CENTRE FOR COMMUNICATION GOVERNANCE AT
NATIONAL LAW UNIVERSITY, DELHI

Response to Call for Submission on Online Violence Against Women

Prepared by Arpita Biswas with inputs from Chinmayi Arun

Summary of Best Practices

- *Section 66E of the Information Technology (Amendment) Act, 2008 and Section 354C of the Indian Penal Code criminalize the sharing of private pictures of women, without their consent. These provisions focus on the consent of women, and do not attempt to censor legitimate sexual expressions.*

Introduction

Online violence against women and its associated harms have been increasingly recognized and acknowledged over the past few years. The UN General Assembly has remarked on this growing concern in reports and has adopted resolutions to this extent.[1] One of their latest resolutions titled the *'Intensification of efforts to prevent and eliminate all forms of violence against women and girls: domestic violence'* was adopted in 2016. This resolution addresses the risks of cyber-bullying and stalking and the role online crimes play in enabling domestic violence as well.[2]

In response to the call for submissions issued by the Special Rapporteur on violence against women, we at the Centre for Communication Governance would like to submit this note, highlighting good practices in India and our evaluation of ways in which they might be enhanced. This submission also flags concerns with the legislative framework in India relating to online violence against women, along with problems emerging in the context of intermediary liability and measures adopted by private platforms to combat such violence, to highlight areas of concern that must be noted in the context of good practices.

Our submission makes references to two working papers authored at the Centre for Communication Governance. The first paper is titled *Protecting Women's Rights Online: Required Legislative Measures and Other Recommendations* (referred to as 'Women's Rights Online') and it analyses issues with online violence against women, focusing on cyber-harassment, cyber-stalking and revenge porn. This paper has been drafted as a part of an ongoing project the Centre is working on, and will be submitted to the Ministry of Electronics and Information Technology, Government of India. The second paper deals with the issue of non-consensual intimate imagery (referred to as 'NCII paper') and addresses the growing problems relating to the creation and use of non-consensual intimate imagery and the legislative and administrative problems surrounding the phenomena in India.

---

[1] United Nations, General Assembly, *Report of the Working Group on the issue of discrimination against women in law and in practice*, A/HRC/23/50 (19 April 2013), http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.50_EN.pdf.

[2] General Assembly Resolution 71/170, *Intensification of efforts to prevent and eliminate all forms violence against women and girls: domestic violence*, A/RES/71/170 (19 December 2016), https://digitallibrary.un.org/record/858763/files/A_RES_71_170-EN.pdf.

Part I of this submission discusses the legislative framework in place in India to prohibit online violence against women. Part II discusses the role private platforms play in enabling online violence. Part III extracts good principles and practices from Parts I and II for the Special Rapporteur's reference. Part III also details recommendations in the context of the legislative framework and the role of private platforms laid out in Part I and Part II.

1. Legislative framework

There are two statutes that are applicable to acts of online violence against women in India. *First*, the Indian Penal Code ('IPC') and *second*, the Information Technology Act (the 'IT Act'). We discuss both below:

1.2. Information Technology Act, 2008

The IT Act contains law that addresses online violence against women. The first sub-part discusses the now repealed Section 66A – this provision criminalized a wide range of 'offensive' messages. The second sub-part discusses Section 66E which deals with the transmission of intimate images, and is applicable in instances of non-consensual intimate images ('NC images'). The third sub-part discusses the relevance Section 67 and 67A, which prohibits the publication or transmission of obscene material, similar to Section 292[3] of the

[3] Section 292 of the IPC:
Sale, etc., of obscene books, etc.—
(1) For the purposes of sub-section (2), a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the pruri-ent interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt person, who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.
(2) Whoever—
(a) sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever, or
(b) imports, exports or conveys any obscene object for any of the purposes aforesaid, or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation, or
(c) takes part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene objects are for any of the purposes aforesaid, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or
(d) advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be procured from or through any person, or
(e) offers or attempts to do any act which is an offence under this section, shall be punished 263 [on first conviction with im-prisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with

IPC. The fourth sub-part discusses Section 69A and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, which lay down the procedure for blocking content, including NC images, in India.

a. Section 66A (repealed)

Section 66A of the IT Act, 2000, was introduced in the year 2008[4]. This provision was concerned with information that was 'grossly offensive' or that which had a 'menacing character', it was also concerned with information transmitted '*for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will'*.[5] Section 66A was also intended to fight sexual harassment online.[6] This provision was criticized for being broadly-worded and prior to its repeal, had led to people being arrested for Facebook posts, and in some instances, for merely liking Facebook posts.[7]

---

imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees].

[4] Statement of Objects and Reasons, Information Technology (Amendment) Act, 2008 as referred to in ¶ 3:
"A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal Code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes."

[5] Section 66A - Punishment for sending offensive messages through communication service, etc.
Any person who sends, by means of a computer resource or a communication device, —
(a) any information that is grossly offensive or has menacing character; or
(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,
(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,
shall be punishable with imprisonment for a term which may extend to three years and with fine.
Explanation.— For the purpose of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message.

[6] Danish, *Dear Sibal, here is why section 66A does not 'protect' women*, Firstpost Tech, (December 12 2012) ,http://tech.firstpost.com/news-analysis/dear-sibal-here-is-why-section-66a-does-not-protect-women-212326.html.

[7] PTI, *Two Mumbai Girls arrested for Facebook post against Bal Thackeray get bail*, India Today, (November 19 2012), http://indiatoday.intoday.in/story/2-mumbai-girls-in-jail-for-tweet-against-bal-thackeray/1/229846.html; A Srinivasa Rao, *PUCL leader Jaya Vindhyala sent to judicial custody for objectionable Facebook post on Tamil Nadu governor K. Rosaiah*, India Today, (May 13 2013), http://indiatoday.intoday.in/story/pucl-leader-jaya-vindhayala-remanded-judicial-custody-objectionable-posts-tn-governor-india-today/1/270867.html

In 2015, a landmark judgment concerning free speech and intermediary liability was passed. In *Shreya Singhal vs. Union of India*[8], the Supreme Court of India struck down Section 66A for its over-breadth and held that it was unconstitutional. The *Shreya Singhal* judgment also strengthened the intermediary liability regime, by mandating government notices for blocking online content.[9]

As stated above, Section 66A was also found to be over-broad to the extent that it interfered unreasonably with the exercise of the right to freedom of expression.

b. Section 66E

Section 66E[10] criminalizes the publication or transmission of images *"of any private area of a person without his or her consent, under circumstances violating the privacy of that person".*

This provision is applicable to instances where 'non-consensual intimate imagery' is shared. This phenomenon is informally referred to as 'revenge porn'. Authors like Halder & Jaishankar[11] and Citron & Franks[12] have remarked on the dangers of NC images. Citron and Franks define the act as one which

"*involves the distribution of sexually graphic images of individuals without their consent. This includes images originally obtained without consent (e.g., hidden recordings or recordings of sexual assaults) as well as images originally obtained with consent, usually within the context*

[8] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
[9] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
[10] Section 66E. Punishment for violation of privacy- Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both
Explanation - For the purposes of this section--
(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;
(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;
(c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;
(d) "publishes" means reproduction in the printed or electronic form and making it available for public;
(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that--
(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.
[11] Debarati Halder & K. Jaishankar, *Revenge Porn by Teens in the United States and India: A Socio-legal Analysis*, 51(1-2) INTERNATIONAL ANNALS OF CRIMINOLOGY 85–111 (2013).
[12] Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, WAKE FOREST LAW REVIEW 49 (2014).

of a private or confidential relationship (e.g., images consensually given to an intimate partner who later distributes them without consent, popularly referred to as 'revenge porn'."[13]

Section 66E prohibits both, the production of and dissemination of non-consensual intimate imagery. Quoted below is an excerpt from our paper on Women's Rights Online which lays down the different stages:

"Section 66E uniquely recognizes the multi-layered nature of consent.[14] *That is, firstly, consenting to the recording or publication of images/videos; and after having consented to such capturing of images/videos, secondly, consenting to the distribution of such content.*

We would therefore recommend Sector 66E as an example of a model law to cope with certain forms of online violence against women.

c. Section 67, 67A

Section 67 and 67A of the Information Technology Act, 2000 criminalizes the publication or transmission of 'obscene material'. The definition of 'obscene' in these provisions is similar to Section 292 of the IPC. Section 292 of the IPC adopts Hicklin's test of obscenity, a standard for determining obscenity that has since been disregarded by the Supreme Court, in favour of the 'community standards' test. [15]

These provisions are still based on Hicklin's test of obscenity. They have been criticised in our paper on Women's Rights Online, which has been quoted below:

"The object of Sections 67 and Sections 67A is, however, not specifically to dis-incentivize or prohibit cyber harassment. These penal provisions seek to stem the circulation of material which is "lascivious or appeals to the prurient interest or tends to deprave or corrupt persons" or which contains "sexually explicit acts or conduct". This archaic legislative formulation of "obscenity" has been extensively criticized for its ambiguous and moralistic tone, which allows

[13] *Ibid.*, Page 12.
[14] Richa Kaul Padte, *Keeping Women Safe? Gender, Online Harassment and Indian Law*, Economic and Political Weekly, Vol. XLVIII No. 26 & 27 (June 29, 2013), pp. 35-40; at 37.
[15] Aveek Sarkar vs. State of West Bengal, (2007) 1 S.C.C. 143 (India).

for a great deal of interpretative subjectivity in courts.[16] *Further, these sections are limited in their application to cyber sexual harassment as they are applicable only to content which meets the requirements of "obscenity" as evolved by courts.* [17]*"*

The language used in Section 67 and Section 67A has been known to limit legitimate sexual expression as well. Unfortunately, the Indian legal framework relies heavily on phrases of this nature. Commenting on this phenomenon, the J.S. Verma Committee Report remarked upon the 'euphemisms of misplaced morality' that laws surrounding sexual assault and rape support.[18] To illustrate, under Section 67 and 67A, women can be punished for producing intimate or sexual images of themselves, akin to 'sexting'.[19] This shows that the law has the effect of conflating legitimate and illegitimate forms of sexual expression.[20] Our recommendation would be to avoid language of this nature.

d. Section 69A

Section 69A of the IT Act[21] read along with Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 constitute the content blocking system in India. This law enables the state to block online content in India.

---

[16] For a more detailed discussion on this, see Richa Kaul Padte, *Keeping Women Safe? Gender, Online Harassment and Indian Law*, Economic and Political Weekly, Vol. XLVIII No. 26 & 27 (June 29, 2013), pp. 35-40. Also see, Anita Gurumurthy & Nivedita Menon, "Violence against Women via Cyberspace", *Economic and Political Weekly*, Vol. XLIV No. 40, October 3, 2009, pp.19-21.

[17] *Ibid.*

[18] Retd. Justice J.S. Verma and Retd. Justice Leila Seth, *Report of the Committee on Amendments to Criminal Law*, (January 23 2013), ¶46.

[19] *See generally* AMY ADELE HASINOFF, SEXTING PANIC: RETHINKING CRIMINALIZATION, PRIVACY AND CONSENT (Feminist Media Studies, University of Illinois Press) (2015).

[20] *Refer to* Ratna Kapur, *Law and the Sexual Subaltern: A Comparative Perspective*, 48 Clev. St. L. Rev. 15 (2000), http://engagedscholarship.csuohio.edu/clevstlrev/vol48/iss1/4.

[21] Section 69A: Power to issue directions for blocking for public access of any information through any computer resource—
(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2) for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.
(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.
(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

Under this system, private individuals can send complaints to 'nodal officers'[22], who forward these complaints to 'designated officers', once they are satisfied with its legitimacy.[23] A designated committee reviews blocking requests forwarded by the designated officer.[24] Their report is then sent forward to the Secretary of the Department of Information Technology, who can pass interim directions to block access to harmful information.[25] There is also a process through which emergency requests can be made to the Secretary of the DoT, without having to go through the preliminary stages.[26] Content blocking orders are confidential.[27]

Certain aspects of the system, like the afore-mentioned confidentiality lead to opacity of what is essentially a censorship system. In addition, there is scarce information in the public domain about the exact nature of the content blocked by the state using section 69A.[28] Although judicial review is possible in theory, the opacity of this system means that users who wish to challenge blocking of online content - that they have a right to access, would not have any information about whether and why this content was blocked.[29] This system therefore lends itself to abuse and over-blocking.[30] Transparency and accountability are necessary in this context.

1.3. Indian Penal Code, 1860

[22] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 6.
[23] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 5.
[24] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 7.
[25] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 8(5).
[26] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 9.
[27] Chinmayi Arun and Sarvjeet Singh, *NOC Online Intermediaries Case Studies Series: Online Intermediaries in India*, (February 18 2015), Centre for Communication Governance, National Law University, Delhi, http://ccgtlr.org/wp-content/uploads/2015/02/CCG-at-NLUD-NOC-Online-Intermediaries-Case-Studies.pdf, Page 24.
[28] Chinmayi Arun and Sarvjeet Singh, *NOC Online Intermediaries Case Studies Series: Online Intermediaries in India*, (February 18 2015), Centre for Communication Governance, National Law University, Delhi, http://ccgtlr.org/wp-content/uploads/2015/02/CCG-at-NLUD-NOC-Online-Intermediaries-Case-Studies.pdf, Page 24-25.
[29] Chinmayi Arun and Sarvjeet Singh, *NOC Online Intermediaries Case Studies Series: Online Intermediaries in India*, (February 18 2015), Centre for Communication Governance, National Law University, Delhi, http://ccgtlr.org/wp-content/uploads/2015/02/CCG-at-NLUD-NOC-Online-Intermediaries-Case-Studies.pdf, Page 24-25.
[30] Chinmayi Arun and Sarvjeet Singh, *NOC Online Intermediaries Case Studies Series: Online Intermediaries in India*, (February 18 2015), Centre for Communication Governance, National Law University, Delhi, http://ccgtlr.org/wp-content/uploads/2015/02/CCG-at-NLUD-NOC-Online-Intermediaries-Case-Studies.pdf, Page 24-25.

The Indian Penal Code is also applicable to online violence against women.

The first sub-part of this part discusses the applicability of Section 354C which criminalizes voyeurism and NC images. This sub-part also briefly discusses Section 503, Section 507 and Section 509.

a. Section 354C

Section 354C was introduced through the Criminal Law Amendment of 2013. This amendment was introduced in the aftermath of the 'Delhi rape case', which set in motion massive changes in the legal framework relating to sexual harassment.[31]

Section 354C of the IPC is applicable in instances of voyeurism and could also extend to instances of non-consensual intimate imagery being distributed.[32]

Explanation 2 of Section 354C[33] addresses non-consensual intimate imagery and makes the provision relevant in instances of NC images. The explanation reads as follows:

"Where the victim consents to the capture of the images or any act, but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered an offence under this section".

1.4. Challenges in securing justice – Issues faced in the aftermath of online violence

Our research indicates that two factors contribute to challenges in securing justice in the aftermath of online violence. *First*, online violence against women does not appear to have

---

[31] Richa Kaul Padte, *Keeping Women Safe? Gender, Online Harassment and Indian Law*, Economic and Political Weekly, Vol. XLVIII No. 26 & 27 (June 29, 2013), pp. 35-40; at 37.

[32] Section 354C of the IPC:
Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine

been a priority technology policy consideration. Policy frameworks like the National Cyber-Security Policy[34] and the 12th Five-Year Plan on the Information Technology Sector do not prioritize online violence against women as a policy consideration.[35] Policy documents dealing with women's issues, like the Draft National Policy for Women 2016[36], also do not adequately address these issues.

Second, there are several shortcomings in the criminal justice system. These include barriers to reporting of crimes, a reluctance of authorities to intervene and ancillary infrastructural issues.[37] Victims of sexual abuse are often reluctant to come forth with complaints. The tedious task of filing a complaint or having to go through a rigorous judicial process could lead to 'secondary victimization'.[38] With regard to online crimes, this issue is amplified since women in India tend to be less technologically adept than women in countries like the US, UK and Germany.[39]

In the event that law of this nature is seen as model legislation, this should ideally be accompanied by an examination of the institutions that implement such laws. The law should also be accompanied by a strategy that promotes awareness, and audits legal institutions to ensure that complainants are reasonably able to access justice.

2. Online violence on private platforms

[33] National Cyber Security Policy 2013, Ministry of Electronics and Information Technology, http://meity.gov.in/sites/upload_files/dit/files/National_cyber_security_policy-2013(1).pdf
[34] 12th five-year plan on information technology sector, Report of sub-group on cyber-security, Ministry of Electronics and Information Technology, http://meity.gov.in/sites/upload_files/dit/files/Plan_Report_on_Cyber_Security.pdf
[35] Draft National Policy for Women 2016, Issued by the Ministry of Women and Child Development (May 2016), ¶6(iii), http://wcd.nic.in/sites/default/files/women%20empowerment%20poliy_Final_17May.pdf.
[36] Part II, Women's Rights Online paper - *Protecting Women's Rights Online: Required Legislative Measures and Other Recommendations.*
[37] Debarati Halder and K. Jaishankar, Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of the United States, the UK, and India, An International Journal of Evidence-based Research, Policy, and Practice, Volume 6, 2011 - Issue 4: Comparative Victim and Offender Research, Part 2: Cross-National and Cross-Cultural Findings from around the World.
[38] The Boston Consulting Group, Retailers Association of India, *Decoding Digital @ Retail – Winning the Omnichannel Consumer* (February 2016), http://image-src.bcg.com/BCG_COM/Decoding-Digital-Retail-Feb-2016-India_tcm21-28732.pdf.

Social media platforms like Facebook, Twitter and YouTube have been criticized for enabling online violence against women, and for not taking adequate measures against perpetrators.[40] Twitter is most often used to perpetrate mass attacks against select individuals. This act is referred to as 'trolling' and is an oft-used weapon of sexual harassment.

Facebook has certain 'community standards' in place, which lay down guidelines relating to prevent hate speech, racism and sexual violence, amongst several others forms of harmful speech.[41]

2.1. Measures taken by private platforms

This sub-part outlines mechanisms and initiatives adopted by Facebook and Twitter to curb online violence against women.

a. Twitter

Twitter has a reporting mechanism in place, through which users can report abusive behavior. Under the rules formulated, 'abusive behaviour' includes 'violent threats, targeted harassment, hateful conduct which promotes violence or threatens people on the basis of various factors including gender, gender identity and sexual orientation, publication of other people's private and confidential information and impersonation'[42].

This platform's ability to effectively regulate content has been under immense scrutiny of late. In 2016, Facebook, Twitter and Microsoft signed a voluntary Code of Conduct against Hate Speech, which required the regulation of 'a majority' of hate speech and extremist content within 24 hours.[43] As per an evaluation published in 2016, Twitter was lagging behind Facebook and Microsoft, by reviewing merely 23.5% of its reported content, while the requirement was 50%.[44] These statistics only refer to instances of hate speech and online

[39] Jack Linshi, *Report gives Facebook, Twitter, YouTube, an 'F' in handling harassment* (September 16 2014), TIME, http://time.com/3387979/twitter-youtube-facebook-user-abuse/.
[40] Community Standards, Facebook, https://www.facebook.com/communitystandards.
[41] The Twitter Rules, Twitter, https://support.twitter.com/articles/18311.
[42] Amar Toor, *Facebook, Twitter, Google, and Microsoft agree to EU hate speech rules* (May 31 2016), The Verge, https://www.theverge.com/2016/5/31/11817540/facebook-twitter-google-microsoft-hate-speech-europe
[43] *Ibid.*

extremism, but they shed light on Twitter's ability and inclination to effectively regulate content.

b. Facebook

As mentioned above, Facebook has certain Community Standards in place, which are available to the public. Recently, the guidelines by which Facebook internally regulates content, were allegedly leaked.[45] The Guardian has uploaded these documents, titled the 'Facebook Files'.[46] Quoted below is an excerpt from our Women's Rights Online paper, which sheds light on the leaked guidelines relating to sexual exploitation and non-consensual intimate imagery:

"As a part of these documents, their comprehensive policy on moderating 'sextortion' and 'revenge porn' came to light.[47] The files state that 'sexual policy' is one of the hardest to follow, because consent is not always evident from pictures relating to non-consensual pornography. However, image matching and detecting software is routinely used by the platform, where images that have already been flagged as problematic or illegal can be detected and taken down."

With regard to matters of non-consensual intimate imagery, Facebook has been held liable by the Amsterdam District Court and the Dutch Supreme Court for not disclosing the identity of the perpetrator and consequently, permitting the dissemination of NC images.[48] These cases have been discussed in detail in the NCII paper.

3. Recommendations and Best Practices

3.1. Recommendations

a. *Recommendations for an improved legislative framework*

---

[44] *Facebook flooded with 'sextortion' and 'revenge porn' files reveal*, The Guardian, https://www.theguardian.com/news/2017/may/22/facebook-flooded-with-sextortion-and-revenge-porn-files-reveal

[45] Facebook Files, *The Guardian*, https://www.theguardian.com/news/series/facebook-files

[46] *Facebook flooded with 'sextortion' and 'revenge porn' files reveal*, The Guardian, available at https://www.theguardian.com/news/2017/may/22/facebook-flooded-with-sextortion-and-revenge-porn-files-reveal

[47] Part III, NCII paper.

As mentioned in Part I, some legal frameworks run the risk of censoring constitutionally protected content and risking over-censorship. With regard to online violence against women, this problem can specifically be found in Section 67 and 67A of the IT Act, where protected forms of sexual expression can be conflated with 'obscenity'. Since Hicklin's test of obscenity has now been read down by the Supreme Court, we recommend that similar measures be made to read down Section 67 of the IT Act.

With regard to Section 69A, we are of the opinion that efforts should be made to introduce accountability and transparency into the blocking procedure. Our report on intermediary liability titled '*NOC Online Intermediaries Case Studies Series: Online Intermediaries in India'* discusses these issues in detail.[49]

b. Exception to safe-harbor provisions

Following from Part II, it can be noticed that certain jurisdictions are moving away from safe-harbor regimes. As mentioned earlier, the EU Code of Conduct on Hate Speech and Netz DG, Germany's new anti-hate speech law places on intermediaries the responsibility of determining the legality of content and its consequent removal. This move has been widely criticized as it threatens the right to freedom of expression. Due to laws of this kind, intermediaries may err on the side of caution and resort to over-censorship, in order to avoid hefty fines.[50]

This attempt at increasing the responsibility of intermediaries may lead to over-censorship and could be dangerous for free speech on the internet.[51]

---

[48] Chinmayi Arun and Sarvjeet Singh, *NOC Online Intermediaries Case Studies Series: Online Intermediaries in India*, (February 18 2015), Centre for Communication Governance, National Law University, Delhi, http://ccgtlr.org/wp-content/uploads/2015/02/CCG-at-NLUD-NOC-Online-Intermediaries-Case-Studies.pdf.
[49] Patrick Evans, *Will Germany's New Law Kill Free Speech Online?* , BBC, (18 September 2017), http://www.bbc.com/news/blogs-trending-41042266.
[50] *Refer to* Chinmayi Arun and Sarvjeet Singh, *NOC Online Intermediaries Case Studies Series: Online Intermediaries in India*, (February 18 2015), Centre for Communication Governance, National Law University, Delhi, http://ccgtlr.org/wp-content/uploads/2015/02/CCG-at-NLUD-NOC-Online-Intermediaries-Case-Studies.pdf.

It is also worth looking closely at Brazil, which is one of the few jurisdictions to have created an exception to safe-harbor protection for instances of 'revenge porn' or non-consensual intimate imagery.[52]

Article 21 of the *Marco Civil Da Internet*[53] ('Brazilian Internet Bill of Rights') creates an exception for certain acts of sexual violence, which involve a breach of privacy. This intermediary liability regime creates an exception for 'revenge porn' or NC images. Under this provision, judicial orders are not necessary to order removal of content. Affected parties or legal representatives can notify platforms of such content, and platforms can be held 'secondarily liable'. [54]

There also needs to be a higher level of transparency and accountability with regard to private platforms and self-regulation to minimise the adverse effects on free speech.

3.2. Best Practices

With regard to best practices, there are a few noteworthy aspects of the Indian legal framework. The recognition of lack of consent in the sharing of images, under Section 66E and Section 354C is commendable. It recognizes the harm of non-consensual sharing at every step and provides adequate remedies.

These provisions are also noteworthy because they focus on the consent of women and are not concerned with moral propriety, like the Hicklin test. By shifting the focus to consent, a clear distinction between legitimate and illegitimate expression is apparent, and the ability of women to exercise sexual freedom on the internet is not compromised.

The legal standard under Section 67 could be improved, based on these best practices and the Hicklin Test could be read down.

---

[51] Nicolo Zingales, *The Brazilian approach to internet intermediary liability: Blueprint for a global regime?*, 4(4) INTERNET POLICY REVIEW: JOURNAL ON INTERNET REGULATION (2015) https://policyreview.info/articles/analysis/brazilian-approach-internet-intermediary-liability-blueprint-global-regime.

[52] Federal Law No. 12965/2014

[53] Nicolo Zingales, *The Brazilian approach to internet intermediary liability: Blueprint for a global regime?*, 4(4) INTERNET POLICY REVIEW: JOURNAL ON INTERNET REGULATION (2015) https://policyreview.info/articles/analysis/brazilian-approach-internet-intermediary-liability-blueprint-global-regime.