

# **An Internet For #YesAllWomen?**

## **Women's rights, gender and equality in digital spaces**

### **Introduction**

1. Women's rights and gender equality are fundamental human rights, guaranteed in international treaties, standards and policy frameworks. These include, most recently, the Sustainable Development Goals which aim to achieve gender equality and empower women and girls as a fundamental human right. They also include the United Nations Convention on the Elimination of all Forms of Discrimination against Women (CEDAW) and its Optional Protocol, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Covenant on Economic, Social and Cultural Rights, and the Declaration on Violence Against Women. Key UN policy frameworks - such as the Vienna, Beijing and Cairo Declarations and Platforms for Action - commit States to gender equality.

2. In the 21<sup>st</sup> century, it is no longer adequate to address women's rights only *offline*. The 21<sup>st</sup> century differs from every other century in that digital technologies are now an integral part of our lives. Today, 95% of the world is covered by a mobile network and almost one out of two people (47%) use the Internet.<sup>i</sup> Globally, 3.9 billion people use the internet and 4.9 billion individuals use mobile technologies.<sup>ii</sup> Men, women and trans persons use the Internet for a wide range of activities: communication, entertainment, information, research, commerce, work and activism.

3. The Feminist Principles of the Internet provide a framework to explore and dive deeper into women's rights in digital spaces. Drafted and updated by more than 100 civil society organizations from Asia, Africa and Latin America, they offer a gendered lens on critical internet-related rights.

The principles are divided into five key clusters as follows:

- Access
- Movements and Public Participation
- Economy
- Expression
- Agency

This paper explores some of the issues that are part of the 'agency' cluster.

## Agency

Key issues: *Consent; Privacy and data; Memory; Anonymity*

4. In September 2017, a young man in India livestreamed on Facebook a video of a sexual act – without the consent of the woman in the video. In September 2016, a young woman in Italy committed suicide after her sex video continued to remain online – without her consent.<sup>iii</sup> The Supreme Court in India is currently hearing a case against 'rape videos' – which embody simultaneous violations of consent in physical and digital spaces. Rape videos also represent consent being violated thrice over: the rape itself, the filming, and the distribution.

5. Consent has emerged as a critical women's rights issue in the digital age. Women's agency lies in their ability to make informed decisions on what aspects of their public or private lives to share in digital spaces – as information, data, text, images or video. This is what consent means in practice.

6. Since most information online involves a two-step process – creation and distribution - digital consent must be understood as a multi-step practice, not a single-step concept. A woman may consent to participating only in the creation of an image or a video (step 1), including one that is intimate or sexual – but not consent to its distribution (step 2). This was what happened in the first two cases mentioned above. Or a woman may not consent to any of it - neither creation nor distribution - as in the rape videos. Either way, consent must be specifically sought, obtained, upheld and respected in each and every step of the digital cycle. In some countries, laws and legal judgements are separating these strands of consent – production and distribution - and separately punishing each violation.

7. While non-consensual production and distribution need to be treated as rights violations, consensual creations need to be protected. Legal distinctions between the 'consensual' and the 'non-consensual' need to be strengthened to enable freedom of expression, including sexual expression. Young women in particular negotiate freedom and censure and use online spaces to challenge cultural and social restrictions around sexuality, relationships and self-determination. Without laws that firmly distinguish the 'consensual' from the 'non-consensual', women who publish intimate digital images of themselves can be booked under statutes related to obscenity or indecency.

8. While the law is critical in upholding consent, it is not a sufficient mechanism to usher in an everyday practice of consent across digital platforms. What's also needed is an ethics of consent that is built and embedded into the culture, design, policies and practices of digital platforms.

9. Consent and privacy are closely linked to one another, both in physical and digital spaces. The concept of informed consent – used in research and medicine - rests on the understanding that participants’ privacy will be respected, both offline and online, where information or data is increasingly stored. Obtaining consent is necessary for any private information to be made public. However, enough information must be provided to an individual for them to exercise 'informed' or 'meaningful' consent. Digital users typically tick the 'terms of service' of digital platforms to signal their consent to a range of conditions, including how their data is collected, stored and used. Such 'terms of service' are considered too legalistic, lengthy and jargon-laden to meet the standards of meaningful consent, or to protect the privacy of users.

10. Privacy has emerged as a critical right in digital spaces for two main reasons. One, the right to privacy is essential for individuals to freely access information and express themselves. Two, the right to privacy is essential given the vast amounts of personal data that digital platforms collect, store, and use, often for their own purposes. The Office of the UN High Commissioner for Human Rights notes that “the Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individuals’ communications and activities on the Internet. Such practices can constitute a violation of the Internet users’ right to privacy, and, by undermining people’s confidence and security on the Internet, impede the free flow of information and ideas online.”

11. In the digital age, surveillance is one of the biggest threats to privacy – and expression. Almost any digital tool, platform or technology allows for mass surveillance, notes the Electronic Frontier Foundation. “In practice, the reach of these technologies is astonishingly broad: governments can listen in on cell phone calls, use voice recognition to scan mobile networks, read emails and text messages, censor web pages, track a citizen’s every movement using GPS, and can even change email contents while en route to a recipient...They can secretly turn on webcams built into personal laptops and microphones in cell phones not being used. And all of this information is filtered and organized on such a massive scale that it can be used to spy on every person in an entire country.”<sup>iv</sup>

12. Surveillance can create a chilling effect on the online expression of ordinary citizens, who may self-censor for fear of being constantly tracked. Surveillance also exerts a disproportionate impact on the freedom of expression of a wide range of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities, members of certain political parties, civil society, human rights defenders, professionals such as journalists, lawyers and trade unionists, victims of violence and abuse, and children.<sup>v</sup>

13. Surveillance is not a new phenomenon where women are concerned; women have always been under stringent surveillance by actors ranging from partners and parents to the State.<sup>vi</sup> The Internet Democracy Project notes that the digital age may have further deepened the scrutiny to which women are subjected - this has shaped and harmed, women's lives in multiple ways. In parts of India, local village bodies have banned young women from using mobile phones. CCTV cameras surveil women who work in garment factories. And safety apps track and collect information about women users, without specifying why or how this is being collected, stored or used.<sup>vii</sup>

14. Surveillance is used in digital spaces much as it is used in physical spaces: to restrict women's bodies, speech and activism. In this context, it is essential to understand surveillance as an obstacle to women's rights and gender equality. This means paying attention to and addressing surveillance practices by individuals, the private sector, the state and non-state actors.

15. Strengthening the right to privacy in digital spaces also means ensuring that an individual has full control over their personal data and information online at all levels. It means ensuring that States and private companies do not use personal data to manipulate digital behaviour or for other profit-making practices.

16. Since data lives on over time in digital spaces, ensuring the right to privacy also translates into enabling individuals to exercise and retain control over their personal data, histories and memories online. Individuals must be able to access personal data and information, know who has access to it and under what conditions, control this use and access, and retain the ability to delete it forever.

17. Strengthening the right to privacy online also means ensuring that individuals have the means to express themselves without revealing their identities. "Throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously," notes the UN Office of the High Commissioner for Human Rights. "The Internet allows individuals to access information and to engage in public debate without having to reveal their real identities, for example through the use of pseudonyms on message boards and chat forums."

18. Although the Internet offers tools and possibilities to hide one's face, voice, image, or location, such privacy is superficial in the absence of encryption. Noted the OHCHR: "The privacy afforded through such pseudonyms is superficial and easily disturbed by Governments or others with the

necessary expertise; in the absence of combinations of encryption and anonymizing tools, the digital traces that users leave behind render their identities easily discoverable. Users seeking to ensure full anonymity or mask their identity (such as hiding the original IP address) against State or criminal intrusion may use tools such as virtual private networks (VPNs), proxy services, anonymizing networks and software, and peer-to-peer networks.”

19. The OHCHR notes further notes that “journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one’s gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression.”

---

i

International Telecommunications Union

ii We Are Social 2017 data in <https://thenextweb.com/contributors/2017/04/11/current-global-state-internet/> or get We Are Social reference

iii <https://www.theguardian.com/world/2016/sep/16/italy-grapples-with-suicide-of-woman-taunted-over-online-sex-video>

iv <https://www.eff.org/issues/mass-surveillance-technologies>

v <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf?OpenElement>

vi <https://genderingsurveillance.internetdemocracy.in/>

vii <https://genderingsurveillance.internetdemocracy.in/>