Comments to the United Nations Human Rights Commission Report on Gender and Privacy

October 24, 2019

By **Aayush Rathi, Ambika Tandon** and **Pallavi Bedi**

The Centre for Internet and Society, India

https://cis-india.org

Template designed by Saumyaa Naidu

Introduction

This submission presents a response by researchers at the Centre for Internet & Society, India (CIS) to the 'Gender issues arising in the digital era and their impacts on women, men and individuals of diverse sexual orientations gender identities, gender expressions and sex characteristics' – A Report of Consultation by the SRP Thematic Taskforce 'Privacy and Personality' (hereafter **HRC Gender Report**).[1]

CIS is an 11-year old non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. Through its diverse initiatives, CIS explores, intervenes in, and advances contemporary discourse and regulatory practices around internet, technology, and society in India, and elsewhere. Current focus areas include cybersecurity, privacy, freedom of speech, labour and artificial intelligence. CIS has been taking efforts to mainstream gender across its programmes, as well as develop specifically gender-focused research using a feminist approach.

CIS appreciates the efforts of Dr. Elizabeth Coombs, Chair, Thematic Action Stream Taskforce on "A better understanding of privacy", and those of Professor Joseph Cannataci, Special Rapporteur on the Right to Privacy. We are also grateful for the opportunity to put forth our views and comment on the HRC Gender Report.

General Comments

Contextual notions of privacy

It is important to call for contextual and situated understandings of privacy. The individualised notion of the rights-based approach to privacy is being imported from traditional solutions to privacy challenges Global North and finding its way into legislative and judicial work in the Global South. This framing of privacy has been critiqued by feminists for starting from the perspective of an individualised subject with bargaining power.[2] Individualisation has the potential to invisibilise the web of power and social relations which mediate decision-making for women across the global South, including about their own bodies.[3] This has implications for how policy

[1] United Nations Human Rights Council. (2019). *'Gender issues arising in the digital era and their impacts on women, men and individuals of diverse sexual orientations gender identities, gender expressions and sex characteristics' – A Report of Consultation by the Srp Thematic Taskforce 'Privacy and Personality.'* A/HRC/40/63. Retrieved from https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf

[2] Allen, A. L. (2011). Unpopular Privacy: What Must We Hide? Oxford: Oxford University Press; Kovacs, A. (2017). Reading surveillance through a gendered lens: Some theory. *Gendering Surveillance*. Retrieved from https://genderingsurveillance.internetdemocracy.in/theory

[3] Weinberg, L. (2017). Rethinking privacy: A feminist approach to privacy rights after Snowden. Westminster Papers in Culture and Communication, 12(3), 5-20.

responses may be generated, especially in the context of information technologies and their design to accord benefits while furthering community interests at large.[4]

Surveillance at the workplace

Surveillance and sexual harassment of women at work requires particular attention. Research on the future of work points to increasingly intrusive forms of technologically-enabled control being placed on workers as the workplace becomes increasingly 'fissured'. This has severe implications for the quality of jobs that the future of work will hold.[5] This is especially the case with workers engaged in the 'informal' economy, has greater women's representation than labour in the 'formal' sectors in large parts of the Global South.[6] Attention should also be paid to sex workers in particular, who are more vulnerable to technologically-mediated violence and exploitation including non-consensual sharing of intimate images, blackmail and extortion.

In India, in the draft Personal Data Protection Bill 2018, Chapter 3, Section 16 deals with issues related to employment in ways that legitimise the use of intrusive supervision mechanism and extensive surveillance of employees.[7] The future of work, then, can be anticipated to mediate access to the workplace and privacy within the workplace in many gendered forms.

Community-focused recommendations

The recommendations, broadly speaking, operate in the solution space comprising of legal-technological fixes. This may be a limited way to respond to the gendered availability of privacy that the report seeks to resolve. This may also be a function of the approach to knowledge-production that dominates policy efforts globally. It has resulted in critical approaches to surveillance resistance only vesting in very particular expert communities, with the linkages to broader social justice movements being glaringly absent.[8] An important starting point to further understand the implications (and then build responses) is to approach research using a feminist methodological approch.[9] While the focus on a gender analysis certainly is

---

[4] Rathi, A. & Tandon, A. (2019). Capturing Gender and Class Inequities: The CCTVisation of Delhi. Development Informatics Working Paper no. 81. Retrieved from https://cis-india.org/internet-governance/files/development-informatics

[5] Gutelius, B., & Theodore, N. (2019). *The Future of Warehouse Work:Technological Change in the U.S. Logistics Industry*. *The Future of Warehouse Work:Technological Change in the U.S. Logistics Industry*. UC Berkeley Center for Labor Research and Education and Working Partnerships USA. Retrieved from http://laborcenter.berkeley.edu/pdf/2019/Future-of-Warehouse-Work.pdf

[6] Tandon, A., & Rathi, A. (2018). A Gendered Future of Work: Perspectives from the Indian Labour Force. *The Centre for Internet and Society, India*. Retrieved from https://cis-india.org/internet-governance/women-in-future-of-work.pdf

[7] The Personal Data Protection Bill, 2018. Retrieved from https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

[8] Dencik, L., Hintz, A. & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data and Society*, 3 (2), 1-12. Retrieved from http://orca.cf.ac.uk/96123/

[9] Tandon, A. (2018). Feminist Methodology in Technology Research - A Literature Review. *The Centre for Internet and Society, India*. Retrieved from https://cis-india.org/internet-governance/feminist-methodoloty-in-technology-research.pdf

overlapping, a feminist approach will entail greater investment in the politics of change and transformation of structures around gender itself.

Specific Comments

Digital technology - social media, apps and smart devices

Communities at risk of facing disproportionate violence online also includes religious minorities and dalit women.

Technologically facilitated violence

The issue of 'trivalisation' of online violence needs to be explored. This encompasses the belief that technologically-facilitated violence is limited to the 'online space', and needs to be dispelled. The psychological impact of such violence also needs to be explored further. This treatment of technologically-facilitated violence as trivial as is also been witnessed among law enforcement in cyber cells.[10] The separation of cyber crime from physical crime has also implied that officers in police stations have refused to deal with such complaints on account of it being a "cyber crime", and creates challenges for women when they try to report such violence.[11]

Security and Surveillance

Persons who belong to discriminated and underprivileged groups are more likely to be scrutinised through the nexus of state-private surveillance in public spaces - both physical and virtual. This raises concerns of the State using the surveillance to criminalise the activities of such communities. At-risk communities also include protesters and activists, especially with the introduction of facial recognition technologies in public spaces. CCTVs in public space can become an instrument to enforce the behavioural norms of dominant communities. However, when placed on authorities, CCTVs can become a mechanism of ensuring transparency and access to justice for marginalised communities. It can also be used to monitor the activists/organisations working with these communities to restrict their freedom of speech and movement.

Big data and open data

The thematic section on 'Big Data and Open Data' needs to capture the gendered nature of open data initiatives. While open data initiatives hold the promise of delivering meaningful benefits for women, research in Africa has shown, open data access and use often entrench the power and access dynamics already prevailing offline and historically.[12] Often neglected in open data discussion are questions

[10] Devika, J. Riding the Tiger vs. Hanging on to its Tail? TMVAW in Kerala and the Resistance to it. *It for Change*. Retrieved from https://itforchange.net/Riding-the-Tiger-vs-Hanging-on-to-its-Tail-TMVAW-in-Kerala
[11] Ibid.
[12] Brandusescu, A., & Nwakanma, N. (2018). *Is Open Data Working for Women in Africa?* World Wide Web Foundation. Retrieved from http://webfoundation.org/docs/2018/07/WF_WomanDataAfrica_Report.pdf

around 'information justice': existing data gaps, what constitutes knowledge, whose data is being opened and who will benefit, and how will it lead to equality and equity of access.[13] Open data initiatives, then, can continue to preclude gender balance and equality issues and may result in the denial of critical data being 'opened up' to the very people it seeks to benefit.

Further, the thematic sections on 'Big Data and Open Data' and 'Health Data' should include focus on the datafication of welfare programmes run by the state. As research in India has shown, access to reproductive health has historically been, and continues to be in the form of surveillance infrastructure.[14] As is the case with surveillance, welfare programmes too are designed with a focus on populations occupying intersecting marginalities including class, caste, sexual orientation and gender. At the same time, the design of these welfare programmes has often being top-down and has translated into the conception and implementation of datafied initiatives.[15] The right to privacy, then gets actualised as trade offs - for example, in the case of surveillance platforms as that between privacy and security and in the case of welfare programmes between privacy and state provided 'entitlements'.

Finally, as government and private actors start to collect enormous amounts of information about individuals, it becomes increasingly difficult disclosure of gender to become voluntary, even if data collection does not make such a disclosure mandatory. The Centre for Internet and Society has carried out research to show that there are several methods to infer an individual's gender without such information being part of the original dataset.[16] This could pose risks to individuals who do not want to disclose their gender.

Recommendations

1. Surveillance mechanisms such as the use of CCTV cameras and facial recognition technology need to backed by a legal and regulatory framework. Use of such mechanisms without a corresponding legislation determining the parameters of legal surveillance (i.e. the purpose of the surveillance, the limits to the collection of data, storage limitation), should not be permitted. At the same time, the use of monitoring tools for 'sousveillance' or inverse

[13] Johnson, J.A. (2014). From open data to information justice. Ethics and Information Technology, 16, 263. https://doi.org/10.1007/s10676-014-9351-8
[14] Rathi, A. & Tandon, A. (2019). Data Infrastructures and Inequities: Why Does Reproductive Health Surveillance in India Need Our Urgent Attention? *EPW Engage*. Retrieved from https://www.epw.in/engage/article/data-infrastructures-inequities-why-does-reproductive-health-surveillance-india-need-urgent-attention
[15] Tandon, A. (2019). Big Data and Reproductive Health in India: A Case Study of the Mother and Child Tracking System. *The Centre for Internet and Society, India*. Retrieved from https://cis-india.org/raw/big-data-reproductive-health-india-mcts
[16] Goudarzi, S. (2018). Identification of Gender and Sexuality of Subjects in Big Data Sets. *The Centre for Internet and Society, India*. Retrieved from https://cis-india.github.io/id-methods-survey/

surveillance[17] can be encouraged as a means to holding public authorities accountable.

2. States should increase the representation of women, non-gender binary and trans officers among operators of video-based surveillance tools.

3. States and civil society should work towards creating safe spaces to facilitate multi-stakeholder collaborations and articulate local knowledges and experiences at the nexus of open data and gender(ed) data.

4. It is necessary for states, especially in the global south, to arrive at context-specific understandings of privacy. This would require the appropriate capturing of the lived experience of communities in ways that structural issues at various intersections can be acknowledged and addressed. Currently, policy making in the global South vis-à-vis data governance suffers from building off of narratives that have become entrenched in Northern discourse.

[17] Mann, S., Nolan, J. and Wellman B. (2004). Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society*, 1(3), 331-355.