# Response to the call for inputs into a report on 'Privacy: A Gender Perspective' by the United Nations Office of the Special Rapporteur on the Right to Privacy

**IT for Change**
**October 2019**

The preliminary report of the Special Rapporteur on the Right to Privacy (SRP) was published in March 2019 (https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx). Feedback on the same has been sought from different stakeholders as an input into the SRP's final report to be submitted to the Human Rights Council in March 2020.

A public consultation was also held in end October to explore whether the report has captured adequately the following:
1. Gender issues arising in the digital era in for example health surveillance, the behavior of large platform companies, and issues such as discrimination, arising from the gender-differentiated impact on privacy.
2. Initiatives and responses to gender-differentiated impacts on privacy and challenges that need to be addressed.
3. Recommendations addressing gender based differences in the enjoyment of the right to privacy.

This response from IT for Change to the report of the Special Rapporteur on the Right to Privacy (A/HRC/40/63) recommends specific focus in relation to the gendered underpinnings of:
1. State surveillance
2. Dataveillance in the platform economy
3. Workplace dataveillance
4. Social and community surveillance
5. The encryption-decryption debate

## 1. State Surveillance

The 34th Session of the UN Human Rights Council has adopted the resolution on "right to privacy in the digital age" (A/HRC/34/L.7/Rev.1), which has crucially insisted on States ensuring "*that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality".*

Women's bodies have a history of being the battlefields of patriarchy and social prejudice. Whether it is through restrictions on clothing (ban on burqas[1]) or control over reproduction – one child policy;[2] forced sterilization of women from particular ethnic or religious groups,[3] women with disabilities[4] and poor women in general;[5] and refusal of abortion;[6] states have upheld, and continue to privilege, other interests over those of women's right to privacy, dignity and bodily integrity.

1 https://www.economist.com/graphic-detail/2019/08/09/burqa-bans-have-proliferated-in-western-europe
2 https://www.vice.com/en_asia/article/wjwqnb/the-kids-of-chinas-80s-one-child-policy-still-feel-its-pain
3 https://www.latimes.com/world-nation/story/2019-10-29/peru-forced-sterilization-alberto-fujimori
4 http://www.pbs.org/independentlens/blog/unwanted-sterilization-and-eugenics-programs-in-the-united-states/, https://www.hrw.org/news/2011/11/10/sterilization-women-and-girls-disabilities
5 http://faculty.webster.edu/woolflm/forcedsterilization.html, https://www.theguardian.com/world/2014/nov/12/india-sterilisation-deaths-women-forced-camps-relatives
6 https://www.theguardian.com/world/2019/jun/14/abortion-texas-waskom-all-white-male-council

The absence of safeguards for sensitive and personal data and information disproportionately targets women. Ethno-patriarchal state policies render the bodies of women citizens from minority religious or ethnic groups highly visible to the state surveillance apparatus.

States are known to deploy digital IDs to create mechanisms for universalizing government services, as part of their digitalization strategies. In his recent report, the UN Special Rapporteur on extreme poverty and human rights has cautioned states against digital solutionism, warning that this might lead to a “digital welfare dystopia”.[7] Digital IDs could accentuate the existing burdens of surveillance that women carry while negotiating their private and public lives. For instance, when digital IDs are linked to shared mobile phones (a phenomenon that is common in South Asia, for example[8]), for verification or authentication, women may not be able to avail of certain services without loss of confidentiality. Digital IDs could also deepen the vulnerabilities of gender minorities. In Malaysia, MyKad, the national identification system, adopts a 12-digit numbering method with odd numbers at the end of the last of the four digits representing biological males and even numbers representing biological females. For transgender people who face stigma and discrimination, the system’s delegitimization of their identity compounds their struggle for official acknowledgment of their gender dysphoria. Muslim transgender people are judged to be impersonating the opposite sex and are criminalized under state-administered syariah (Sharia) laws.[9]

With the advent of smart cities, a range of human and non-human non-personal data[10] will be collected by the state through IoT devices in public spaces. This is likely to have deeply personal impacts. Given the inextricable links between personal and non-personal data in these mixed data sets, it would always be possible to re-identify individuals even when their data has been anonymized or de-identified. Such legibility could potentially make women and those with non-normative gender identities easy targets for surveillance and social control/censure. Mixed data sets (for instance, mobility data based on GPS, when combined with personal identifiers) could pose the real threat that women visiting reproductive health facilities are traced and penalized by states that seek to regulate pregnancies/ have passed anti-abortion laws. There needs to be a restriction therefore on the nature of data that can be collected by states, and the UN HRC’s recommendation that a ‘necessity and proportionality’ principle for data collection be applied[11] should be implemented through legislative mechanisms. There should be safeguards to ensure that techno-design architectures for reproductive health programs preclude the possibility of individual identification/targeting. Estonia, for example, has incorporated built in accountability and transparency mechanisms into its digital identity program through which access to secure e-services is provided.[12]

- **States must recognize that privacy in the digital age cannot be guaranteed in the absence of comprehensive data protection legislation.**
- **Data protection legislation needs to pay attention to the particular ways in which violation of privacy negatively impacts women and gender minorities.**

7 https://cdn.netzpolitik.org/wp-upload/2019/10/UN-Report-poverty-humanrights.pdf
8 https://www.gsma.com/mobilefordevelopment/resources/mobile-gender-gap-report-2019/
9 https://egov4women.unescapsdd.org/case-studies
10 https://www.medianama.com/2019/09/223-non-personal-data-flows-policy/
11 A/HRC/34/L.7/Rev.1
12 https://blogs.worldbank.org/developmenttalk/development-e-story-estonia

- **National laws must also account for the potential risk of reidentification and loss of privacy in mixed-data sets.**
- **A necessity and proportionality principle needs to be applied for all use-cases of digital IDs.**

## 2. Dataveillance in the platform economy

The digital economy is based on a data extractivism, which rests on the bulwark of free and informed consent (FAIC) from users whose data is being harvested. The idea of FAIC is a fiction that does not match with the reality of experiences of most users, especially from the global south. The assumption of FAIC gives undeserved legal protection to the collection of data as the standard of obtaining consent in most places around the world is a mere click-through form; an 'I Agree' button. This fails to take into account the ability to give such FAIC of persons who have lower educational attainments or digital fluency, or those who do not understand the language in which consent is taken. In Africa and South Asia, for example, a majority of women live in rural areas, have low levels of literacy and are unlikely to be sophisticated users of the internet.[13] This puts them at a disadvantage with respect to informed consent.

Inability to protect one's self-interest is not a permissible ground for the violation of human rights to privacy and dignity. The overwhelming weight placed upon consent requirements for the legitimacy of the data protection framework becomes an exercise in futility if those most vulnerable to excesses of the data economy cannot be protected. This raises the necessity of a fiduciary role to be played by entities, including intermediaries, that collect, process and make use of data.

Unregulated data markets predicated on consent, thrive on gender-based profiling and targeting. Opaque algorithmic targeting is known to be based on gender stereotypes that in turn have discriminatory consequences for women's equal access to economic opportunities (housing access,[14] credit access,[15] job access[16]), undermining their decisional autonomy.

Technologies that map women's bodies and reproductive choices have been a site for the performance of patriarchal control even as they have provided women an illusion of choice. From ultrasound machines to fit-bits is a singular narrative of incursion into female bodies benefiting the medical-industrial complex.

Apps that track reproductive health are powered by data voluntarily fed by users and processed using basic algorithms which are not programmed to serve user needs[17] as much as those of

13 GSMA Connected Women – The Mobile Gender Gap Report 2019, https://www.gsma.com/mobilefordevelopment/resources/mobile-gender-gap-report-2019/; https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Individuals%20using%20the%20internet%20by%20gender_Jun2019.xlsx

14 US Lawmaker's to probe algorithmic bias https://www.bbc.com/news/technology-47894492

15 https://www.fintechfutures.com/2019/11/facebook-target-of-financial-services-discrimination-lawsuit/

16 Amazon scraps secret AI recruiting tool that showed bias against women,https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G; Google translate's gender bias pairs he with hardworking and she with lazy, https://qz.com/1141122/google-translates-gender-bias-pairs-he-with-hardworking-and-she-with-lazy-and-other-examples/; https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study

17 https://www.vox.com/the-goods/2018/11/13/18079458/menstrual-tracking-surveillance-glow-clue-apple-health

potential marketers.[18] Normal experiences for women, such as a missed period or abortion are not accounted for by these apps. This not only leads to predictions that are way off the mark, but also to a derecognition of the user's experience through an invalidation of her entire data archive as 'bad data'.[19] Emerging evidence suggests that apps like Flo and Clue which present themselves as 'pre-diagnostic tools' and 'smart assessment that can be shared with doctors' are exclusively based on hormonal information and do not account for eating disorders or physical training, which can mislead women to believing that they have hormonal imbalances.[20] Triangulation of information through app-based forums where sexual/reproductive health is discussed could easily render LGBTQI users participating in such communities vulnerable to the risk of 'outing'.

- **States should introduce legally backed privacy protection standards that go beyond individualized modes of obtaining consent and spell out rules that obligate intermediaries to enforce these standards.**
- **Intermediaries must adopt a fiduciary 'duty of care' approach towards their data subjects.[21]**
- **National mechanisms for personal data protection must account for the gendered consequences of profiling and also incorporate a right to explanation.**
- **States must include reproductive health data as sensitive personal data and information deserving greater degree of protection under their data protection laws.**

## 3. Work place dataveillance

Work place surveillance through Closed-Circuit Television (CCTV) cameras tends to single out and target women's bodies.[22] Cameras in predominantly female work spaces, like garment factories, or in domestic work settings/homes, regulate the behavior of women workers, ensuring they are 'working properly' and cannot unionize.[23] Through mandatory prescriptions or perverse incentivization for the use of wearables, employers track female employees, including their data about menstruation.[24] In a context where firms/employers have been known to discriminate against pregnant employees, the collection of reproductive health data heightens the risk of gender discrimination at the workplace. Given the cultural taboos on pre-marital sex in many countries, app-based tracking can lead to stigmatization of sexually active women who are single/unmarried.

There is documented evidence of sexual surveillance of female employees in feminized work-sectors, with one in seven women workers having said that they had left their job due to harassment or violence.[25] Emerging forms of surveillance through datafication, such as through CCTV cameras, will only exacerbate the problem. Also, ostensibly 'objective' visual information captured by cameras may be seen as more reliable sources of evidence, undermining women

18 https://www.washingtonpost.com/news/the-switch/wp/2016/08/03/how-your-period-tracking-app-could-leak-your-most-intimate-information/%20,/?arc404=true,https://www.bloomberg.com/news/articles/2019-01-24/how-period-tracking-apps-are-monetizing-women-s-extremely-personal-data.
19 https://www.vox.com/the-goods/2018/11/13/18079458/menstrual-tracking-surveillance-glow-clue-apple-health
20 https://www.nytimes.com/2019/10/27/technology/personaltech/health-apps-hormonal-disorder-pcos.html
21 UK Online Harms White Paper, https://www.gov.uk/government/consultations/online-harms-white-paper
22 https://cis-india.org/raw/digital-domestic-work-india-announcement; https://www.channelnewsasia.com/news/cnainsider/maids-domestic-workers-cctv-cameras-abuse-employer-10796738
23 https://genderingsurveillance.internetdemocracy.in/cctv/
24 https://www.theguardian.com/world/2019/apr/13/theres-a-dark-side-to-womens-health-apps-menstrual-surveillance
25 https://www.ituc-csi.org/eliminating-violence-against-women-18661

workers' experiences of verbal violence.[26] Vocal female employees may be isolated and placed under CCTV surveillance as a form of punishment.[27]

- **National laws on personal data protection and labor rights must incorporate the data rights of women and gender minorities to privacy and personal data protection.**
- **In this regard, it may be noted that UNI Global Union has come up with 10 Principles for Workers' Data Privacy and Protection,[28] including that workers may not waive their privacy rights. The Principles propose limitations on workers' personal data collection, use and processing by employers, for instance, through use of polygraphs and truth verification instruments, mandatory personality tests, extra-judicial genetic screening and secret monitoring of workers.**

## 4. Social and community surveillance

Policing of women by family, friends and local communities is typical of honor cultures,[29] ensuring their conformity with traditional gender norms. Such surveillance further inhibits the already limited opportunities that women have for self-exploration as well as community building. Access to the internet enables women to discover themselves, expand their networks and participate in new communities. But in some parts of the world, participating in online social media platforms implies the risk of perpetual surveillance and patriarchal policing. For instance, in a primary study by IT for Change with 881 college-going young women between the ages of 19 and 24 in three southern states of India, we found that women were afraid of sharing their experience of gender based cyberviolence with their families lest their access to mobile devices was taken away.[30] Restrictions on access to gadgets is accompanied by surveillance of use, and women may be compelled to share passwords of their social media accounts with brothers.[31] Women in the study reported that boyfriends and relatives continuously monitor their gender performance online, subjecting them even to extreme forms censure, if found violating acceptable standards of 'modesty'.[32] Young women turn to self-policing their online behavior, sticking with socially accepted gender codes in order to be able to stay online. The threat of social, communitarian and familial surveillance not only violates women's right to privacy, but also obliterates their aspiration to be part of digitally mediated public and social spaces. The option before women is to either conform to traditional gendered norms of behavior or leave the internet.

In some Indian villages, women are banned from owning mobile phones for fear that they might get "distracted from their studies"; whereas no such restrictions exist for young boys.[33] Educational institutions are also known to take a similar stance.[34] Recently, in a case where a female student

26 https://genderingsurveillance.internetdemocracy.in/cctv/
27 https://genderingsurveillance.internetdemocracy.in/cctv/
28 http://www.thefutureworldofwork.org/opinions/10-principles-for-workers-data-rights/
29 The torture, abduction and killing primarily of women, but also men, by families and community governance bodies for transgressing supposed 'codes of honour' is well-chronicled. See Baxi, Pratiskha; Rai, Shirin, M and Ali, Shaheen Sardar. "Legacies of Common Law: 'crimes of honour' in India and Pakistan' Third World Quarterly 27:7. 2006. https://www.researchgate.net/profile/Pratiksha_Baxi/publication/242511496_Legacies_of_common_law_'Crimes_of_honour'_in_India_and_Pakistan/links/53dfdb740cf27a7b8306c90f.pdf
30 https://itforchange.net/sites/default/files/1662/Executive_Summary_Born%20digital-Born-free%20.pdf
31 One survey participant described it as akin to having a joint bank account which protects her from making "bad mistakes".
32 Another survey participant said, "My boyfriend saw a pic of mine, where I am sitting with one leg (crossed) on the other. He told me I should not pose for pics like that. Put both feet on the floor, he said."
33 https://www.aljazeera.com/news/2016/02/india-banning-women-owning-mobile-phones-160226120014162.html
34 https://www.deccanherald.com/national/south/student-files-plea-in-hc-against-mobile-ban-in-hostel-749749.html

challenged restrictions placed by the college on accessing mobile phones in the girls' hostel, an Indian Court upheld her right to access the internet arguing that such access was part of her rights to education and privacy.[35]

IoT enabled devices such as publicly placed CCTV cameras are already being deployed towards domestic abuse by women's current and former partners.[36] Digital abuse by spouses,[37] partners and strangers, and the use of 'revenge porn' to violate a woman's bodily privacy and cause her reputational harm,[38] has become shockingly commonplace.[39]

Visible women who participate in the public sphere find themselves attacked by sexist hate speech,[40] social media hate campaigns,[41] doxxing[42] and other forms of harassment.[43] The fear of facing reprobation for their non-conforming (private) lives causes a chilling effect on women's speech and decreases the participation of women in online publics.

The non-consensual circulation of intimate images (NCII) of women by former partners is used as a mechanism to control, coerce or otherwise cause reputational harm to women. Patriarchal cultures imply that online misogyny is not recognized as a form of violence against women in laws of most countries. The techno-social underpinnings of misogyny in online spaces – anonymity and toxic disinhibition, virality and 'bro cultures' – present new challenges in developing appropriate legal responses to tackle such ubiquitous harm.

Argentina has proposed a law that would make NCII into a criminal offense and seek its removal by judicial order.[44] The Canadian province of Saskatechewan, on the other hand, has developed a civil/tort liability standard against the sharing of non-consensual intimate images, which reverses the onus on to the distributor of the image, who must demonstrate that he had consent to share the image.[45]

The virality of NCII in the digital age has led to a crisis for women's bodily privacy. The circulation of patently illegal content such as 'rape videos' – not only violative of women's rights, but grievously inimical to their dignity – has become distressingly common. The Indian Supreme Court's order recommending that internet intermediaries propose a standard operating procedure for implementing algorithmic monitoring tools to filter and auto-delete unlawful content such as rape videos illustrates efforts to bring justice closer to women.[46]

- **States should recognize that access to the internet is a precondition for exploring, understanding and becoming aware of one's sexuality and identity and to forge new**

35 https://www.livelaw.in/top-stories/right-to-access-internet-is-part-of-right-to-privacy-and-right-to-education-kerala-hc-148240
36 https://www.theguardian.com/commentisfree/2018/jul/01/smart-home-devices-internet-of-things-domestic-abuse
37 https://www.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x
38 https://time.com/4811561/revenge-porn/
39 https://slate.com/technology/2018/03/apps-cant-stop-exes-who-use-technology-for-stalking.html
40 https://www.genderit.org/feminist-talk/false-paradox-freedom-expression-and-sexist-hate-speech
41 https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23126&LangID=E
42 https://www.amnesty.org/en/latest/campaigns/2017/11/what-is-online-violence-and-abuse-against-women/
43 https://www.vice.com/en_us/article/yw74zb/twitter-harassment-of-woman-journalists-and-politicians-happens-every-30-seconds-amnesty-study-finds
44 https://www.refworld.org/docid/5be16b2b4.html, https://www.internetlab.org.br/en/inequalities-and-identities/how-do-countries-fight-the-non-consensual-dissemination-of-intimate-images/
45 https://lsslib.wpcomstaging.com/2018/12/06/saskatchewans-new-revenge-porn-law/
46 https://www.livemint.com/Companies/eRMEjTWA9sjxadVnJNsKWL/Google-Facebook-WhatsApp-rape-child-porn-videos.html

**communities and build solidarities. The right to access the internet is thus an important facet of the right to privacy.**

- **Law as an instrument of justice for women can be made more accessible if civil remedies accompany criminal provisions. Pursuing the latter tends to be long drawn, resource intensive and even humiliating, for women. In a digitally mediated public sphere, a pragmatic via-media to address the virality of egregious content that denigrates women is to explore a variegated approach to different kinds of content, examining the merits in each case of algorithmic tools for filtering and auto-deleting.**
- **While a broad and overarching approach to the use of such algorithmic tools is antithetical to freedom of speech and expression, states could adopt these measures to protect and promote women's rights, making sure that intermediaries are transparent about the procedure followed and algorithms used. Algorithmic monitoring also needs necessary human supervision and associated processes for democratic scrutiny that the state is accountable for.**
- **Internet intermediaries have a duty and responsibility to cooperate with law enforcement agencies towards solving cybercrimes against women.**

## 5. The encryption/decryption debate

States are increasingly arguing for the need to create backdoors to encryption in online communication.[47] Recently, security advisors from the US, UK and Australia approached Facebook appealing that it refrain from adding end-to-end encryption on its messaging platform.[48] They have submitted that this is necessary to track down and combat illegal activities conducted through Facebook, including child sexual exploitation, terrorism and extortion, broadly, the protection of their most vulnerable citizens.[49] States have also been demanding that over-the-top services (such as Whatsapp calling) should have the same design architecture as traditional telephony and afford the same surveillance architectures.[50]

The clamor for decryption from state agencies partly reflects the legitimate need to interfere with encryption for the purposes of law enforcement. Oftentimes, law enforcement agencies face a lack of responsiveness from platform intermediaries during crime investigation. Mechanisms like Mutual Legal Assistance Treaties (MLATs) have not proven to be efficient. Women's access to justice in cases of gender-based cyberviolence may be compromised when enforcement agencies are not able to marshal the necessary electronic evidence that lies beyond the territorial jurisdiction of national agencies.

However, breaking encryption may be tantamount to a violation of citizen rights. The Special Rapporteur on the freedom of expression, David Kaye, has underscored the importance of encryption for providing a "zone of privacy", protecting users from arbitrary interference and enabling free speech and opinions.[51] In the digital age, the right to encryption is thus closely tied to the right to privacy. States are hence duty-bound to follow the legality, necessity and proportionality

47 https://www.indiatoday.in/india/story/centre-facebook-spar-over-decryption-laws-at-supreme-court-1611980-2019-10-22
48 https://www.theguardian.com/technology/2019/oct/03/facebook-surveillance-us-uk-australia-backdoor-encryption
49 https://www.buzzfeednews.com/article/ryanmac/bill-barr-facebook-letter-halt-encryption
50 https://www.accessnow.org/watch-bad-regulation-ott-services-can-risk-rights/; https://indianexpress.com/article/opinion/editorials/trai-ott-service-providers-whatsapp-user-data-encryption-6063219/
51 https://freedex.org/2018/07/06/uns-chief-freedom-of-expression-monitor-urges-states-companies-to-protect-encryption-online/

principles of international human rights law, and adopt least-restrictive-means in cases where decryption is sought to be pursued.

- **State measures that systematically weaken encryption interfere with rights to opinion, expression and privacy. As proposed by the Special Rapporteur on the freedom of expression, court-ordered decryption may be permitted only on a case-by-case basis. That is, decryption may be resorted to provided the legal criteria are transparent and publicly accessible, conforming with the requirements of Article 19(3) of ICCPR, and based on prior judicial authorization and associated due process safeguards.**

## Conclusions and final recommendations

In light of our observations above, we recommend that the High Commissioner should mandate states to:

- Recognize that access to the internet is a precondition for exploring, understanding and becoming aware of one's sexuality and identity, participating in community life and building solidarities. The right to access the internet is thus an important facet of the right to privacy.
- Follow a legality, necessity and proportionality principle for use-cases of digital IDs and bring into force legislation that prohibits disproportionate incursions into the rights of women and gender minorities.
- Adopt least-restrictive-means in cases where decryption is sought, with judicial authorization and associated due process safeguards.
- Recognize the importance of bringing into force comprehensive data protection legislation for guaranteeing privacy protection to their subjects. Such legislation must go beyond individualized modes of obtaining consent. It should account for the disproportionate gendered consequences of profiling on women and gender minorities, be cognizant of the risks of deanonymization in the use of mixed-data sets, and incorporate a right to explanation.
- Provide higher degree of protection to reproductive health data, classifying it as sensitive personal information in data protection legislation.
- Amend existing laws to incorporate worker data rights, especially the rights of women and gender minorities for privacy and personal data protection.

The High Commissioner should equally recommend that platform intermediaries:

- Adopt a 'duty of care' approach vis-a-vis platform users.
- Recognize that they have a fiduciary duty to protect the privacy of women and sexual minorities.