transparency of content reported by intermediaries, and to protect against the expansion of categories of content that the hash database is used for (safeguards to guard against this possibility are discussed below). A robust vetting process by the Independent Body is essential to ensure that only NCII, and no other content is included in the database. This is especially important since vetted technology partners and individuals are able to submit content to the database.

The method of funding the Independent Body would have significant implications for its independence. A method similar to the one used by IWF, where members (or in this case, technology platforms vetted by the Independent Body) pay a fee to the Independent Body may be adopted.[24]

It is also essential to institute mechanisms to ensure that the Independent Body is accountable to multiple stakeholders. This can be addressed through periodic transparency reporting and audits. Transparency reporting would ideally be directed to multiple stakeholders such as the public, Parliament, and trusted partners, and include information on metrics such as: (a) the total number of reports of NCII received from both complainants and trusted partners; (b) outcome of the reports (that is, whether they were subsequently included in the database, which could also provide insight into error rates in content reporting by trusted partners); and (c) whether the NCII content was blocked by ISPs (providing an indication of the effectiveness of DoT coordination).

Periodic independent audits of the hash database and its management, audits of the data protection measures instituted by the Independent Body, and independent verification of the tools used by the Independent Body to detect and report NCII content would also foster accountability in the Independent Body.

Need for safeguards: We recognise that the proposal described above could pose significant free speech risks, particularly if this regulatory logic is extended to other forms of unlawful speech (eg, it could lead to governments creating a hash database of politically unfavourable content and direct

[23] 'Web Crawler from the Internet Watch Foundation' (*Internet Watch Foundation*) <https://www.iwf.org.uk/our-technology/crawler/> accessed 20 October 2022.

[24] 'Membership Pricing | IWF | IWF' <https://www.iwf.org.uk/membership/fees/> accessed 18 November 2022.

intermediaries to take down all instances of such content). However, we note that unlike other types of online expression such as copyright, defamation, and hate speech, the illegality associated with the vast majority of NCII content can be determined with a high degree of certainty by a body such as the Independent Body. Further, we propose several safeguards.

First, the charter and statutory exemptions for the Independent Body should expressly state that the hash database may only be used for NCII content. Another, more rigorous proposal could be the imposition of penal or financial sanctions on key functionaries of the Independent Body if the database or technology is used for any content beyond NCII. Second, all entries to the database would be vetted by multiple human reviewers from the Independent Body. This is to ensure that: (i) human input is used to verify that the hash database is limited to NCII, to guard against over removal of content; and (ii) the operation of the database is not subject to external or governmental influence, since the reviewers would be employed by the Independent Body and free from external influence. Third, as noted above, any content requiring public interest, privacy, and free speech considerations to be balanced would not be included into the database and would instead be subject to judicial proceedings. Fourth, the Independent Body would be subject to transparency and accountability safeguards described above, to ensure that the database is limited to NCII and that the Independent Body is operating as intended.

Fifth, vetted technology partners would only submit NCII content that they have chosen to remove for violating their terms of service. Sixth, the Independent Body would be required to conduct a risk impact assessment (for potential harms to free expression and privacy) prior to conducting targeted crawling exercises. Finally, intermediaries would not be legally required to contribute to the database.

Summary of recommendations

Our core recommendations are summarised below. As noted previously, our intent is to propose a regulatory solution to a complex socio-legal problem. Our recommendations seek to effectively address the dissemination of NCII through a multi-stakeholder approach. The proposed model seeks to reduce the administrative burden of seeking the removal of NCII for victims, while guarding against the pitfalls of using proactive monitoring tools for speech on platforms.

- Efforts should be made towards setting up an independently maintained hash database for NCII content.
- The hash database should be maintained by the Independent Body and it must undertake stringent vetting processes to ensure that only NCII content is added to the hash database.
- Individuals and vetted technology platforms should be able to submit NCII content for inclusion into the database; NCII content removed pursuant to a court order can also be included in the database.
- The Independent Body may be provided with a mandate allowing it to proactively crawl the web in a targeted manner to detect copies of identified NCII content pursuant to a risk impact assessment. This will substantially shift the burden of identifying NCII from victims.
- The Independent Body can supply the DoT with URLs hosting known NCII content, and work with victims to alleviate the burdens of locating and identifying repeat instances of NCII content.
- The Independent Body should be able to work with organisations to provide social, legal, and administrative support to victims of NCII; it would also be able to coordinate with, law enforcement, and regulatory agencies in facilitating the removal of NCII.

About the Centre for Communication Governance

The Centre for Communication Governance (CCG) was established at one of India's premier legal institutions, the National Law University, Delhi in 2013. CCG is India's only academic research centre which is dedicated to working on information technology law and policy. Its central aim is contributing towards improved governance and policymaking across relevant disciplines. CCG undertakes academic research, provides policy input, and facilitates capacity building of relevant stakeholders in the ecosystem. CCG works on areas such as cybersecurity, platform governance, governance of emerging technologies, and privacy and data governance. CCG uses its research to engage meaningfully with both domestic and international policy-making processes by participating in public consultations, engaging with relevant parliamentary and international committees/working groups.

About the National Law University Delhi

The National Law University Delhi established in 2008 (by Act. No. 1 of 2009) is a premier Law University established in the capital city of India. Dynamic in vision and robust in commitment, the University has shown terrific promise to become a world-class institution in a very short span of time. It follows a mandate to transform and redefine the process of legal education. The primary mission of the University will be to create lawyers who will be professionally competent, technically sound and socially relevant, and will not only enter the Bar and the Bench but also be equipped to address the imperatives of the new millennium and uphold Constitutional values. The University aims to evolve and impart comprehensive and interdisciplinary legal education which will promote legal and ethical values, while fostering the rule of law.