CENTRE FOR COMMUNICATION GOVERNANCE

NATIONAL LAW UNIVERSITY DELHI

SUBMISSION TOWARDS THE CONSULTATION ON 'GENDER PERSPECTIVES ON PRIVACY' BY THE SPECIAL RAPPORTEUR ON THE RIGHT TO PRIVACY

The Centre for Communication Governance (Centre) is an academic research centre within the National Law University Delhi and is dedicated to working on information law and policy in India. It seeks to embed human rights and good governance within communication policy and protect digital rights in India through rigorous academic research and capacity building.

We welcome the efforts of the Office of the Special Rapporteur on the Right to Privacy towards discussing the different aspects of the right. Our comments on questions 1 and 2 (and in part 3) of the Consultation on Gender Perspectives Privacy are below. The following inputs limit themselves to experiences of digital privacy in the Indian context, and are therefore approached from an Indian perspective.

1. **What gender issues arise in the digital era in the Thematic Action Streams (Privacy and Personality; Security and Surveillance; Big Data and Open Data; Health Data, and the Use of Personal Data by Corporations)? What challenges need to be addressed and what positives can be promoted more widely?**

Privacy and Personality

Only 30%, or 143 million of Indian internet users are women[1]. In addition to a vast gap in mobile ownership (the major point of internet access in rural India) between men and women, many women are unable to actually use their phones beyond answering calls, and are dependent on male family members for assistance. The threat of internet access empowering women has even prompted cases of local Panchayats[2] banning women from owning mobile phones in some villages in India[3]. These measures deny women from accessing platforms and spaces where they may readily find information and knowledge, freely express themselves, and connect and interact with individuals outside the local community. This could in turn threaten the control exercised over them by their families, and male authority figures in particular. As a study by the Internet Democracy Project points out:

> *"…by creating spaces for privacy that were previously not available to young women in these communities, mobiles have disrupted the existing patriarchal regimes of control and surveillance. As a consequence, they have also emerged as a major threat to a girl's - and by extension her family's - reputation and izzat (honour)."*[4]

[1] The Economic Times, ONLY 30% OF INTERNET USERS IN INDIA ARE WOMEN: REPORT, THE ECONOMIC TIMES (2018), https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/only-30-of-internet-users-in-india-are-women-report/articleshow/63008082.cms (last visited November 24, 2018).

[2] Panchayats or village councils are a form of self-government that form the grassroots level of the Panchayati Raj (local self-government) system in India.

[3] Osama Manzar, MOBILE PHONES EMPOWER WOMEN, LIVEMINT (2015), https://www.livemint.com/Opinion/DwiRdnamLz6pAKAEZhKaeL/Mobile-phones-empower-women.html (last visited November 24, 2018).

[4] Dr. Anja Kovacs, 'CHUPKE, CHUPKE': GOING BEHIND THE MOBILE PHONE BANS IN NORTH INDIA, GENDERING SURVEILLANCE (2017), https://genderingsurveillance.internetdemocracy.in/phone_ban/ (last visited November 24, 2018).

Shilpa Phadke *et al.* observe that women in India have only conditional access and not claim to public city spaces; thus greater access to public spaces via economic and political visibility has not necessarily translated into greater *rights* to these spaces[5]. This parallels the experiences of women and other minority/ marginalized groups (sexual and gender minorities) on the internet, where the same unequal power structures and structural imbalances are replicated (and at times amplified) online.

The idealised female archetype continues to be that of the "devi" (goddess) who is pure, non-sexual and hence worthy of respect and worship. As a result, any overt expression of female agency (including sexual) automatically justifies the resulting harassment that they may face. Even Supreme Court judgments are sometimes guilty of reinforcing these patriarchal views by linking notions of "dignity" and "honour" with a woman's sexuality and bodily autonomy in cases of rape and sexual assault[6]. It is no wonder, then, that women must navigate these same obstacles when attempting to express themselves online.

The right to privacy is a fundamental right guaranteed under the Indian Constitution. This right, although not explicitly provided for in writing in the Constitution, has been recognised by the Indian Supreme Court in several judgments over the past 60 years[7]. The gendered aspects of privacy have been discussed and acknowledged in many of these judgments. For instance, the Court has held that a mother's fundamental right to privacy cannot be violated by mandating the disclosure of the name and particulars of the biological father of her child for the child's passport[8]. The right to privacy of victims of sexual assault was upheld when the Court condemned performing of Per Vaginal or "two finger" tests on victims of rape in order to verify if the victim was habituated to sexual intercourse[9]. Privacy, self-identity, autonomy and personal integrity were upheld by the

[5] Shilpa Phadke, *'Why Loiter? Radical Possibilities for Gendered Dissent*, DISSENT AND CULTURAL RESISTANCE IN ASIA'S CITIES (2009), https://www.academia.edu/343458/_Why_Loiter_Radical_Possibilities_for_Gendered_Dissent (last visited November 24, 2018).
[6] Betwa Sharma, AN EXCELLENT SUPREME COURT DECISION IS MARRED BY THE LINKING OF HONOUR AND RAPE, HUFFPOST INDIA (2016), https://www.huffingtonpost.in/2015/07/01/supreme-court-judgment-_n_7703744.html (last visited November 24, 2018).
[7] Centre for Communication Governance, The Indian Supreme Court on the Right to Privacy: 63 Years of Progress (2017), https://ccgnludelhi.wordpress.com/2017/08/13/h/ (last visited November 24, 2018).
[8] *ABC v. State (NCT of Delhi),* (2015) 10 SCC.
[9] *Lillu v. State of Haryana* (2013), 14 SCC 643.

Court as fundamental rights guaranteed to members of the transgender community under Article 19(1)(a) of the Constitution of India that the State is bound to recognise and protect, in a petition filed by the National Legal Services Authority (NALSA)[10].

In 2017, the landmark judgment of the Court in *Puttaswamy v. Union of India*[11] reaffirmed the fundamental right to privacy as a core value which the protection of life and liberty is intended to achieve. Chandrachud J. discussed the negative elements (placing restrictions on the State from unfairly infringing individual privacy) and positive elements (obligations to institute legislative frameworks) of privacy. In addition, he also recognised that sexual orientation is an essential component of the right to privacy, and rejected the *de minimus* rationale of the previous 2014 Supreme Court judgment in *Suresh Kumar Koushal v. Naz Foundation*[12].

The NALSA and Puttaswamy judgments laid the foundation for the recent landmark judgment reading down Section 377 of the Indian Penal Code, 1860 ("IPC") that criminalised sexual acts against the order of nature, holding that the Right to Privacy and the protection of sexual orientation lie at the core of the fundamental rights guaranteed by Articles 14, 15 and 21 of the Constitution. Chandrachud J. held that, "Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, home and sexual orientation." Sexual orientation is an essential attribute of privacy, and discrimination on the basis of sexual orientation is deeply offensive to the dignity and self-worth of the individual[13].

Specific to the question of privacy in the digital age, in Puttaswamy, Chandrachud J. focused on the informational aspect of privacy and its deep associations with autonomy and dignity. While rejecting the claim that privacy is an elitist construct, he highlighted the role of privacy in the digital economy, dangers of data mining, positive obligations on the State, and the urgent need for data protection legislation. The recent judgment of the Supreme Court on the Indian government's biometric national identity project (Aadhaar),

[10] *National Legal Services Authority v. Union of India,* (2014) 5 SCC 438.
[11] *Justice K.S Puttaswamy (Retd.) v. Union of India*, (2017) 6 MLJ 267.
[12] *Justice K.S Puttaswamy (Retd.) v. Union of India*, (2017) 6 MLJ 267.
[13] *Navtej Singh Johar v. Union of India*, W. P. (Crl.) No. 76 of 2016.

also touches upon the question of informational privacy[14]. However, there has been little discussion in the Courts on the gendered aspects of privacy in the context of the digital age.

The anonymity of the internet has however, provided a safe haven for sexual freedom and exploration, especially for LGBTQ+ individuals who still face discrimination in mainstream Indian society. This allows members of the community to meet others who can provide support and kinship where they may not be able to find it offline. This anonymity also enables freedom of expression in ways that may not be fully expressed in one's daily interactions with people who may not be aware or supportive of the person's sexual or gender identity. However, attempts at censorship or classifying LGBTQ+ content as "obscene" often stifles free speech and expression in this area. LGBTQ+ content is routinely censored in films and other works of art[15], but these bans are harder to enforce online (despite India having one of the highest instances of website blocking and content filtering[16]). However, many companies are pre-emptively resorting to self-censorship in order to avoid offending the government and more conservative sections of society[17].

Security and Surveillance

The Indian government has been subject to much criticism due to the lack of proper law and oversight governing surveillance by the State. Surveillance is typically conducted in the interest of the 'security of the state', or for the purpose of law enforcement. However,

[14] WRIT PETITION (CIVIL) NO. 494 OF 2012

[15] Freemuse, INDIA: ARTISTS STRUGGLE WITH CENSORS OVER LGBT AND OTHER THEMES (2016), https://freemuse.org/news/india-artists-struggle-with-censors-over-lgbt-and-other-themes/ (last visited November 24, 2018).

[16] Jay Mazoomdaar & Ritu Sarin, INDIA TOPS LIST OF WEBSITES BLOCKED, ITS TELCOS FILTER THE MOST, THE INDIAN EXPRESS(2018), https://indianexpress.com/article/india/india-tops-list-of-websites-blocked-its-telcos-filter-the-most-netsweeper-5150620/ (last visited November 24, 2018).

[17] Meeran Karim, AS AMERICAN TECH FIRMS MOVE TO INDIA, MANY CHOOSE TO SELF-CENSOR, SLATE MAGAZINE(2017), http://www.slate.com/blogs/future_tense/2017/07/18/american_tech_firms_are_preemptively_censoring_content_in_india.html (last visited November 24, 2018).

the existing provisions of the law in India that do touch upon surveillance are outdated, and do not take into account the kind of surveillance that today's technology enables[18].

The government recently published the Personal Data Protection Bill, 2018[19], which many civil society actors hoped would remedy this situation. However, the Bill has instead raised concerns regarding the minimal safeguards that it provides against government surveillance. The report accompanying the Bill recognises this lack of safeguards[20], however, the Bill leaves it to other legislation to provide such safeguards, only providing that all access to personal data by intelligence or law enforcement authorities must be authorized by law, necessary and proportionate in order to be exempted from the requirements under the Bill[21].

It has been argued that in addition to traditional forms of surveillance by intelligence or law enforcement authorities, several government projects also enable surveillance. For instance, the constitutionality of the Aadhaar project was challenged on this basis. However, the recent Supreme Court judgment on the Aadhaar project[22] upheld the validity of Aadhaar, holding that the architecture of the Aadhaar scheme and the provisions of the Aadhaar Act do not enable surveillance, and serves as a legitimate state aim despite many instances of data leaks[23]. The majority judgment remained silent on whether sensitive personal and biometric data of individuals across various databases could constitute surveillance, choosing to focus instead solely on the implications of metadata for surveillance. In addition, the Supreme Court held that allowing private sector access to biometric and demographic information would amount to commercial exploitation.

---

[18] Chinmayi Arun, *Paper-Thin Safeguards and Mass Surveillance in India,* NATIONAL LAW SCHOOL OF INDIA REVIEW 26 (2014): 105 available at https://ssrn.com/abstract=2615958 (last visited November 24, 2018).

[19] The Draft Personal Data Protection Bill, 2018, http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf (last visited November 24, 2018).

[20] A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians, http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last visited November 24, 2018).

[21] The Draft Personal Data Protection Bill, 2018, Sections 42 and 43

[22] WRIT PETITION (CIVIL) NO. 494 OF 2012

[23] Sushovan Sircar, AADHAAR DETAILS ON GOOGLE SEARCH? DATA OF THOUSANDS KEPT PUBLICTHE QUINT(2018), https://www.thequint.com/news/india/aadhaar-data-leak-google-privacy-uidai (last visited November 24, 2018).

Thus, part of Section 57 that enables bodies corporate and individuals to seek authentication, was declared unconstitutional. This raises questions about whether any private entities can use the authentication infrastructure at all, and how this can be reconciled with the Judgment's approval of Aadhaar to dispense subsidies and other government benefits that are dispensed via Public-Private Partnership frameworks.

While the law itself does not look specifically into gendered perspectives on surveillance, or its impact, experts suggest that the impact of surveillance on marginalised communities, including sexual and gender minorities, is often felt to a higher degree[24]. This is also seen as a particularly relevant issue in South Asian communities, including India, where women and sexual minorities are subject to specific forms of discrimination and violence, and are often not allowed to express themselves freely. We now see that the violence and discrimination that these communities have traditionally faced, are being replicated in the context of their access to the technology, the internet, and their online activities.

For instance, we are already seeing that the forced linking of the Aadhaar identity numbers with health services, has caused many individuals to be denied access to healthcare services, including abortion procedures[25]. While the Supreme Court's recent judgment may effect some change in this particular context, schemes for digitisation of health records[26] could hinder access to abortion services, which is already inaccessible to many women, if badly designed. Records of abortions and contraceptive methods are sensitive, and instances of data being exposed could place such women in a dangerous position.

[24] Shmyla Khan, Surveillance as a Feminist Issue, Privacy International (2017), https://privacyinternational.org/partner-update/142/surveillance-feminist-issue; and Nehmat Kaur, What Studying the Impact of Surveillance on Women Can Teach Us About Power, The Wire (2017), https://thewire.in/culture/what-studying-the-impact-of-surveillance-on-women-can-teach-us-about-power (last visited November 24, 2018)

[25] Activists Slam Mandatory Linking of Aadhaar to Health Services After Woman Denied Abortion, The Wire (2017), https://thewire.in/government/activists-slam-mandatory-linking-aadhaar-health-services-woman-denied-abortion (last visited November 24, 2018)

[26] The Indian government has introduced initiatives to digitise all health records in the country in order to ensure health records are easily accessible to medical service providers. See https://mohfw.gov.in/sites/default/files/17739294021483341357.pdf (last visited November 24, 2018)

In addition to relations with government / government provided services, we also see that the impact of surveillance on gender and sexual minorities is also felt in the context of surveillance by their communities. While many platforms on the internet do allow individuals the privacy to express themselves more freely, fears of surveillance by the community, and even families, threats and harassment and other offline repercussions of their online activity continue to exist. Those women who do have the option, sometimes try to break these barriers by creating social media profiles under fake or male names[27]. It has also been reported that authorities often react to online violence against women by suggesting that they use fake (if not specifically male) names, and refrain from posting identifying information about them on public platforms online[28]. In the same vein, sexual and gender minorities may have their online activity monitored due to insufficient safeguards imposed on collection of data by data processors under current Indian law. Instances of data breaches and loopholes in privacy settings at companies such as Facebook[29] could unwittingly expose sensitive information about identities of individuals that they may not be ready to reveal (such as outing members of a closed support group[30]). In a socially conservative country like India, this could result in social boycott or even harassment and death. Such information is also available to the government[31], and

[27] Maya Palit, HERE'S YET ANOTHER REPORT ON HOW INDIAN WOMEN DON'T USE FACEBOOK AS MUCH AS MEN. SHOULD WE CARE?, THE LADIES FINGER (2017), http://theladiesfinger.com/india-women-on-facebook/ (last visited November 24, 2018).

[28] Japleen Pasricha, "VIOLENCE" ONLINE IN INDIA: CYBERCRIMES AGAINST WOMEN & MINORITIES ON SOCIAL MEDIA, FEMINISM IN INDIA (https://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf (last visited November 24, 2018).

[29] Mike Isaac & Sheera Frenkel, FACEBOOK SECURITY BREACH EXPOSES ACCOUNTS OF 50 MILLION USERS, THE NEW YORK TIMES(2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html (last visited November 24, 2018).

[30] Russell Brandom, FACEBOOK CHANGES PRIVACY SETTINGS AFTER OUTING MEMBERS OF A CLOSED MEDICAL SUPPORT GROUP, THE VERGE (2018), https://www.theverge.com/2018/7/12/17565754/facebook-brca-private-group-breast-cancer (last visited November 24, 2018).

[31] Gopal Sathe, THE INDIAN GOVERNMENT HAS BEEN SPYING ON YOUR SOCIAL MEDIA IN SECRET, HUFFPOST INDIA (2018), https://www.huffingtonpost.in/2018/09/07/the-indian-government-has-been-spying-on-your-social-media-in-secret_a_23519703/ (last visited November 24, 2018).

could be used to profile voters[32], or individuals who the government may classify as a threat to national security[33].

Health Data

The Supreme Court's judgments discussed above, including *Puttaswamy*, often discuss privacy in the context of health information, noting that the protection of such information is an important aspect of the right to privacy. However, reports suggest that discrimination against sexual (and gender) minorities by healthcare service providers is prevalent in India[34]. There is a lack of awareness and sensitivity, even within the medical community, on LGBTQ+ issues, as well as reproductive rights of women. Although abortion is legal upto a certain stage of pregnancy in India, reports suggest that due to the sensitivity of the subject from a cultural perspective, and the lack of institutionalised support in a non-discriminatory manner, women prioritise their privacy, and resort to unsafe medical practices in this regard[35].

The Indian government has now introduced initiatives to digitise all health records in the country in order to ensure health records are easily accessible to medical service providers. Earlier in 2018, a draft of the Digital Information Security in Healthcare Act was published[36]. The purpose of the act is to provide for electronic health data privacy, confidentiality, security and standardization and provide for establishment of National Digital Health Authority, and Health Information Exchanges. The Ministry of Health and Family Welfare, which published this draft, called for public comments in April 2018.

---

[32] Gilles Verniers & Sudheendra Hangal, LIKE CAMBRIDGE ANALYTICA, INDIAS POLITICAL PARTIES MINED VOTERS PSYCHOGRAPHIC DATA, QUARTZ INDIA(2018), https://qz.com/india/1247197/cambridge-analytica-indias-bjp-and-congress-mined-voters-psychographic-data/ (last visited November 24, 2018).

[33] Press Trust of India, SECURITY AGENCIES TO GET SOCIAL MEDIA MINING, FACE RECOGNITION TOOLS: SINGH, NDTV GADGETS360.COM (2018), https://gadgets.ndtv.com/internet/news/social-media-data-mining-face-recognition-tools-to-be-given-to-security-agencies-home-minister-1912542 (last visited November 24, 2018).

[34] Ashwaq Masoodi, ACCESSING HEALTHCARE STILL AN ORDEAL FOR LGBTQ IN INDIA, LIVEMINT (2018), https://www.livemint.com/Politics/w6C5ws5POJ7d1O590mP6mJ/Accessing-healthcare-still-an-ordeal-for-LGBTQ-in-India.html (last visited November 24, 2018).

[35] Ritu Mahendru, INDIA'S ABORTION EPIDEMIC, THE DIPLOMAT (2017), https://thediplomat.com/2017/07/indias-abortion-epidemic/ (last visited November 24, 2018)

[36] Call for Comments on the Draft Digital Information Security in Health Care Act https://mohfw.gov.in/newshighlights/comments-draft-digital-information-security-health-care-actdisha (last visited November 24, 2018)

However, it is not clear what direction this bill will take given subsequent developments on the data protection law.

In the meantime, other initiatives to digitise health records are also being discussed. The NITI Aayog, a government think-tank recently published a paper calling for a 'National Health Stack', to make both personal health records and service provider records available on cloud-based services using the internet. This paper calls for creation of 'health IDs' which would in turn potentially be linked to the Aadhaar number of individuals who would benefit from the health stack. While digitisation of health records is seen as a positive step, there are several privacy concerns that have been raised given the proposed means for such digitisation[37].

2. **Has the digital era produced new or significantly different gender-based experiences of privacy?[38] If so, what are these?**

Although the anonymity and privacy afforded by the internet has done much to safeguard individual freedoms, it has also enabled individuals to violate the rights and dignity of others, often without consequences. Contradictory to the popular notion of the internet being an open, democratic space, the experiences of women, sexual minorities and gender non-conforming individuals online are disproportionately fraught with constant abuse, domination, intimidation and threats.

The most common form that this abuse takes is the sexual objectification of women in order to fetishize or degrade them without their consent. Twitter is a leading example – women who express strong opinions are constant targets of abuse that seeks to intimidate and silence. A vast majority of threats consist of rape threats, questioning "character", insinuating "loose morals" and other means to attack a woman's "honour". In

[37] Nayantara Narayanan, NITI AAYOG PLAN FOR AADHAAR-LINKED DIGITAL HEALTH RECORDS RAISES CONCERNS OVER SAFETY AND PRIVACY, SCROLL.IN (2018), https://scroll.in/pulse/886153/niti-aayog-plan-for-aadhaar-linked-digital-health-records-raises-concerns-over-safety-and-privacy (last visited November 24, 2018)
[38] Including experience inclusive of sexual orientation, gender identity, gender expression and sex characteristics.

India, we see that the abuse is often magnified by the use of the individual's caste as an identifying factor while targeting abuse[39].

It is also important to note that very few come forward to report these violations to the police, and even fewer go to trial. This can be attributed to a hostile environment for women, transgendered individuals and sexual minorities which often results in apathy, pressure to settle the matter privately, slut-shaming, counter-threats, or even further sexual abuse at the hands of law enforcement. Sexual minorities often face additional threats of being blackmailed, humiliated or publicly outed.

The *#metoo* movement in India has seen many allegations of sexual harassment. This has two aspects - first, the ethicality of anonymous crowd-sourced lists that name and shame harassers has been called into question for bypassing due process and violating the privacy of accused who have not yet been proven guilty. Secondly, the response to many of these accusations has been to publicly post screenshots of social media pages and private messages in order to discredit the accuser. This could range from pictures of them with alcohol or cigarettes, sexual images or messages, or even friendly pictures with the accused. This results in a public trial that inevitably entails slut shaming the accuser, often doxxing and exposing her to threats of rape and bodily harm.

The experiences of violence / abuse that women suffer online can be classified into the following categories:

- **Cyberstalking, cyberbullying and harassment:** Information relating to a particular individual is collated from various sources available online. This could include social media profiles, friends and professional networks, public databases and geolocation, and manifests through attempting contact and harassing via phone calls, messaging services such as SMS or Whatsapp, email, or comments on social media and public posts. Harassment in India often takes the form of morphing a woman's face onto sexually explicit images and posting them on social

[39] Kiruba Munusamy, INTERSECTION OF IDENTITIES: ONLINE GENDER AND CASTE BASED VIOLENCE, GENDERIT.ORG (2018), https://www.genderit.org/articles/intersection-identities-online-gender-and-caste-based-violence (last visited November 24, 2018).

media – this is particularly serious in a conservative society such as India, where questions of a woman's honour and public reputation can impact all aspects of her life, including marriage and employment. It can even result in a woman being thrown out of her home for sullying her family's honour, driving many women to commit suicide[40].

Cyber stalking has been included in Section 354D[41] of the IPC as monitoring the use by a person of the Internet, email or any other form of electronic communication, or watching or spying on a person in a manner that results in a fear of violence or serious alarm or distress in the mind of such person, or interfering with the mental peace of such person. While legislative measures exist, cyber stalking is not treated as a serious offence by law enforcement, often leaving little action that can be taken by victims of cyber stalking and online harassment against perpetrators.

- **Electronic Voyeurism:** The increasing availability of inexpensive but high quality video recording equipment has fuelled the incidence of voyeurism, which is defined as deriving sexual gratification from the covert observation of others as they undress or engage in sexual activities.[42] While this is not limited to use against women, they are overwhelmingly targeted in most reported cases. This electronic voyeurism is undertaken via hidden cameras placed in rooms, or covert recordings of "upskirt" or "down-blouse" pictures/ videos, as well as non-consensual recording of other body parts that may be fetishized despite not being considered "sexual", such as feet. There have been a number of instances in India of women finding hidden cameras in their hotel rooms, hostel rooms and apartments[43].

---

[40] Ashwaq Masoodi, FOR VICTIMS OF CYBER STALKING, JUSTICE IS ELUSIVE, LIVEMINT (2016), https://www.livemint.com/Politics/St93190XdGvpiclGWwnX0I/For-victims-of-cyber-stalking-justice-is-elusive.html (last visited November 24, 2018).

[41] This Section was introduced in the Criminal Law Amendment Act, 2013

[42] Singh Dalla Harpreet. Cyber Crime – A threat to person, property, Government and Societies. IJARCSSE. 2013; 3(5).

[43] Munish Pandey, DOCTOR ALLEGEDLY VIDEOTAPED WHILE TAKING BATH IN DELHI HOTEL, FIR LODGED, INDIA TODAY (2018), https://www.indiatoday.in/india/story/doctor-allegedly-videotaped-while-taking-bath-in-delhi-hotel-fir-lodged-1233871-2018-05-15 (last visited November 24, 2018); and The Times of India, YOUTH UPLOADS NUDE VIDEOS OF COLLEGEMATES TO FACEBOOK, ARRESTED, THE TIMES OF INDIA (2018),

Electronic voyeurism has been brought into the ambit of the IPC, under Section 354C[44] as a form of sexual harassment. However, this is limited to images of the victim's genitals, buttocks or breasts – and thus unsolicited images of women which do not fall within this definition will not be punishable under this section. Section 66E of the Information Technology Act, 2000 ("IT Act") is also limited to the capture and publishing of "private areas" of a person. Additionally, these laws limit themselves to places where a person may have a reasonable expectation of privacy, disregarding that an individual may not want her images being broadcast publicly for the purposes of voyeurism even if she is sitting in a public place. Section 67 of the IT Act could also be used to penalise electronic voyeurism. This provision penalises the publication and transmission of 'obscene material', which is described as '*any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it*'.

- **Non-Consensual Sexual Imagery:** Popularly known as "revenge porn", this includes images shared in the course of an intimate relationship (both consensually and non-consensually) which are later shared publicly without the consent of the partner who is in these images. This most often occurs on social media or on websites dedicated to intimate images of ex-partners. Although the National Crime Records Bureau documents cyber-crimes against women, there are no official statistics available that pertain specifically to such non-consensual sharing in India.

https://timesofindia.indiatimes.com/city/bengaluru/youth-uploads-nude-videos-of-collegemates-to-fb-arrested/articleshow/65664055.cms (last visited November 24, 2018).

[44] This Section was introduced in the Criminal Law Amendment Act, 2013

Filming and circulating videos of rapes are another form of such violations – most often disseminated by the rapist and his abettors through private messaging apps and then eventually surfacing on social media[45].

At present, there are no legal provisions that directly address non-consensual sexual imagery in India. While certain sections in the IPC and IT Act can be invoked, they fail to capture the complexity of such cases and do not specifically target non-consensual pornography published online.

- **Doxxing:** Derived from "documents" or "docs", this is the act of publicly releasing someone's personal and/or identifiable information without their consent. This can include details like their full legal name, social security number, home or work addresses and contact information[46]. Anyone who comes across this information is then free to use it in whatever way they choose. This was faced by journalist Rana Ayyub, when her address, phone number and a sexually explicit video with her face morphed onto it was released on Twitter, leading her to fear not only for her own safety but that of her family[47]. Fears of mass doxxing arise with instances of Aadhaar data being publicly available via a simple google search[48].

- **Surveillance by family or intimate partners:** It is common for many Indian women to have their phones and internet activity monitored[49] as a means of control and often harassment and abuse. This includes accessing incoming and outgoing

[45] Michael Safi, TWO MEN ARRESTED IN INDIA OVER ALLEGED RAPE ON SHORE OF GANGES, THE GUARDIAN (2018), https://www.theguardian.com/world/2018/oct/04/men-arrested-india-ganges-gang-rape-video (last visited November 24, 2018).
[46] Andrew Coates, DOXXING, SWATTING AND THE NEW TRENDS IN ONLINE HARASSMENT, SCROLL.IN (2017), https://scroll.in/article/722509/doxxing-swatting-and-the-new-trends-in-online-harassment (last visited November 24, 2018).
[47] Mariya Salim, ITS TIME TO ADDRESS ONLINE VIOLENCE AGAINST WOMEN IN INDIA, AL JAZEERA (2018), https://www.aljazeera.com/indepth/opinion/time-address-online-violence-women-india-180513095849630.html (last visited November 24, 2018).
[48] Meghnad Bose, ANOTHER AADHAAR DATA LEAK: JUST GOOGLE 'MERA AADHAAR MERI PEHCHAN', THE QUINT (2018), https://www.thequint.com/news/india/another-aadhaar-data-leak-google-mera-aadhaar-meri-pehchan (last visited November 24, 2018).
[49] Sujatha Subramanian, WHY ARE THERE SO FEW WOMEN ON THE INTERNET IN INDIA?, HINDUSTAN TIMES (2017), https://www.hindustantimes.com/opinion/locating-gender-in-the-digital-divide/story-zt10VjNAwnOqcChjkYCLfN.html (last visited November 24, 2018).

messages and emails, knowledge of passwords, and monitoring web activity via browser histories. In some cases, this could also extend to using GPS to track phones and monitor a partner's physical location at all times.

While many of these activities have a direct impact on the privacy of women, we also see that there is a chilling effect on their ability or desire to express themselves freely. In addition to the abusive behaviour described above, the #metoo movement has also brought focus on the use of 'SLAPP suits' and defamation charges against the women alleging abuse or harassment[50].

[50] Defamation is still punishable under criminal laws in India (specifically, under Section 499 and Section 500 of the Indian Penal Code, 1860).